StorageGRID 11.9 Softwaredokumentation

StorageGRID software

NetApp
October 07, 2025

Inhalt

StorageGRID 11.9 Softwaredokumentation

StorageGRID -Geräte

Gehe zu "StorageGRID Appliance-Dokumentation" um zu erfahren, wie Sie StorageGRID Speicher- und Servicegeräte installieren, konfigurieren und warten.

Versionshinweise

Erhalten Sie versionsspezifische Informationen zu behobenen und bekannten Problemen.

Melden Sie sich bei der NetApp Support Site an, um "PDF-Datei anzeigen oder herunterladen" enthält die Versionshinweise zu StorageGRID 11.9.

Erste Schritte mit einem StorageGRID -System

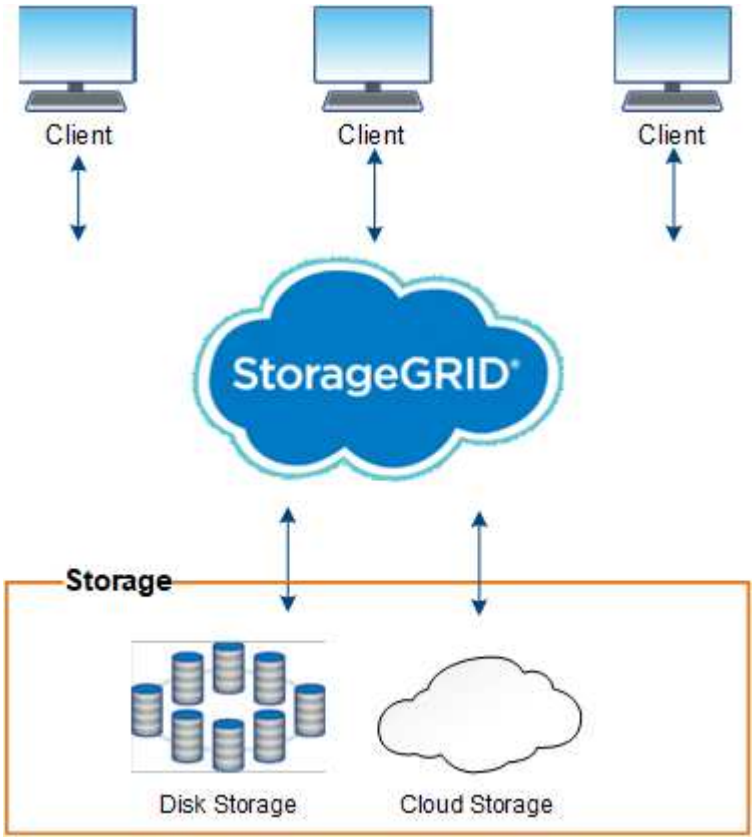
Erfahren Sie mehr über StorageGRID

Was ist StorageGRID?

NetApp® StorageGRID® ist eine softwaredefinierte Objektspeichersuite, die eine breite Palette von Anwendungsfällen in öffentlichen, privaten und hybriden Multicloud-Umgebungen unterstützt. StorageGRID bietet native Unterstützung für die Amazon S3-API und liefert branchenführende Innovationen wie automatisiertes Lebenszyklusmanagement, um unstrukturierte Daten über lange Zeiträume kostengünstig zu speichern, zu sichern, zu schützen und aufzubewahren.

StorageGRID bietet sicheren, dauerhaften Speicher für unstrukturierte Daten in großem Umfang. Integrierte, metadatengesteuerte Richtlinien zur Lebenszyklusverwaltung optimieren den Verbleib Ihrer Daten während ihrer gesamten Lebensdauer. Um die Kosten zu senken, werden Inhalte zur richtigen Zeit am richtigen Ort und auf der richtigen Speicherebene platziert.

StorageGRID besteht aus geografisch verteilten, redundanten, heterogenen Knoten, die sowohl in bestehende als auch in Clientanwendungen der nächsten Generation integriert werden können.



Die Unterstützung für Archivknoten wurde entfernt. Das Verschieben von Objekten von einem Archivknoten in ein externes Archivspeichersystem über die S3-API wurde ersetzt durch"ILM Cloud-Speicherpools" , die mehr Funktionalität bieten.

Vorteile von StorageGRID

Zu den Vorteilen des StorageGRID -Systems gehören:

- Ein massiv skalierbares und benutzerfreundliches, geografisch verteiltes Daten-Repository für unstrukturierte Daten.
- Standardprotokolle für die Objektspeicherung:
  - Amazon Web Services Simple Storage Service (S3)
  - OpenStack Swift

> Die Unterstützung für Swift-Clientanwendungen ist veraltet und wird in einer zukünftigen Version entfernt.

- Hybrid Cloud aktiviert. Das richtlinienbasierte Information Lifecycle Management (ILM) speichert Objekte in öffentlichen Clouds, darunter Amazon Web Services (AWS) und Microsoft Azure. Die Dienste der StorageGRID -Plattform ermöglichen die Inhaltsreplikation, Ereignisbenachrichtigung und Metadatensuche von in öffentlichen Clouds gespeicherten Objekten.
- Flexibler Datenschutz zur Gewährleistung von Langlebigkeit und Verfügbarkeit. Daten können durch Replikation und mehrschichtige Löschcodierung geschützt werden. Die Überprüfung ruhender und übertragener Daten gewährleistet die Integrität für die langfristige Speicherung.
- Dynamisches Datenlebenszyklusmanagement zur Unterstützung der Verwaltung der Speicherkosten. Sie können ILM-Regeln erstellen, die den Datenlebenszyklus auf Objektebene verwalten und dabei Datenlokalität, Haltbarkeit, Leistung, Kosten und Aufbewahrungszeit anpassen.
- Hohe Verfügbarkeit der Datenspeicherung und einiger Verwaltungsfunktionen mit integriertem Lastenausgleich zur Optimierung der Datenlast über StorageGRID -Ressourcen hinweg.
- Unterstützung für mehrere Speichermandantenkonten, um die auf Ihrem System nach verschiedenen Entitäten gespeicherten Objekte zu trennen.
- Zahlreiche Tools zur Überwachung des Zustands Ihres StorageGRID -Systems, darunter ein umfassendes Warnsystem, ein grafisches Dashboard und detaillierte Statusinformationen für alle Knoten und Sites.
- Unterstützung für software- oder hardwarebasierte Bereitstellung. Sie können StorageGRID auf einem der folgenden Geräte bereitstellen:
  - Virtuelle Maschinen, die in VMware ausgeführt werden.
  - Container-Engines auf Linux-Hosts.
  - Von StorageGRID entwickelte Geräte.
    - Speichergeräte bieten Objektspeicher.
    - Service-Appliances bieten Netzverwaltungs- und Lastausgleichsdienste.
- Konform mit den relevanten Aufbewahrungsanforderungen dieser Verordnung:
  - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), die Börsenmitglieder, Makler oder Händler reguliert.
  - Regel 4511(c) der Financial Industry Regulatory Authority (FINRA), die sich den Format- und Medienanforderungen der SEC-Regel 17a-4(f) unterwirft.
  - Commodity Futures Trading Commission (CFTC) in Verordnung 17 CFR § 1.31(c)-(d), die den Handel mit Rohstoff-Futures regelt.
- Unterbrechungsfreie Upgrade- und Wartungsvorgänge. Behalten Sie den Zugriff auf Inhalte während Upgrade-, Erweiterungs-, Außerbetriebnahme- und Wartungsverfahren bei.

- Föderiertes Identitätsmanagement. Integriert sich zur Benutzerauthentifizierung in Active Directory, OpenLDAP oder Oracle Directory Service. Unterstützt Single Sign-On (SSO) mithilfe des Security Assertion Markup Language 2.0 (SAML 2.0)-Standards zum Austausch von Authentifizierungs- und Autorisierungsdaten zwischen StorageGRID und Active Directory Federation Services (AD FS).

Hybrid Clouds mit StorageGRID

Verwenden Sie StorageGRID in einer Hybrid-Cloud-Konfiguration, indem Sie ein richtliniengesteuertes Datenmanagement implementieren, um Objekte in Cloud-Speicherpools zu speichern, StorageGRID -Plattformdienste nutzen und Daten mit NetApp FabricPool von ONTAP auf StorageGRID verschieben.

Cloud-Speicherpools

Mit Cloud-Speicherpools können Sie Objekte außerhalb des StorageGRID -Systems speichern. Beispielsweise möchten Sie möglicherweise selten aufgerufene Objekte in einen kostengünstigeren Cloud-Speicher verschieben, etwa Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archivzugriffsebene im Microsoft Azure Blob-Speicher. Oder Sie möchten möglicherweise ein Cloud-Backup von StorageGRID -Objekten verwalten, mit dem Sie Daten wiederherstellen können, die aufgrund eines Speichervolumes- oder Speicherknotenausfalls verloren gegangen sind.

Auch Speicher von Drittanbietern wird unterstützt, darunter Festplatten- und Bandspeicher.

> Die Verwendung von Cloud Storage Pools mit FabricPool wird aufgrund der zusätzlichen Latenz beim Abrufen eines Objekts vom Cloud Storage Pool-Ziel nicht unterstützt.

S3-Plattformdienste

S3-Plattformdienste bieten Ihnen die Möglichkeit, Remotedienste als Endpunkte für die Objektreplikation, Ereignisbenachrichtigungen oder Suchintegration zu verwenden. Plattformdienste arbeiten unabhängig von den ILM-Regeln des Grids und sind für einzelne S3-Buckets aktiviert. Folgende Dienste werden unterstützt:

- Der CloudMirror-Replikationsdienst spiegelt angegebene Objekte automatisch in einen Ziel-S3-Bucket, der sich auf Amazon S3 oder einem zweiten StorageGRID System befinden kann.
- Der Ereignisbenachrichtigungsdienst sendet Nachrichten über angegebene Aktionen an einen externen Endpunkt, der den Empfang von Simple Notification Service (Amazon SNS)-Ereignissen unterstützt.
- Der Suchintegrationsdienst sendet Objektmetadaten an einen externen Elasticsearch-Dienst, sodass Metadaten mithilfe von Tools von Drittanbietern gesucht, visualisiert und analysiert werden können.

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.

ONTAP -Daten-Tiering mit FabricPool

Sie können die Kosten für ONTAP -Speicher senken, indem Sie Daten mithilfe von FabricPool auf StorageGRID auslagern. FabricPool ermöglicht die automatische Zuordnung von Daten zu kostengünstigen Objektspeicherebenen, entweder vor Ort oder außerhalb.

Im Gegensatz zu manuellen Tiering-Lösungen reduziert FabricPool die Gesamtbetriebskosten, indem es das Tiering der Daten automatisiert und so die Speicherkosten senkt. Es bietet die Vorteile der Cloud-Ökonomie durch die Einstufung in öffentliche und private Clouds, einschließlich StorageGRID.

Ähnliche Informationen

- "Was ist ein Cloud-Speicherpool?"
- "Plattformdienste verwalten"
- "Konfigurieren von StorageGRID für FabricPool"

StorageGRID -Architektur und Netzwerktopologie

Ein StorageGRID -System besteht aus mehreren Arten von Grid-Knoten an einem oder mehreren Rechenzentrumsstandorten.

Siehe die"Beschreibungen der Rasterknotentypen" .

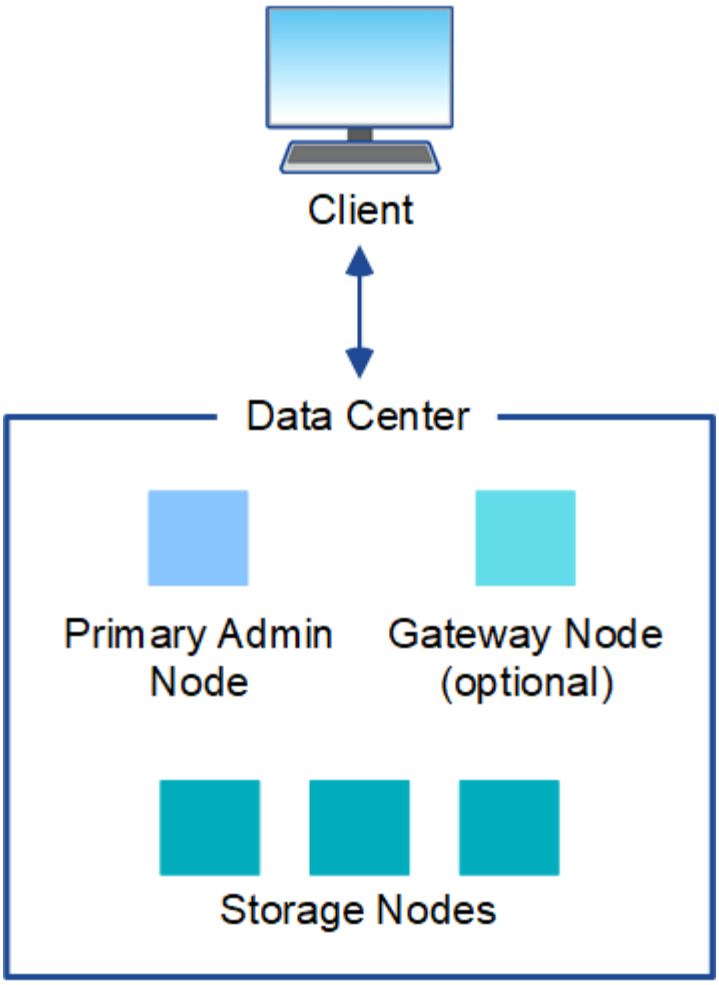
Weitere Informationen zur StorageGRID -Netzwerktopologie, den Anforderungen und der Grid-Kommunikation finden Sie im"Netzwerkrichtlinien" .

Bereitstellungstopologien

Das StorageGRID -System kann an einem einzelnen oder an mehreren Rechenzentrumsstandorten bereitgestellt werden.

Einzelne Site

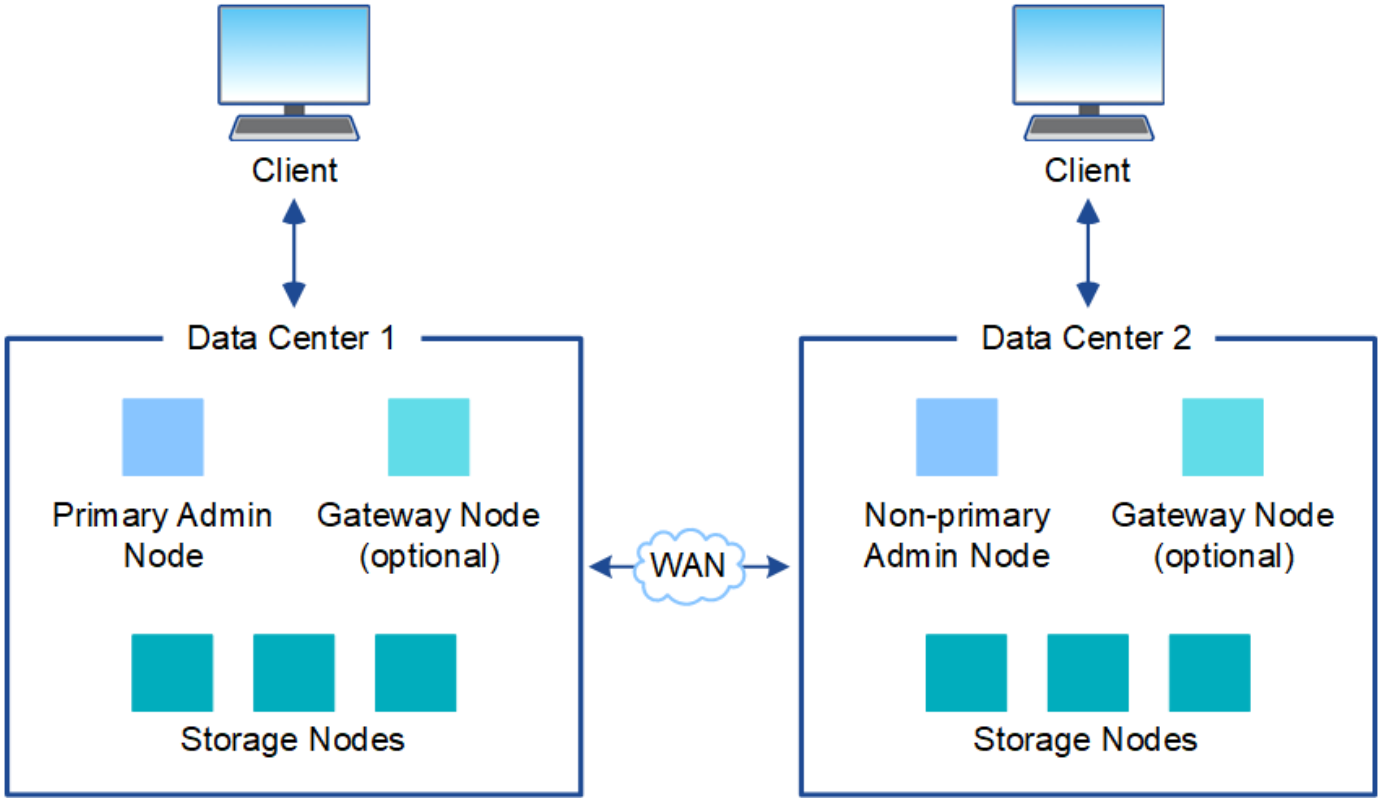
Bei einer Bereitstellung mit einem einzelnen Standort sind die Infrastruktur und der Betrieb des StorageGRID -Systems zentralisiert.



Mehrere Standorte

Bei einer Bereitstellung mit mehreren Standorten können an jedem Standort unterschiedliche Typen und Anzahlen von StorageGRID -Ressourcen installiert werden. Beispielsweise kann in einem Rechenzentrum mehr Speicherplatz erforderlich sein als in einem anderen.

Verschiedene Standorte liegen oft an geografisch unterschiedlichen Orten in unterschiedlichen Störungsbereichen, beispielsweise an einer Erdbebenverwerfungslinie oder in einem Überschwemmungsgebiet. Datenfreigabe und Notfallwiederherstellung werden durch die automatisierte Verteilung der Daten an andere Standorte erreicht.



Innerhalb eines einzigen Rechenzentrums können auch mehrere logische Standorte vorhanden sein, um die Verwendung von verteilter Replikation und Erasure Coding zur Erhöhung der Verfügbarkeit und Ausfallsicherheit zu ermöglichen.

Netzknotenredundanz

Bei einer Bereitstellung an einem oder mehreren Standorten können Sie aus Redundanzgründen optional mehr als einen Admin-Knoten oder Gateway-Knoten einschließen. Sie können beispielsweise mehr als einen Admin-Knoten an einem einzelnen Standort oder an mehreren Standorten installieren. Allerdings kann jedes StorageGRID -System nur einen primären Admin-Knoten haben.

Systemarchitektur

Dieses Diagramm zeigt, wie Grid-Knoten innerhalb eines StorageGRID Systems angeordnet sind.

S3-Clients speichern und rufen Objekte in StorageGRID ab. Andere Clients werden zum Senden von E-Mail-Benachrichtigungen, zum Zugriff auf die StorageGRID -Verwaltungsschnittstelle und optional zum Zugriff auf die Audit-Freigabe verwendet.

S3-Clients können eine Verbindung zu einem Gateway-Knoten oder einem Admin-Knoten herstellen, um die Lastausgleichsschnittstelle zu Speicherknoten zu verwenden. Alternativ können S3-Clients über HTTPS eine direkte Verbindung zu Speicherknoten herstellen.

Objekte können innerhalb von StorageGRID auf software- oder hardwarebasierten Speicherknoten oder in Cloud-Speicherpools gespeichert werden, die aus externen S3-Buckets oder Azure Blob-Speichercontainern bestehen.

Netzknoten und Dienste

Netzknoten und Dienste

Der grundlegende Baustein eines StorageGRID -Systems ist der Grid-Knoten. Knoten enthalten Dienste, bei denen es sich um Softwaremodule handelt, die einem Grid-Knoten eine Reihe von Funktionen bereitstellen.

Arten von Gitterknoten

Das StorageGRID -System verwendet vier Arten von Grid-Knoten:

Admin-Knoten

Bereitstellung von Verwaltungsdiensten wie Systemkonfiguration, Überwachung und Protokollierung. Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her. Jedes Grid muss über einen primären Admin-Knoten verfügen und kann zur Redundanz über zusätzliche nicht-primäre Admin-Knoten verfügen. Sie können eine Verbindung zu jedem Admin-Knoten herstellen und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID Systems an. Wartungsverfahren müssen jedoch mithilfe des primären Admin-Knotens durchgeführt werden.

Admin-Knoten können auch zum Lastenausgleich des S3-Client-Verkehrs verwendet werden.

Sehen"Was ist ein Admin-Knoten?"

Speicherknoten

Verwalten und speichern Sie Objektdaten und Metadaten. Jeder Standort in Ihrem StorageGRID -System muss über mindestens drei Speicherknoten verfügen.

Sehen"Was ist ein Speicherknoten?"

Gateway-Knoten (optional)

Stellen Sie eine Lastausgleichsschnittstelle bereit, die Clientanwendungen zum Herstellen einer Verbindung mit StorageGRID verwenden können. Ein Load Balancer leitet Clients nahtlos zu einem optimalen Speicherknoten weiter, sodass der Ausfall von Knoten oder sogar einer ganzen Site transparent ist.

Sehen"Was ist ein Gateway-Knoten?"

Hardware- und Softwareknoten

StorageGRID Knoten können als StorageGRID Appliance-Knoten oder als softwarebasierte Knoten bereitgestellt werden.

StorageGRID -Geräteknoten

StorageGRID Hardwaregeräte sind speziell für die Verwendung in einem StorageGRID -System konzipiert. Einige Geräte können als Speicherknoten verwendet werden. Andere Appliances können als Admin-Knoten oder Gateway-Knoten verwendet werden. Sie können Appliance-Knoten mit softwarebasierten Knoten kombinieren oder vollständig entwickelte Grids mit ausschließlich Appliances bereitstellen, die nicht von externen Hypervisoren, Speichern oder Computerhardware abhängig sind.

Im Folgenden finden Sie Informationen zu den verfügbaren Geräten:

- "StorageGRID Appliance-Dokumentation"

- "NetApp Hardware Universe"

Softwarebasierte Knoten

Softwarebasierte Grid-Knoten können als virtuelle VMware-Maschinen oder innerhalb von Container-Engines auf einem Linux-Host bereitgestellt werden.

- Virtuelle Maschine (VM) in VMware vSphere: Siehe"Installieren Sie StorageGRID auf VMware" .
- Innerhalb einer Container-Engine auf Red Hat Enterprise Linux: Siehe"Installieren Sie StorageGRID unter Red Hat Enterprise Linux" .
- Innerhalb einer Container-Engine auf Ubuntu oder Debian: Siehe"Installieren Sie StorageGRID unter Ubuntu oder Debian" .

Verwenden Sie die "NetApp Interoperability Matrix Tool (IMT)" um die unterstützten Versionen zu ermitteln.

Bei der Erstinstallation eines neuen softwarebasierten Storage Node können Sie festlegen, dass dieser nur für"Metadaten speichern" .

StorageGRID Dienste

Nachfolgend finden Sie eine vollständige Liste der StorageGRID -Dienste.

Service	Beschreibung	Standort
Kontodienst-Weiterleitung	Stellt eine Schnittstelle für den Load Balancer-Dienst bereit, um den Account-Dienst auf Remote-Hosts abzufragen, und sendet Benachrichtigungen über Konfigurationsänderungen des Load Balancer-Endpunkts an den Load Balancer-Dienst.	Load Balancer-Dienst auf Admin-Knoten und Gateway-Knoten
ADC (Administrativer Domänencontroller)	Verwaltet Topologieinformationen, stellt Authentifizierungsdienste bereit und antwortet auf Anfragen der LDR- und CMN-Dienste.	Mindestens drei Speicherknoten, die den ADC-Dienst an jedem Standort enthalten
AMS (Audit-Management-System)	Überwacht und protokolliert alle geprüften Systemereignisse und Transaktionen in einer Textprotokolldatei.	Admin-Knoten
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch.	Speicherknoten
Chunk-Dienst	Verwaltet erasure-coded Daten und Paritätsfragmente.	Speicherknoten
CMN (Konfigurationsverwaltungsknoten)	Verwaltet systemweite Konfigurationen und Grid-Aufgaben. Jedes Grid verfügt über einen CMN-Dienst.	Primärer Admin-Knoten

Service	Beschreibung	Standort
DDS (Verteilter Datenspeicher)	Schnittstellen mit der Cassandra-Datenbank zur Verwaltung von Objektmetadaten.	Speicherknoten
DMV (Datenverschieber)	Verschiebt Daten zu Cloud-Endpunkten.	Speicherknoten
Dynamische IP (dynip)	Überwacht das Grid auf dynamische IP-Änderungen und aktualisiert lokale Konfigurationen.	Alle Knoten
Grafana	Wird zur Visualisierung von Metriken im Grid Manager verwendet.	Admin-Knoten
Hohe Verfügbarkeit	Verwaltet hochverfügbare virtuelle IPs auf Knoten, die auf der Seite „Hochverfügbarkeitsgruppen“ konfiguriert sind. Dieser Dienst wird auch als Keepalived-Dienst bezeichnet.	Admin- und Gateway-Knoten
Identität (idnt)	Föderiert Benutzeridentitäten aus LDAP und Active Directory.	Speicherknoten, die den ADC-Dienst verwenden
Lambda-Schiedsrichter	Verwaltet S3 Select SelectObjectContent-Anfragen.	Alle Knoten
Lastenausgleich (nginx-gw)	Bietet Lastausgleich des S3-Verkehrs von Clients zu Speicherknoten. Der Load Balancer-Dienst kann über die Konfigurationsseite „Load Balancer-Endpunkte“ konfiguriert werden. Dieser Dienst ist auch als nginx-gw-Dienst bekannt.	Admin- und Gateway-Knoten
LDR (Lokaler Verteilungsrouter)	Verwaltet die Speicherung und Übertragung von Inhalten innerhalb des Grids.	Speicherknoten
MISCd Information Service Control Daemon	Bietet eine Schnittstelle zum Abfragen und Verwalten von Diensten auf anderen Knoten und zum Verwalten von Umgebungskonfigurationen auf dem Knoten, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Knoten
nginx	Fungiert als Authentifizierungs- und sicherer Kommunikationsmechanismus für verschiedene Grid-Dienste (wie Prometheus und Dynamic IP), um über HTTPS-APIs mit Diensten auf anderen Knoten kommunizieren zu können.	Alle Knoten

Service	Beschreibung	Standort
nginx-gw	Unterstützt den Load Balancer-Dienst.	Admin- und Gateway-Knoten
NMS (Netzwerkmanagementsystem)	Unterstützt die Überwachungs-, Berichts- und Konfigurationsoptionen, die über den Grid Manager angezeigt werden.	Admin-Knoten
Persistenz	Verwaltet Dateien auf der Root-Festplatte, die nach einem Neustart erhalten bleiben müssen.	Alle Knoten
Prometheus	Sammelt Zeitreihenmetriken von Diensten auf allen Knoten.	Admin-Knoten
RSM (Replizierte Zustandsmaschine)	Stellt sicher, dass Plattformdienstanfragen an die jeweiligen Endpunkte gesendet werden.	Speicherknoten, die den ADC-Dienst verwenden
SSM (Server Status Monitor)	Überwacht den Zustand der Hardware und meldet ihn an den NMS-Dienst.	Auf jedem Grid-Knoten ist eine Instanz vorhanden
Spurensammler	Führt eine Ablaufverfolgung durch, um Informationen für den technischen Support zu sammeln. Der Trace-Collector-Dienst verwendet die Open-Source-Software von Jaeger.	Admin-Knoten

Was ist ein Admin-Knoten?

Admin-Knoten bieten Verwaltungsdienste wie Systemkonfiguration, Überwachung und Protokollierung. Admin-Knoten können auch zum Lastenausgleich des S3-Client-Verkehrs verwendet werden. Jedes Grid muss über einen primären Admin-Knoten verfügen und kann aus Redundanzgründen eine beliebige Anzahl nicht-primärer Admin-Knoten haben.

Unterschiede zwischen primären und nicht-primären Admin-Knoten

Wenn Sie sich beim Grid Manager oder Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her. Sie können eine Verbindung zu jedem Admin-Knoten herstellen und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID Systems an. Der primäre Admin-Knoten bietet jedoch mehr Funktionen als nicht-primäre Admin-Knoten. Beispielsweise müssen die meisten Wartungsvorgänge von den primären Admin-Knoten aus durchgeführt werden.

Die Tabelle fasst die Funktionen primärer und nicht primärer Admin-Knoten zusammen.

Funktionen	Primärer Admin-Knoten	Nicht-primärer Admin-Knoten
Beinhaltet dieAMS Service	Ja	Ja

Funktionen	Primärer Admin-Knoten	Nicht-primärer Admin-Knoten
Beinhaltet dieCMN Service	Ja	Nein
Beinhaltet dieNMS Service	Ja	Ja
Beinhaltet diePrometheus Service	Ja	Ja
Beinhaltet dieSSM Service	Ja	Ja
Beinhaltet dieLastenausgleich UndHohe Verfügbarkeit Dienstleistungen	Ja	Ja
Unterstützt dieManagement-Anwendungsprogrammschnittstelle (MGMT-API)	Ja	Ja
Kann für alle netzwerkbezogenen Wartungsaufgaben verwendet werden, beispielsweise IP-Adressänderung und Aktualisierung von NTP-Servern	Ja	Nein
Kann nach der Erweiterung des Speicherknotens eine EC-Neuverteilung durchführen	Ja	Nein
Kann für die Volumenwiederherstellung verwendet werden	Ja	Ja
Kann Protokolldateien und Systemdaten von einem oder mehreren Knoten sammeln	Ja	Nein
Sendet Warnmeldungen, AutoSupport -Pakete und SNMP-Traps und informiert	Ja. Fungiert alsbevorzugter Absender .	Ja. Fungiert als Standby-Sender.

Admin-Knoten des bevorzugten Absenders

Wenn Ihre StorageGRID -Bereitstellung mehrere Admin-Knoten umfasst, ist der primäre Admin-Knoten der bevorzugte Absender für Warnbenachrichtigungen, AutoSupport -Pakete sowie SNMP-Traps und -Informationen.

Im normalen Systembetrieb sendet nur der bevorzugte Absender Benachrichtigungen. Alle anderen Admin-Knoten überwachen jedoch den bevorzugten Absender. Wenn ein Problem erkannt wird, fungieren andere Admin-Knoten als *Standby-Sender*.

In diesen Fällen können mehrere Benachrichtigungen gesendet werden:

- Wenn Admin-Knoten voneinander isoliert werden, versuchen sowohl der bevorzugte Absender als auch die Standby-Absender, Benachrichtigungen zu senden, und es können mehrere Kopien der Benachrichtigungen empfangen werden.
- Wenn der Standby-Absender Probleme mit dem bevorzugten Absender erkennt und mit dem Senden von

Benachrichtigungen beginnt, kann der bevorzugte Absender möglicherweise seine Fähigkeit zum Senden von Benachrichtigungen wiedererlangen. In diesem Fall werden möglicherweise doppelte Benachrichtigungen gesendet. Der Standby-Absender stellt das Senden von Benachrichtigungen ein, wenn er beim bevorzugten Absender keine Fehler mehr erkennt.

Wenn Sie AutoSupport Pakete testen, senden alle Admin-Knoten den Test. Wenn Sie Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Konnektivität zu überprüfen.

Primäre Dienste für Admin-Knoten

Die folgende Tabelle zeigt die primären Dienste für Admin-Knoten. Allerdings sind in dieser Tabelle nicht alle Knotendienste aufgeführt.

Service	Tastenfunktion
Audit Management System (AMS)	Verfolgt Systemaktivitäten und Ereignisse.
Konfigurationsverwaltungsknoten (CMN)	Verwaltet die systemweite Konfiguration.
Hohe Verfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Knoten und Gateway-Knoten. **Hinweis:** Dieser Dienst ist auch auf Gateway-Knoten verfügbar.
Lastenausgleich	Bietet Lastausgleich des S3-Verkehrs von Clients zu Speicherknoten. **Hinweis:** Dieser Dienst ist auch auf Gateway-Knoten verfügbar.
Management-Anwendungsprogrammschnittstelle (mgmt-api)	Verarbeitet Anfragen von der Grid Management API und der Tenant Management API.
Netzwerkmanagementsystem (NMS)	Bietet Funktionen für den Grid Manager.
Prometheus	Sammelt und speichert Zeitreihenmetriken von den Diensten auf allen Knoten.
Server Status Monitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

Was ist ein Speicherknoten?

Speicherknoten verwalten und speichern Objektdaten und Metadaten. Speicherknoten umfassen die Dienste und Prozesse, die zum Speichern, Verschieben, Überprüfen und Abrufen von Objektdaten und Metadaten auf der Festplatte erforderlich sind.

Jeder Standort in Ihrem StorageGRID -System muss über mindestens drei Speicherknoten verfügen.

Arten von Speicherknoten

Während der Installation können Sie den Typ des Speicherknotens auswählen, den Sie installieren möchten. Diese Typen sind für softwarebasierte Speicherknoten und für gerätebasierte Speicherknoten verfügbar, die die Funktion unterstützen:

- Kombinierter Daten- und Metadaten-Speicherknoten
- Nur-Metadaten-Speicherknoten
- Nur-Daten-Speicherknoten

Sie können den Speicherknotentyp in folgenden Situationen auswählen:

- Bei der Erstinstallation eines Storage Node
- Wenn Sie während der StorageGRID -Systemerweiterung einen Speicherknoten hinzufügen

> ⓘ Sie können den Typ nicht mehr ändern, nachdem die Installation des Speicherknotens abgeschlossen ist.

Daten- und Metadaten-Speicherknoten (kombiniert)

Standardmäßig speichern alle neuen Speicherknoten sowohl Objektdaten als auch Metadaten. Dieser Speicherknotentyp wird als *kombinierter* Speicherknoten bezeichnet.

Nur-Metadaten-Speicherknoten

Die Verwendung eines Speicherknotens ausschließlich für Metadaten kann sinnvoll sein, wenn Ihr Grid eine sehr große Anzahl kleiner Objekte speichert. Durch die Installation dedizierter Metadatenkapazität wird ein besseres Gleichgewicht zwischen dem für eine sehr große Anzahl kleiner Objekte benötigten Speicherplatz und dem für die Metadaten dieser Objekte benötigten Speicherplatz erreicht. Darüber hinaus können reine Metadaten-Speicherknoten, die auf Hochleistungsgeräten gehostet werden, die Leistung steigern.

Für reine Metadaten-Speicherknoten gelten bestimmte Hardwareanforderungen:

- Bei Verwendung von StorageGRID -Geräten können reine Metadatenknoten nur auf SGF6112-Geräten mit zwölf 1,9-TB- oder zwölf 3,8-TB-Laufwerken konfiguriert werden.
- Bei der Verwendung softwarebasierter Knoten müssen die Knotenressourcen, die nur Metadaten enthalten, mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:
  - Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
    - 128 GB RAM
    - 8-Kern-CPU
    - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)
  - Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).
- Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

Bei der Installation von reinen Metadatenknoten muss das Grid auch eine Mindestanzahl von Knoten zur

Datenspeicherung enthalten:

- Konfigurieren Sie für ein Single-Site-Grid mindestens zwei kombinierte oder reine Datenspeicherknoten.
- Konfigurieren Sie für ein Grid mit mehreren Standorten mindestens einen kombinierten oder Nur-Daten-Speicherknoten *pro Standort*.

> Obwohl reine Metadaten-Speicherknoten dieLDR-Dienst und S3-Clientanforderungen verarbeiten kann, wird die StorageGRID Leistung möglicherweise nicht gesteigert.

Nur-Daten-Speicherknoten

Die Verwendung eines Speicherknotens ausschließlich für Daten kann sinnvoll sein, wenn Ihre Speicherknoten unterschiedliche Leistungsmerkmale aufweisen. Um die Leistung potenziell zu steigern, könnten Sie beispielsweise ausschließlich Daten speichernde, hochleistungsfähige rotierende Festplatten-Speicherknoten zusammen mit ausschließlich Metadaten speichernden Hochleistungs-Speicherknoten einsetzen.

Beim Installieren von Nur-Daten-Knoten muss das Raster Folgendes enthalten:

- Mindestens zwei kombinierte oder reine Datenspeicherknoten *pro Raster*
- Mindestens ein kombinierter oder reiner Datenspeicherknoten *pro Site*
- Mindestens drei kombinierte oder reine Metadaten-Speicherknoten *pro Site*

Primäre Dienste für Speicherknoten

Die folgende Tabelle zeigt die primären Dienste für Speicherknoten. Allerdings sind in dieser Tabelle nicht alle Knotendienste aufgeführt.

> Einige Dienste, wie etwa der ADC-Dienst und der RSM-Dienst, sind normalerweise nur auf drei Speicherknoten an jedem Standort vorhanden.

Service	Tastenfunktion
Konto (acct)	Verwaltet Mieterkonten.

Service	Tastenfunktion
Administrativer Domänencontroller (ADC)	Behält die Topologie und die netzweite Konfiguration bei. **Hinweis**: Reine Datenspeicherknoten hosten den ADC-Dienst nicht. **Details** Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen untereinander. Der ADC-Dienst wird auf mindestens drei Speicherknoten an einem Standort gehostet. Der ADC-Dienst verwaltet Topologieinformationen, einschließlich des Standorts und der Verfügbarkeit von Diensten. Wenn ein Grid-Knoten Informationen von einem anderen Grid-Knoten benötigt oder eine Aktion von einem anderen Grid-Knoten ausgeführt werden soll, kontaktiert er einen ADC-Dienst, um den besten Grid-Knoten zur Verarbeitung seiner Anfrage zu finden. Darüber hinaus behält der ADC-Dienst eine Kopie der Konfigurationspakete der StorageGRID -Bereitstellung bei, sodass jeder Grid-Knoten aktuelle Konfigurationsinformationen abrufen kann. Um verteilte und isolierte Vorgänge zu ermöglichen, synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen zu Diensten und Topologie mit den anderen ADC-Diensten im StorageGRID System. Im Allgemeinen halten alle Grid-Knoten eine Verbindung zu mindestens einem ADC-Dienst aufrecht. Dadurch wird sichergestellt, dass die Grid-Knoten immer auf die neuesten Informationen zugreifen. Wenn Grid-Knoten eine Verbindung herstellen, speichern sie die Zertifikate anderer Grid-Knoten im Cache, sodass Systeme auch dann mit bekannten Grid-Knoten weiter funktionieren, wenn ein ADC-Dienst nicht verfügbar ist. Neue Grid-Knoten können Verbindungen nur mithilfe eines ADC-Dienstes herstellen. Durch die Verbindung jedes Grid-Knotens kann der ADC-Dienst Topologieinformationen sammeln. Zu diesen Grid-Knoteninformationen gehören die CPU-Auslastung, der verfügbare Speicherplatz (sofern vorhanden), unterstützte Dienste und die Site-ID des Grid-Knotens. Andere Dienste fragen den ADC-Dienst über Topologieabfragen nach Topologieinformationen. Der ADC-Dienst antwortet auf jede Abfrage mit den neuesten Informationen, die er vom StorageGRID -System erhält.
Kassandra	Speichert und schützt Objektmetadaten. **Hinweis**: Reine Datenspeicherknoten hosten den Cassandra-Dienst nicht.
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch. **Hinweis**: Reine Datenspeicherknoten hosten den Cassandra Reaper-Dienst nicht.
Brocken	Verwaltet erasure-coded Daten und Paritätsfragmente.

Service	Tastenfunktion
Datenverschieber (dmv)	Verschiebt Daten in Cloud-Speicherpools.
Verteilter Datenspeicher (DDS)	Überwacht die Speicherung von Objektmetadaten. **Details** Jeder Speicherknoten umfasst den Distributed Data Store (DDS)-Dienst. Dieser Dienst interagiert mit der Cassandra-Datenbank, um Hintergrundaufgaben an den im StorageGRID System gespeicherten Objektmetadaten auszuführen. Der DDS-Dienst verfolgt die Gesamtzahl der in das StorageGRID System aufgenommenen Objekte sowie die Gesamtzahl der über jede der unterstützten Schnittstellen des Systems aufgenommenen Objekte (S3).
Identität (idnt)	Föderiert Benutzeridentitäten aus LDAP und Active Directory.

Service	Tastenfunktion
Lokaler Verteilungsrouter (LDR)	Verarbeitet Objektspeicherprotokollanforderungen und verwaltet Objektdaten auf der Festplatte.

Service	Tastenfunktion
Replizierte Zustandsmaschine (RSM)	Stellt sicher, dass Anfragen zu S3-Plattformdiensten an die jeweiligen Endpunkte gesendet werden.
Serverstatusmonitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

Was ist ein Gateway-Knoten?

Gateway-Knoten bieten eine dedizierte Lastausgleichsschnittstelle, die S3-Clientanwendungen zum Herstellen einer Verbindung mit StorageGRID verwenden können. Durch Lastenausgleich werden Geschwindigkeit und Verbindungskapazität maximiert, indem die Arbeitslast auf mehrere Speicherknoten verteilt wird. Gateway-Knoten sind optional.

Der StorageGRID Load Balancer-Dienst wird auf allen Admin-Knoten und allen Gateway-Knoten bereitgestellt. 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 leitet Clients nahtlos zu einem optimalen Speicherknoten weiter, sodass der Ausfall von Knoten oder sogar einer ganzen Site transparent ist.

Sie konfigurieren einen oder mehrere Load Balancer-Endpunkte, um den Port und das Netzwerkprotokoll (HTTPS oder HTTP) zu definieren, die eingehende und ausgehende Clientanforderungen für den Zugriff auf die Load Balancer-Dienste auf Gateway- und Admin-Knoten verwenden. Der Load Balancer-Endpunkt definiert außerdem den Clienttyp (S3), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten. Sehen "Überlegungen zum Lastenausgleich"

Bei Bedarf können Sie die Netzwerkschnittstellen mehrerer Gateway-Knoten und Admin-Knoten in einer Hochverfügbarkeitsgruppe (HA) zusammenfassen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast der Client-Anwendung verwalten. Sehen "Verwalten von Hochverfügbarkeitsgruppen (HA)"

Primäre Dienste für Gateway-Knoten

Die folgende Tabelle zeigt die primären Dienste für Gateway-Knoten. Allerdings sind in dieser Tabelle nicht alle Knotendienste aufgeführt.

Service	Tastenfunktion
Hohe Verfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Knoten und Gateway-Knoten. **Hinweis:** Dieser Dienst ist auch auf Admin-Knoten zu finden.
Lastenausgleich	Bietet Layer-7-Lastausgleich des S3-Verkehrs von Clients zu Speicherknoten. Dies ist der empfohlene Lastausgleichsmechanismus. **Hinweis:** Dieser Dienst ist auch auf Admin-Knoten zu finden.

Grösstell der harten Arbeit des StorageGRID Systems, indem er Datenübertragungslasten und Datenverkehrsfunktionen handhabt.

Der LDR-Dienst übernimmt folgende Aufgaben:

- Anfragen
- Aktivität zum Information Lifecycle Management (ILM)
- Objektlöschung
- Objektdatenspeicherung
- Objektdatenübertragungen von einem anderen LDR-Dienst (Storage Node)
- Datenspeicherverwaltung
- S3-Protokollschnittstelle

Der LDR-Dienst ordnet außerdem jedes S3-Objekt seiner eindeutigen SGUID zu.

Objektspeicher

Der zugrunde liegende Datenspeicher eines LDR-Dienstes ist in eine feste Anzahl von Objektspeichern (auch als Speichervolumes bezeichnet) unterteilt. Jeder Objektspeicher ist ein separater Einhängepunkt.

Die Objektspeicher in einem Speicherknoten werden durch eine Hexadezimalzahl von 0000 bis 002F identifiziert, die als Volume-ID bezeichnet wird. Im ersten Objektspeicher (Volume 0) ist Speicherplatz für Objektmetadaten in einer Cassandra-Datenbank reserviert. Der verbleibende Speicherplatz auf diesem Volume wird für Objektdaten verwendet. Alle anderen Objektspeicher werden ausschließlich für Objektdaten verwendet, darunter replizierte Kopien und löschcodierte

die mit dem LDR-Dienst interagiert.

Um Redundanz und damit Schutz vor Verlust zu gewährleisten, werden an jedem Standort drei Kopien der Objektmetadaten vorgehalten. Diese Replikation ist nicht konfigurierbar und wird automatisch durchgeführt. Weitere Informationen finden Sie unter "Verwalten des

Service	Tastenfunktion
Serverstatusmonitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

Was ist ein Archivknoten?

Die Unterstützung für Archivknoten wurde entfernt.

Informationen zu Archivknoten finden Sie unter "Was ist ein Archivknoten (StorageGRID 11.8-Dokumentationsseite)" .

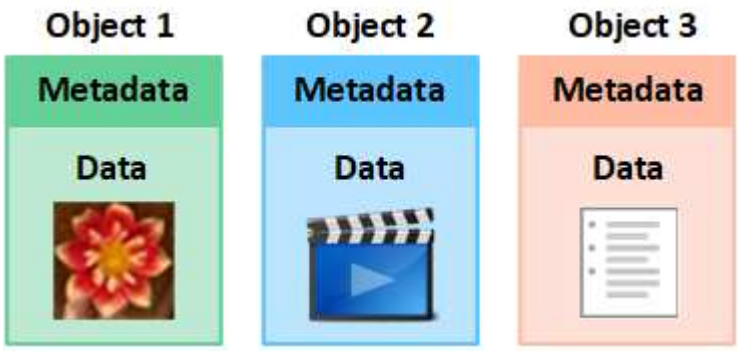
So verwaltet StorageGRID Daten

Was ist ein Objekt

Bei der Objektspeicherung ist die Speichereinheit ein Objekt und keine Datei oder ein Block. Im Gegensatz zur baumartigen Hierarchie eines Dateisystems oder Blockspeichers organisiert der Objektspeicher Daten in einem flachen, unstrukturierten Layout.

Durch die Objektspeicherung wird der physische Speicherort der Daten von der Methode entkoppelt, die zum Speichern und Abrufen dieser Daten verwendet wird.

Jedes Objekt in einem objektbasierten Speichersystem besteht aus zwei Teilen: Objektdaten und Objektmetadaten.



Was sind Objektdaten?

Objektdaten können alles Mögliche sein, beispielsweise ein Foto, ein Film oder eine Krankenakte.

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.

Zu den Objektmetadaten gehören beispielsweise die folgenden Informationen:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), des Objektnamens, des Namens des S3-Buckets oder Swift-Containers, des Mandantenkontonamens oder der ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Erstellung des Objekts sowie des Datums und

der Uhrzeit der letzten Änderung des Objekts.

- Der aktuelle Speicherort jeder Objektkopie oder jedes Erasure-Coded-Fragments.
- Alle mit dem Objekt verknüpften Benutzermetadaten.

Objektmetadaten sind anpassbar und erweiterbar, sodass sie für Anwendungen flexibel nutzbar sind.

Ausführliche Informationen dazu, wie und wo StorageGRID Objektmetadaten speichert, finden Sie unter"Verwalten des Objektmetadatenspeichers" .

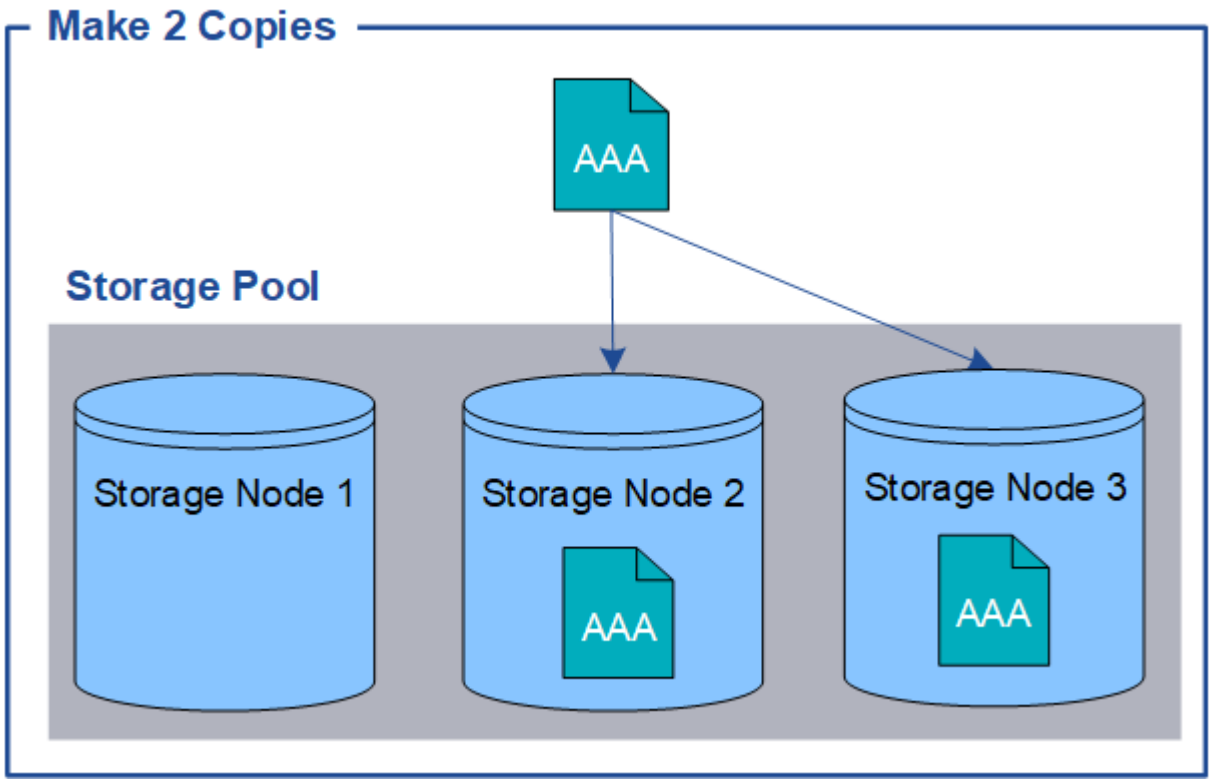
Wie werden Objektdaten geschützt?

Das StorageGRID -System bietet Ihnen zwei Mechanismen zum Schutz von Objektdaten vor Verlust: Replikation und Erasure Coding.

Replikation

Wenn StorageGRID Objekte einer ILM-Regel (Information Lifecycle Management) zuordnet, die für die Erstellung replizierter Kopien konfiguriert ist, erstellt das System exakte Kopien der Objektdaten und speichert sie auf Speicherknoten oder Cloud-Speicherpools. ILM-Regeln bestimmen die Anzahl der erstellten Kopien, den Speicherort dieser Kopien und die Dauer ihrer Aufbewahrung durch das System. Wenn eine Kopie verloren geht, beispielsweise durch den Verlust eines Speicherknotens, ist das Objekt weiterhin verfügbar, wenn an anderer Stelle im StorageGRID -System eine Kopie davon vorhanden ist.

Im folgenden Beispiel gibt die Regel „2 Kopien erstellen“ an, dass zwei replizierte Kopien jedes Objekts in einem Speicherpool abgelegt werden, der drei Speicherknoten enthält.

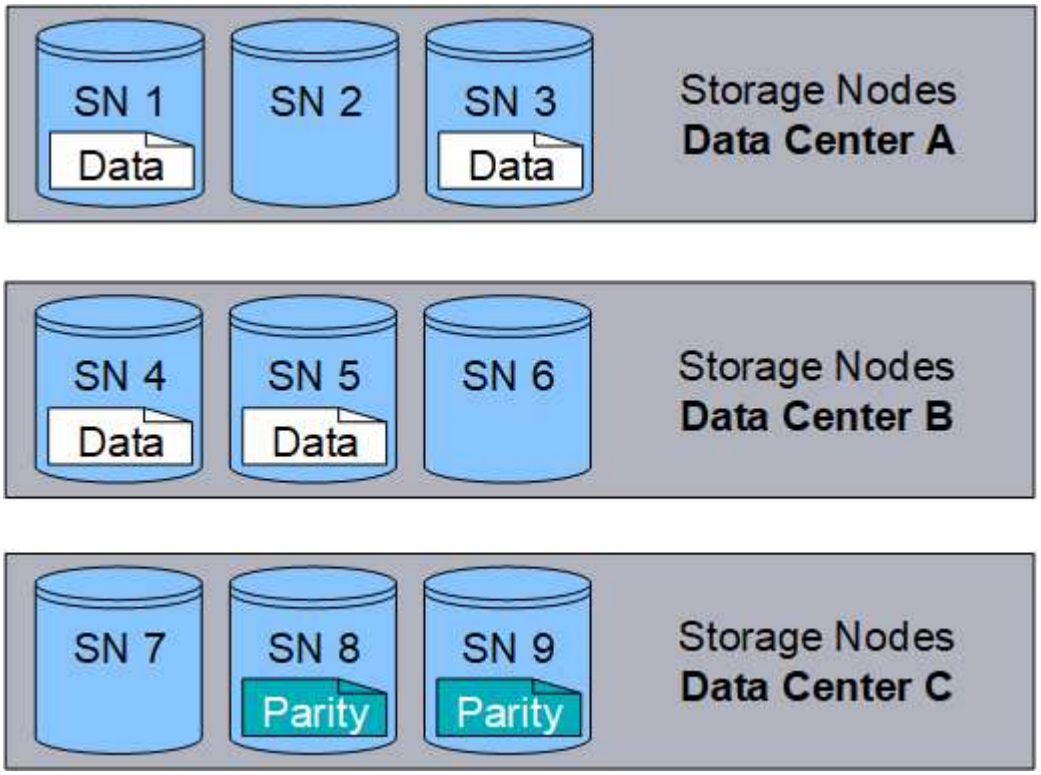


Löschcodierung

Wenn StorageGRID Objekte einer ILM-Regel zuordnet, die zum Erstellen von Erasure-Coded-Kopien konfiguriert ist, zerlegt es die Objektdaten in Datenfragmente, berechnet zusätzliche Paritätsfragmente und

speichert jedes Fragment auf einem anderen Speicherknoten. Beim Zugriff auf ein Objekt wird es anhand der gespeicherten Fragmente wieder zusammengesetzt. Wenn Daten oder ein Paritätsfragment beschädigt werden oder verloren gehen, kann der Erasure-Coding-Algorithmus dieses Fragment mithilfe einer Teilmenge der verbleibenden Daten und Paritätsfragmente wiederherstellen. ILM-Regeln und Erasure-Coding-Profile bestimmen das verwendete Erasure-Coding-Schema.

Das folgende Beispiel veranschaulicht die Verwendung von Erasure Coding auf die Daten eines Objekts. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Erasure-Coding-Schema. Jedes Objekt wird in vier gleiche Datenfragmente aufgeteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente wird auf einem anderen Speicherknoten in drei Rechenzentren gespeichert, um Datenschutz bei Knotenausfällen oder Standortverlusten zu gewährleisten.



Ähnliche Informationen

- "Objekte mit ILM verwalten"
- "Nutzen Sie Information Lifecycle Management"

Das Leben eines Objekts

Das Leben eines Objekts besteht aus verschiedenen Phasen. Jede Phase stellt die Vorgänge dar, die mit dem Objekt durchgeführt werden.

Zum Lebenszyklus eines Objekts gehören die Vorgänge Aufnahme, Kopierverwaltung, Abrufen und Löschen.

- **Ingest**: Der Prozess einer S3-Clientanwendung, die ein Objekt über HTTP im StorageGRID -System speichert. In dieser Phase beginnt das StorageGRID -System mit der Verwaltung des Objekts.
- **Kopienverwaltung**: Der Prozess der Verwaltung replizierter und löschcodierter Kopien in StorageGRID, wie in den ILM-Regeln in den aktiven ILM-Richtlinien beschrieben. Während der Kopierverwaltungsphase schützt StorageGRID Objektdaten vor Verlust, indem es die angegebene Anzahl und Art von Objektkopien auf Speicherknoten oder in einem Cloud-Speicherpool erstellt und verwaltet.

- **Abrufen**: Der Prozess einer Client-Anwendung, die auf ein vom StorageGRID -System gespeichertes Objekt zugreift. Der Client liest das Objekt, das von einem Speicherknoten oder Cloud-Speicherpool abgerufen wird.
- **Löschen**: Der Vorgang zum Entfernen aller Objektkopien aus dem Raster. Objekte können entweder gelöscht werden, indem die Clientanwendung eine Löschanforderung an das StorageGRID -System sendet, oder als Ergebnis eines automatischen Prozesses, den StorageGRID ausführt, wenn die Lebensdauer des Objekts abläuft.

Ähnliche Informationen

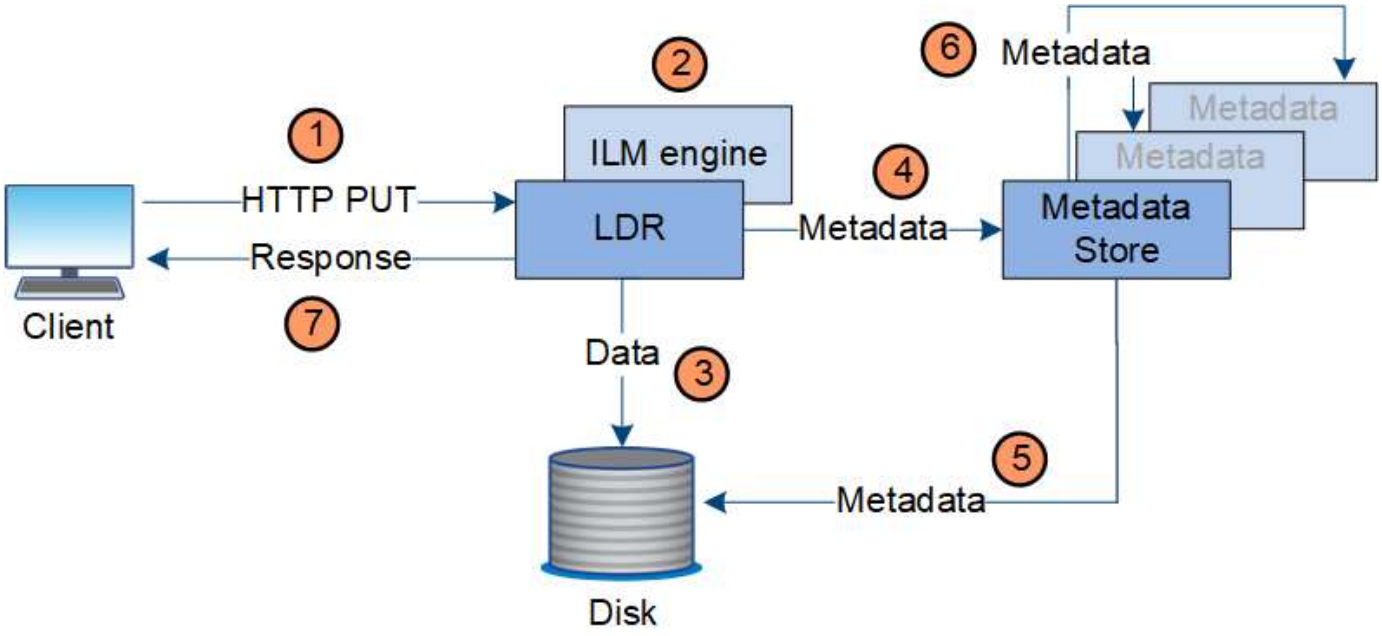
- "Objekte mit ILM verwalten"
- "Nutzen Sie Information Lifecycle Management"

Datenfluss erfassen

Ein Aufnahme- oder Speichervorgang besteht aus einem definierten Datenfluss zwischen dem Client und dem StorageGRID -System.

Datenfluss

Wenn ein Client ein Objekt in das StorageGRID -System einspeist, verarbeitet der LDR-Dienst auf den Speicherknoten die Anforderung und speichert die Metadaten und Daten auf der Festplatte.



1. Die Clientanwendung erstellt das Objekt und sendet es über eine HTTP-PUT-Anfrage an das StorageGRID -System.
2. Das Objekt wird anhand der ILM-Richtlinie des Systems ausgewertet.
3. Der LDR-Dienst speichert die Objektdaten als replizierte Kopie oder als Erasure-Coded-Kopie. (Das Diagramm zeigt eine vereinfachte Version der Speicherung einer replizierten Kopie auf der Festplatte.)
4. Der LDR-Dienst sendet die Objektmetadaten an den Metadatenspeicher.
5. Der Metadatenspeicher speichert die Objektmetadaten auf der Festplatte.
6. Der Metadatenspeicher überträgt Kopien von Objektmetadaten an andere Speicherknoten. Diese Kopien

werden auch auf der Festplatte gespeichert.

7. Der LDR-Dienst gibt eine HTTP 200 OK-Antwort an den Client zurück, um zu bestätigen, dass das Objekt aufgenommen wurde.

Kopierverwaltung

Objektdaten werden durch die aktiven ILM-Richtlinien und zugehörigen ILM-Regeln verwaltet. ILM-Regeln erstellen replizierte oder löschcodierte Kopien, um Objektdaten vor Verlust zu schützen.

Zu unterschiedlichen Zeitpunkten im Lebenszyklus eines Objekts können unterschiedliche Typen oder Speicherorte von Objektkopien erforderlich sein. ILM-Regeln werden regelmäßig ausgewertet, um sicherzustellen, dass Objekte wie erforderlich platziert werden.

Die Objektdaten werden vom LDR-Dienst verwaltet.

Inhaltsschutz: Replikation

Wenn die Anweisungen zur Inhaltsplatzierung einer ILM-Regel replizierte Kopien von Objektdaten erfordern, werden Kopien erstellt und von den Speicherknoten, aus denen der konfigurierte Speicherpool besteht, auf der Festplatte gespeichert.

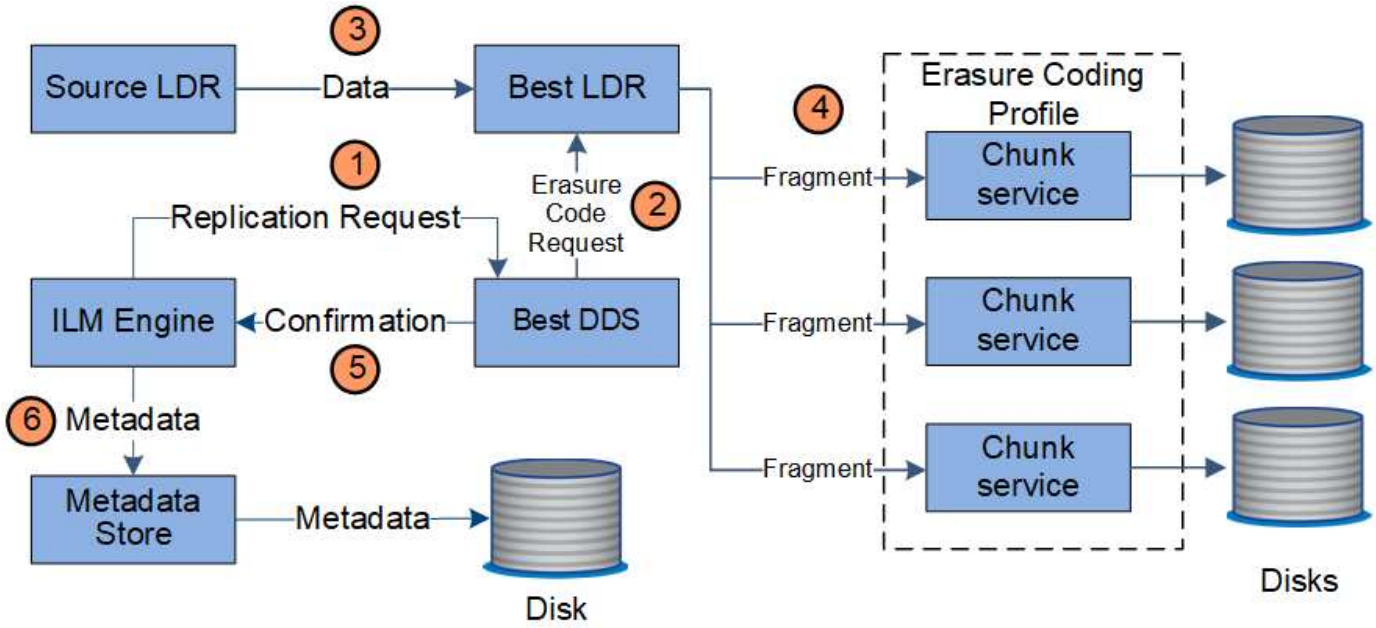
Die ILM-Engine im LDR-Dienst steuert die Replikation und stellt sicher, dass die richtige Anzahl von Kopien an den richtigen Orten und für die richtige Zeit gespeichert wird.

1. Die ILM-Engine fragt den ADC-Dienst ab, um den besten Ziel-LDR-Dienst innerhalb des durch die ILM-Regel angegebenen Speicherpools zu ermitteln. Anschließend sendet es diesem LDR-Dienst einen Befehl zum Starten der Replikation.
2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellstandort ab. Anschließend sendet es eine Replikationsanforderung an den Quell-LDR-Dienst.
3. Der Quell-LDR-Dienst sendet eine Kopie an den Ziel-LDR-Dienst.
4. Der Ziel-LDR-Dienst benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.
5. Die ILM-Engine aktualisiert den Metadatenspeicher mit Objektstandortmetadaten.

Inhaltsschutz: Erasure Coding

Wenn eine ILM-Regel Anweisungen zum Erstellen von Erasure-Coding-Kopien von Objektdaten enthält, zerlegt das entsprechende Erasure-Coding-Schema die Objektdaten in Daten- und Paritätsfragmente und verteilt diese Fragmente auf die im Erasure-Coding-Profil konfigurierten Speicherknoten.

Die ILM-Engine, die Bestandteil des LDR-Dienstes ist, steuert das Erasure Coding und stellt sicher, dass das Erasure-Coding-Profil auf die Objektdaten angewendet wird.

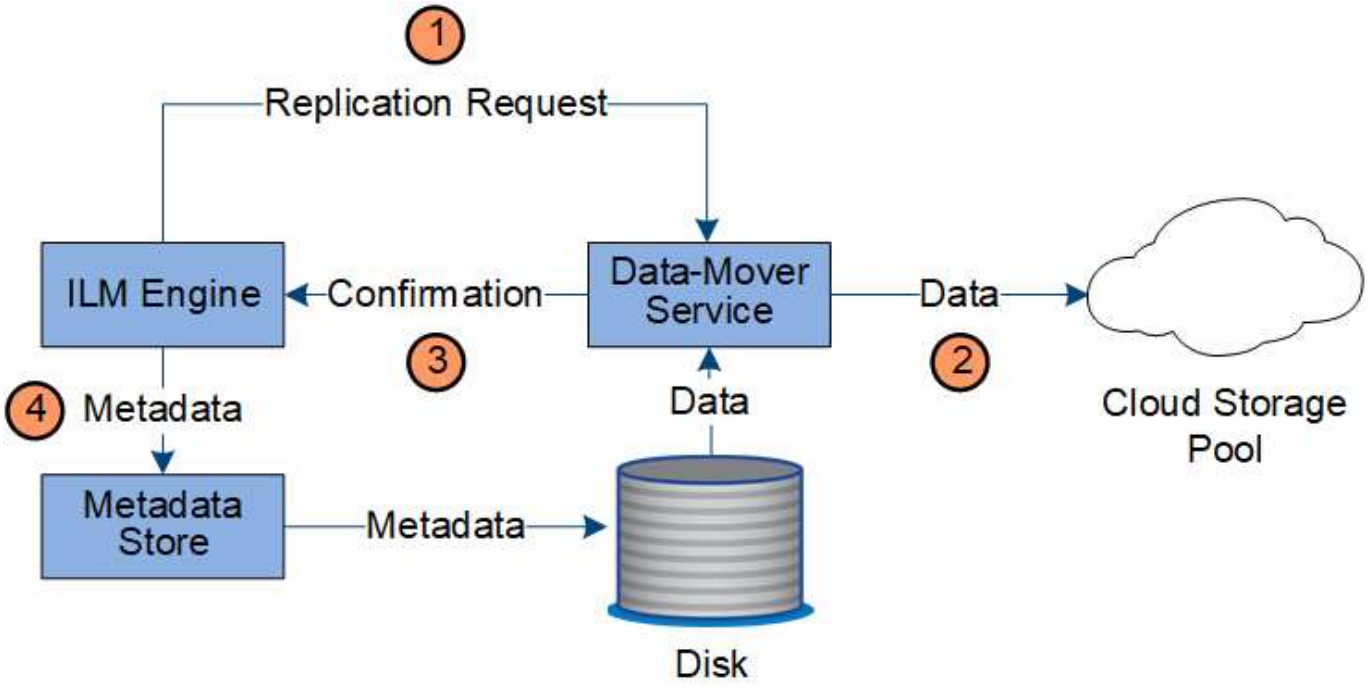


1. Die ILM-Engine fragt den ADC-Dienst ab, um zu ermitteln, welcher DDS-Dienst den Erasure-Coding-Vorgang am besten durchführen kann. Wenn dies festgestellt wird, sendet die ILM-Engine eine „Initialisierungs“-Anforderung an diesen Dienst.
2. Der DDS-Dienst weist einen LDR an, die Objektdaten mit einem Löschcode zu versehen.
3. Der Quell-LDR-Dienst sendet eine Kopie an den für die Erasure Coding ausgewählten LDR-Dienst.
4. Nachdem die entsprechende Anzahl an Paritäts- und Datenfragmenten erstellt wurde, verteilt der LDR-Dienst diese Fragmente auf die Speicherknoten (Chunk-Dienste), die den Speicherpool des Erasure-Coding-Profils bilden.
5. Der LDR-Dienst benachrichtigt die ILM-Engine und bestätigt, dass die Objektdaten erfolgreich verteilt wurden.
6. Die ILM-Engine aktualisiert den Metadatenspeicher mit Objektstandortmetadaten.

Inhaltsschutz: Cloud-Speicherpool

Wenn die Anweisungen zur Inhaltsplatzierung einer ILM-Regel erfordern, dass eine replizierte Kopie der Objektdaten in einem Cloud-Speicherpool gespeichert wird, werden die Objektdaten in den externen S3-Bucket oder Azure Blob-Speichercontainer dupliziert, der für den Cloud-Speicherpool angegeben wurde.

Die ILM-Engine, die eine Komponente des LDR-Dienstes ist, und der Data Mover-Dienst steuern die Bewegung von Objekten in den Cloud Storage Pool.



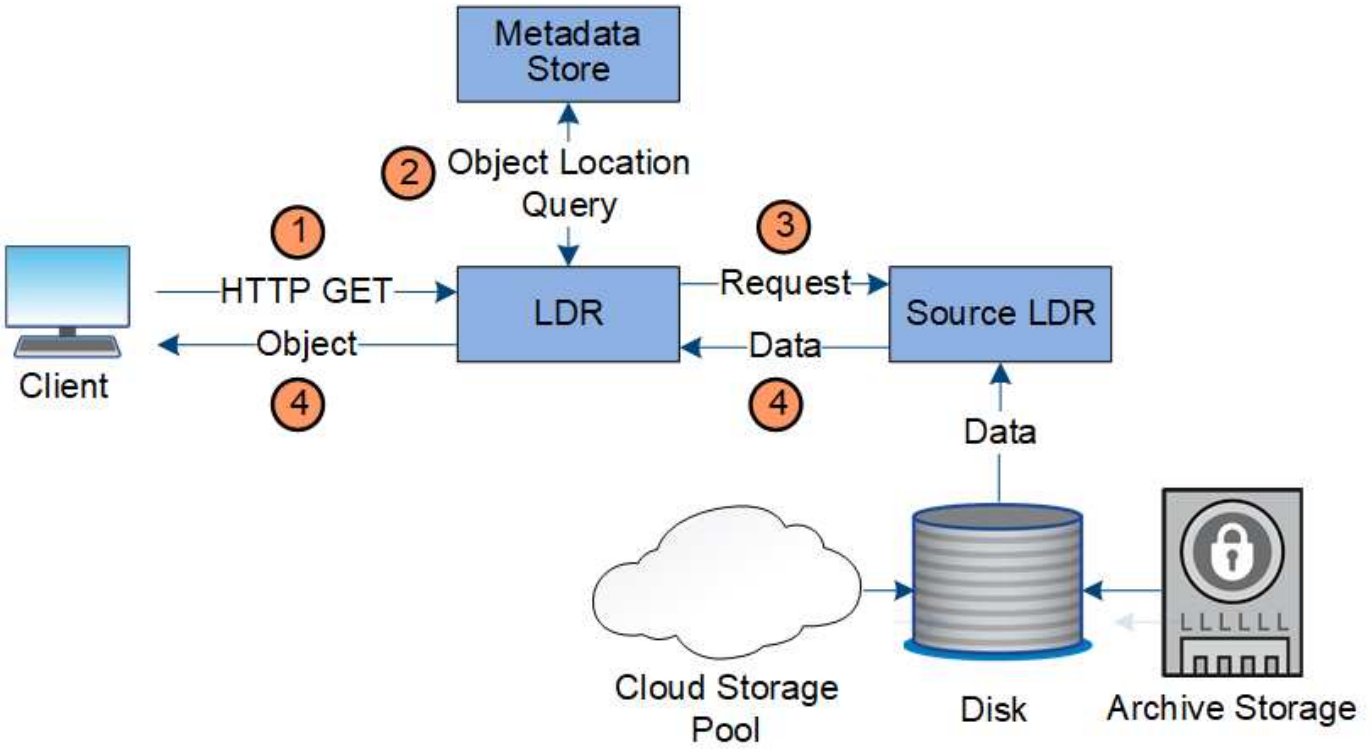
1. Die ILM-Engine wählt einen Data Mover-Dienst zur Replikation in den Cloud Storage Pool aus.
2. Der Data Mover-Dienst sendet die Objektdaten an den Cloud Storage Pool.
3. Der Data Mover-Dienst benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.
4. Die ILM-Engine aktualisiert den Metadatenspeicher mit Objektstandortmetadaten.

Datenfluss abrufen

Ein Abrufvorgang besteht aus einem definierten Datenfluss zwischen dem StorageGRID -System und dem Client. Das System verwendet Attribute, um den Abruf des Objekts von einem Speicherknoten oder, falls erforderlich, einem Cloud-Speicherpool zu verfolgen.

Der LDR-Dienst des Speicherknotens fragt den Metadatenspeicher nach dem Speicherort der Objektdaten ab und ruft sie vom Quell-LDR-Dienst ab. Der Abruf erfolgt vorzugsweise von einem Speicherknoten. Wenn das Objekt auf einem Speicherknoten nicht verfügbar ist, wird die Abrufanforderung an einen Cloud-Speicherpool weitergeleitet.

> Wenn sich die einzige Objektkopie im AWS Glacier-Speicher oder in der Azure-Archivebene befindet, muss die Clientanwendung eine S3 RestoreObject-Anforderung ausgeben, um eine abrufbare Kopie im Cloud-Speicherpool wiederherzustellen.



1. Der LDR-Dienst empfängt eine Abrufanforderung von der Clientanwendung.
2. Der LDR-Dienst fragt den Metadatenspeicher nach dem Speicherort der Objektdaten und den Metadaten ab.
3. Der LDR-Dienst leitet die Abrufanforderung an den Quell-LDR-Dienst weiter.
4. Der Quell-LDR-Dienst gibt die Objektdaten vom abgefragten LDR-Dienst zurück und das System gibt das Objekt an die Clientanwendung zurück.

Datenfluss löschen

Alle Objektkopien werden aus dem StorageGRID -System entfernt, wenn ein Client einen Löschvorgang durchführt oder wenn die Lebensdauer des Objekts abläuft und dadurch seine automatische Entfernung ausgelöst wird. Für die Objektlöschung gibt es einen definierten Datenfluss.

Löschhierarchie

StorageGRID bietet mehrere Methoden zur Steuerung, wann Objekte aufbewahrt oder gelöscht werden. Objekte können auf Clientanforderung oder automatisch gelöscht werden. StorageGRID priorisiert alle S3-Objektsperreinstellungen immer gegenüber Client-Löschanforderungen, die wiederum Vorrang vor dem S3-Bucket-Lebenszyklus und ILM-Platzierungsanweisungen haben.

- **S3-Objektsperre**: Wenn die globale Einstellung „S3-Objektsperre“ für das Raster aktiviert ist, können S3-Clients Buckets mit aktivierter S3-Objektsperre erstellen und dann die S3-REST-API verwenden, um Einstellungen für die Aufbewahrungsdauer und die rechtliche Aufbewahrung für jede diesem Bucket hinzugefügte Objektversion festzulegen.
  - Eine Objektversion, die einer rechtlichen Sperre unterliegt, kann mit keiner Methode gelöscht werden.
  - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version mit keiner Methode gelöscht werden.

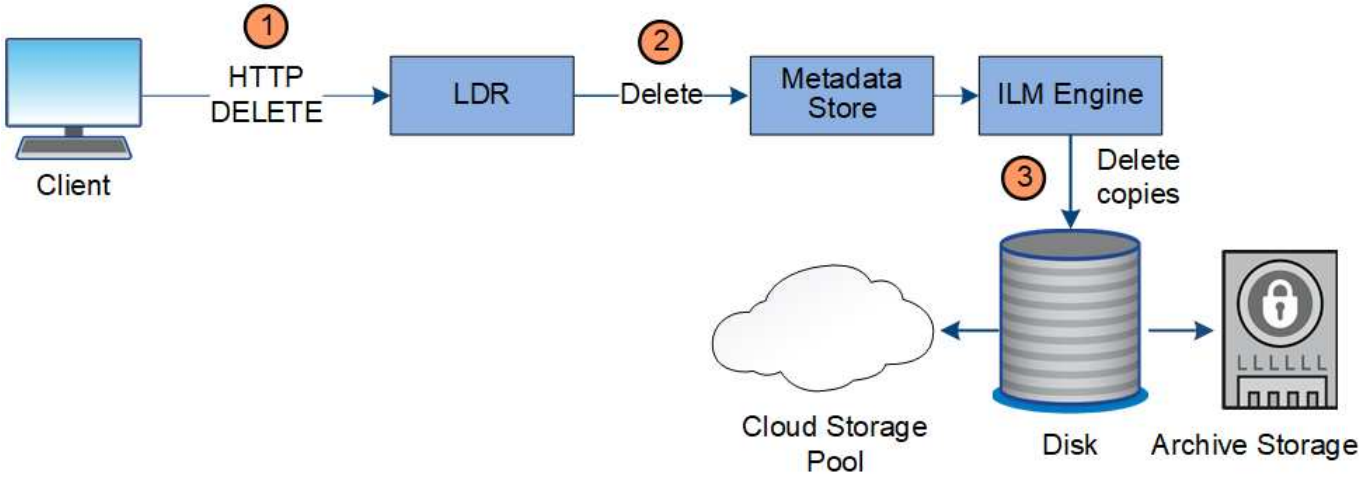
- Objekte in Buckets mit aktivierter S3-Objektsperre werden von ILM „für immer“ aufbewahrt. Nach Erreichen des Aufbewahrungsdatums kann eine Objektversion jedoch durch eine Clientanforderung oder den Ablauf des Bucket-Lebenszyklus gelöscht werden.
- Wenn S3-Clients ein Standard-Aufbewahrungsdatum auf den Bucket anwenden, müssen sie nicht für jedes Objekt ein Aufbewahrungsdatum angeben.

- **Client-Löschanforderung**: Ein S3-Client kann eine Löschanforderung für ein Objekt stellen. Wenn ein Client ein Objekt löscht, werden alle Kopien des Objekts aus dem StorageGRID System entfernt.
- **Objekte im Bucket löschen**: Tenant Manager-Benutzer können diese Option verwenden, um alle Kopien der Objekte und Objektversionen in ausgewählten Buckets dauerhaft aus dem StorageGRID System zu entfernen.
- **S3-Bucket-Lebenszyklus**: S3-Clients können ihren Buckets eine Lebenszykluskonfiguration hinzufügen, die eine Ablaufaktion angibt. Wenn ein Bucket-Lebenszyklus vorhanden ist, löscht StorageGRID automatisch alle Kopien eines Objekts, wenn das in der Ablaufaktion angegebene Datum oder die Anzahl der Tage erreicht ist, es sei denn, der Client löscht das Objekt zuerst.
- **Anweisungen zur ILM-Platzierung**: Vorausgesetzt, für den Bucket ist die S3-Objektsperre nicht aktiviert und es gibt keinen Bucket-Lebenszyklus, löscht StorageGRID ein Objekt automatisch, wenn der letzte Zeitraum in der ILM-Regel endet und keine weiteren Platzierungen für das Objekt angegeben sind.

> Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Aktionen zum Ablauf des Lebenszyklus die ILM-Richtlinie für Objekte, die dem Lebenszyklusfilter entsprechen. Dies kann dazu führen, dass ein Objekt auch dann noch auf dem Raster verbleibt, wenn keine ILM-Anweisungen zum Platzieren des Objekts mehr vorliegen.

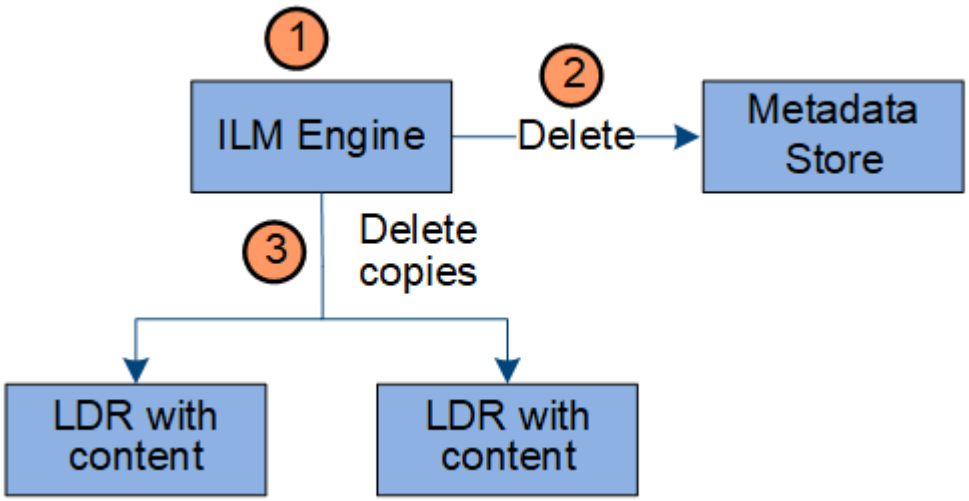
Sehen "So werden Objekte gelöscht" für weitere Informationen.

Datenfluss für Clientlöschungen



1. Der LDR-Dienst empfängt eine Löschanforderung von der Clientanwendung.
2. Der LDR-Dienst aktualisiert den Metadatenspeicher, sodass das Objekt für Clientanforderungen als gelöscht angezeigt wird, und weist die ILM-Engine an, alle Kopien der Objektdaten zu entfernen.
3. Das Objekt wird aus dem System entfernt. Der Metadatenspeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Datenfluss für ILM-Löschvorgänge



1. Die ILM-Engine stellt fest, dass das Objekt gelöscht werden muss.
2. Die ILM-Engine benachrichtigt den Metadatenspeicher. Der Metadatenspeicher aktualisiert die Objektmetadaten, sodass das Objekt für Clientanforderungen gelöscht aussieht.
3. Die ILM-Engine entfernt alle Kopien des Objekts. Der Metadatenspeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Informationslebenszyklusmanagement

Sie verwenden Information Lifecycle Management (ILM), um die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System zu steuern. ILM-Regeln bestimmen, wie StorageGRID Objekte im Laufe der Zeit speichert. Sie konfigurieren eine oder mehrere ILM-Regeln und fügen sie dann einer ILM-Richtlinie hinzu. Ein Grid kann gleichzeitig über mehrere aktive Richtlinien verfügen.

ILM-Regeln definieren:

- Welche Objekte sollen gespeichert werden? Eine Regel kann für alle Objekte gelten, oder Sie können Filter angeben, um zu ermitteln, für welche Objekte eine Regel gilt. Beispielsweise kann eine Regel nur für Objekte gelten, die mit bestimmten Mandantenkonten, bestimmten S3-Buckets oder Swift-Containern oder bestimmten Metadatenwerten verknüpft sind.
- Der Speichertyp und -ort. Objekte können auf Speicherknoten oder in Cloud-Speicherpools gespeichert werden.
- Der Typ der erstellten Objektkopien. Kopien können repliziert oder mit einem Erasure Code versehen werden.
- Bei replizierten Kopien die Anzahl der erstellten Kopien.
- Bei Erasure-Coding-Kopien das verwendete Erasure-Coding-Schema.
- Die Änderungen im Laufe der Zeit am Speicherort eines Objekts und an der Art der Kopien.
- Wie Objektdaten geschützt werden, wenn Objekte in das Raster aufgenommen werden (synchrone Platzierung oder Dual Commit).

Beachten Sie, dass Objektmetadaten nicht durch ILM-Regeln verwaltet werden. Stattdessen werden Objektmetadaten in einer Cassandra-Datenbank in einem sogenannten Metadatenspeicher gespeichert. Um die Daten vor Verlust zu schützen, werden an jedem Standort automatisch drei Kopien der Objektmetadaten

verwaltet.

Beispiel einer ILM-Regel

Beispielsweise könnte eine ILM-Regel Folgendes festlegen:

- Gilt nur für die Objekte, die Mieter A gehören.
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Ort.
- Bewahren Sie die beiden Kopien „für immer“ auf, was bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte, bis sie durch eine Löschanforderung des Clients oder durch Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die Option „Ausgewogen“ für das Aufnahmeverhalten: Die Anweisung zur Platzierung an zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, beide erforderlichen Kopien sofort zu erstellen.

  Wenn beispielsweise Site 2 nicht erreichbar ist, wenn Mandant A ein Objekt speichert, erstellt StorageGRID zwei Zwischenkopien auf Speicherknoten an Site 1. Sobald Site 2 verfügbar ist, erstellt StorageGRID die erforderliche Kopie an diesem Site.

So bewertet eine ILM-Richtlinie Objekte

Die aktiven ILM-Richtlinien für Ihr StorageGRID -System steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte.

Wenn Clients Objekte in StorageGRID speichern, werden die Objekte anhand des geordneten ILM-Regelsatzes in der aktiven Richtlinie wie folgt ausgewertet:

1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten dieser Regel aufgenommen und gemäß den Platzierungsanweisungen dieser Regel gespeichert.
2. Wenn die Filter für die erste Regel nicht mit dem Objekt übereinstimmen, wird das Objekt anhand jeder nachfolgenden Regel in der Richtlinie ausgewertet, bis eine Übereinstimmung gefunden wird.
3. Wenn keine Regeln mit einem Objekt übereinstimmen, werden das Aufnahmeverhalten und die Platzierungsanweisungen für die Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie und kann keine Filter verwenden. Es muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

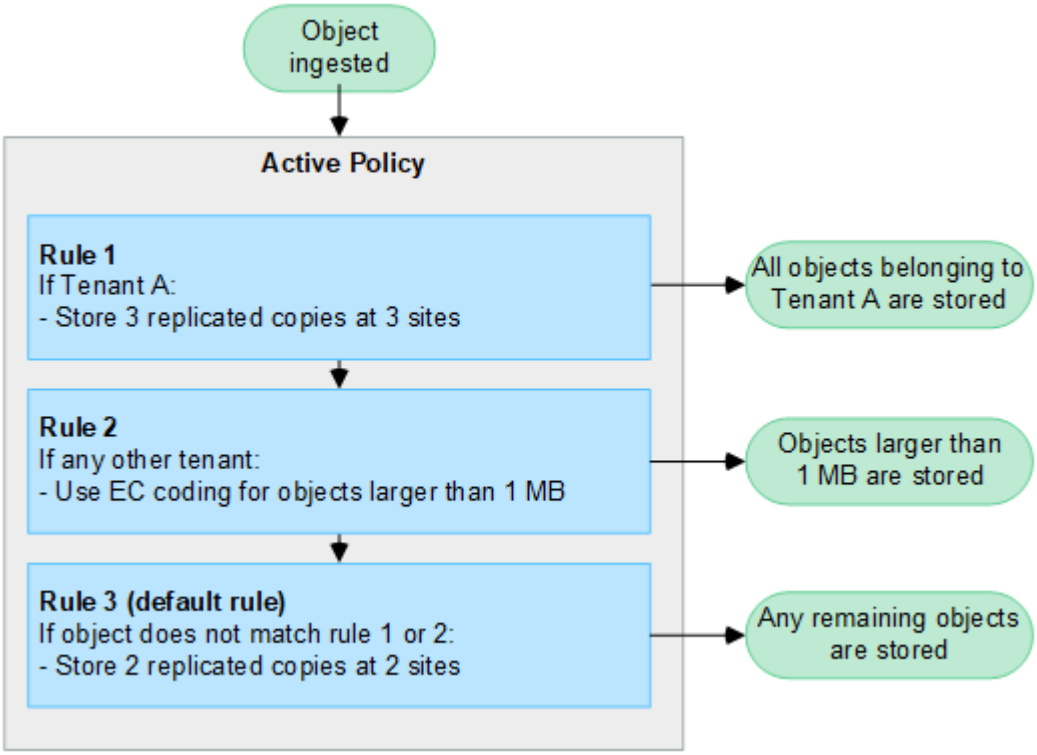
Beispiel einer ILM-Richtlinie

Beispielsweise könnte eine ILM-Richtlinie drei ILM-Regeln enthalten, die Folgendes festlegen:

- **Regel 1: Replikate für Mieter A**
  - Alle Objekte abgleichen, die zu Mieter A gehören.
  - Speichern Sie diese Objekte als drei replizierte Kopien an drei Standorten.
  - Objekte, die anderen Mandanten gehören, werden nicht mit Regel 1 abgeglichen, daher werden sie anhand von Regel 2 ausgewertet.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
  - Alle Objekte anderer Mandanten werden abgeglichen, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mittels 6+3-Erasure-Coding an drei Standorten gespeichert.

- Stimmt nicht mit Objekten überein, die 1 MB oder kleiner sind. Daher werden diese Objekte anhand von Regel 3 ausgewertet.

- **Regel 3: 2 Kopien, 2 Rechenzentren** (Standard)
  - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
  - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und 1 MB oder kleiner sind).



Ähnliche Informationen

- "Objekte mit ILM verwalten"

Entdecken Sie StorageGRID

Entdecken Sie den Grid Manager

Der Grid Manager ist die browserbasierte grafische Benutzeroberfläche, mit der Sie Ihr StorageGRID -System konfigurieren, verwalten und überwachen können.

> Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispiel-Screenshots auf dieser Seite überein.

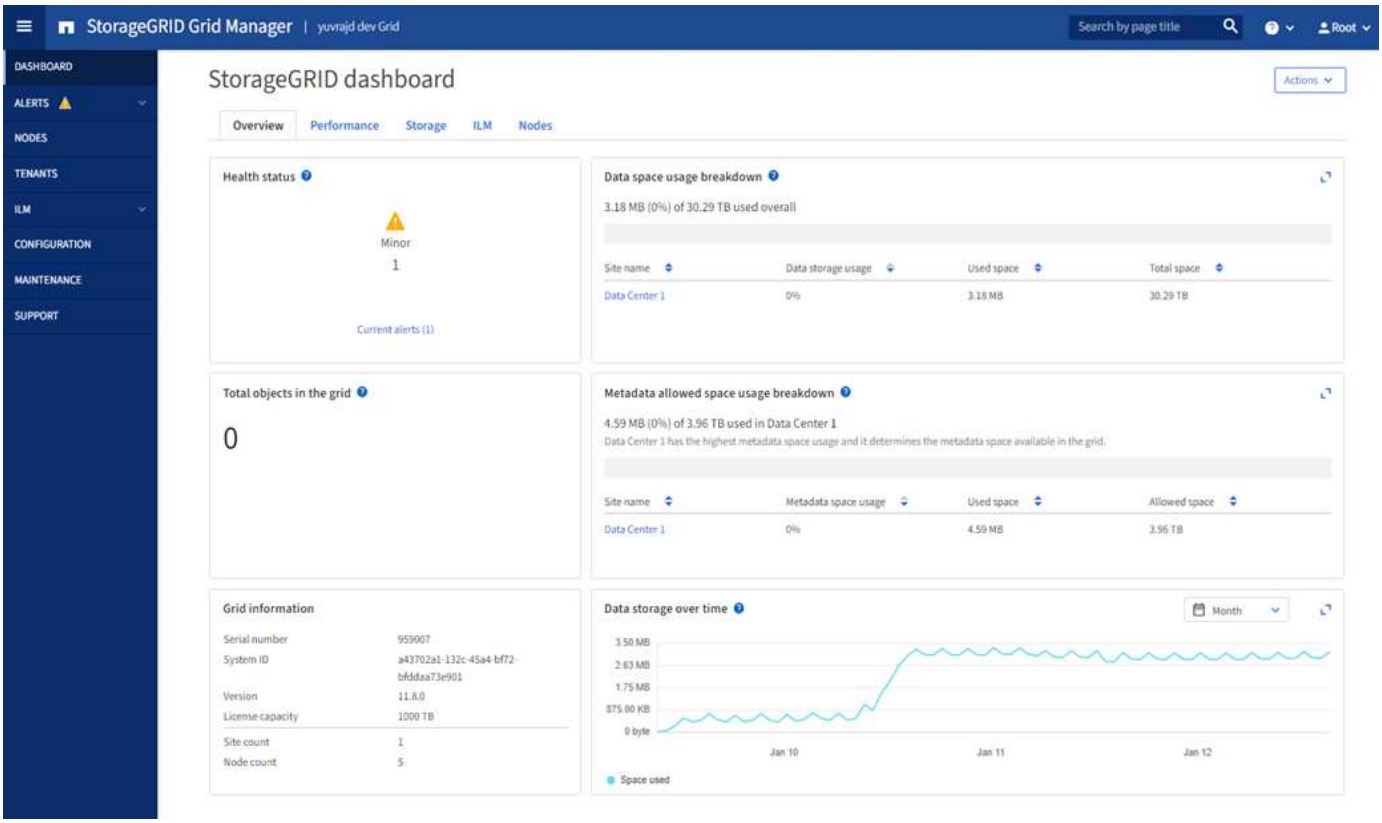
Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her. Jedes StorageGRID -System umfasst einen primären Admin-Knoten und eine beliebige Anzahl nicht-primärer Admin-Knoten. Sie können eine Verbindung zu jedem Admin-Knoten herstellen und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID Systems an.

Sie können auf den Grid Manager zugreifen, indem Sie"unterstützter Webbrowser" .

Grid Manager-Dashboard

Wenn Sie sich zum ersten Mal beim Grid Manager anmelden, können Sie das Dashboard verwenden, um"Systemaktivitäten überwachen" auf einen Blick.

Das Dashboard enthält Informationen zu Systemzustand und -leistung, Speichernutzung, ILM-Prozessen, S3-Vorgängen und den Knoten im Grid. Du kannst"Konfigurieren Sie das Dashboard" indem Sie aus einer Sammlung von Karten auswählen, die die Informationen enthalten, die Sie zur effektiven Überwachung Ihres Systems benötigen.



Für eine Erklärung der auf jeder Karte angezeigten Informationen wählen Sie das Hilfesymbol für diese Karte.

Suchfeld

Über das Feld **Suchen** in der Kopfzeile können Sie schnell zu einer bestimmten Seite im Grid Manager navigieren. Sie können beispielsweise **km** eingeben, um auf die Seite des Schlüsselverwaltungsservers (KMS) zuzugreifen.

Mit der **Suche** können Sie Einträge in der Seitenleiste des Grid Managers und in den Menüs „Konfiguration“, „Wartung“ und „Support“ finden. Sie können auch nach Namen nach Elementen wie Grid-Knoten und Mandantenkonten suchen.

Hilfemenü

Das Hilfemenü bietet Zugriff auf:

- Der"FabricPool" Und"S3-Einrichtung" Zauberer
- Das StorageGRID Dokumentationszentrum für die aktuelle Version
- "API-Dokumentation"

- Informationen darüber, welche Version von StorageGRID aktuell installiert ist

Menü „Benachrichtigungen“

Das Menü „Warnungen“ bietet eine benutzerfreundliche Oberfläche zum Erkennen, Auswerten und Beheben von Problemen, die während des StorageGRID -Betriebs auftreten können.

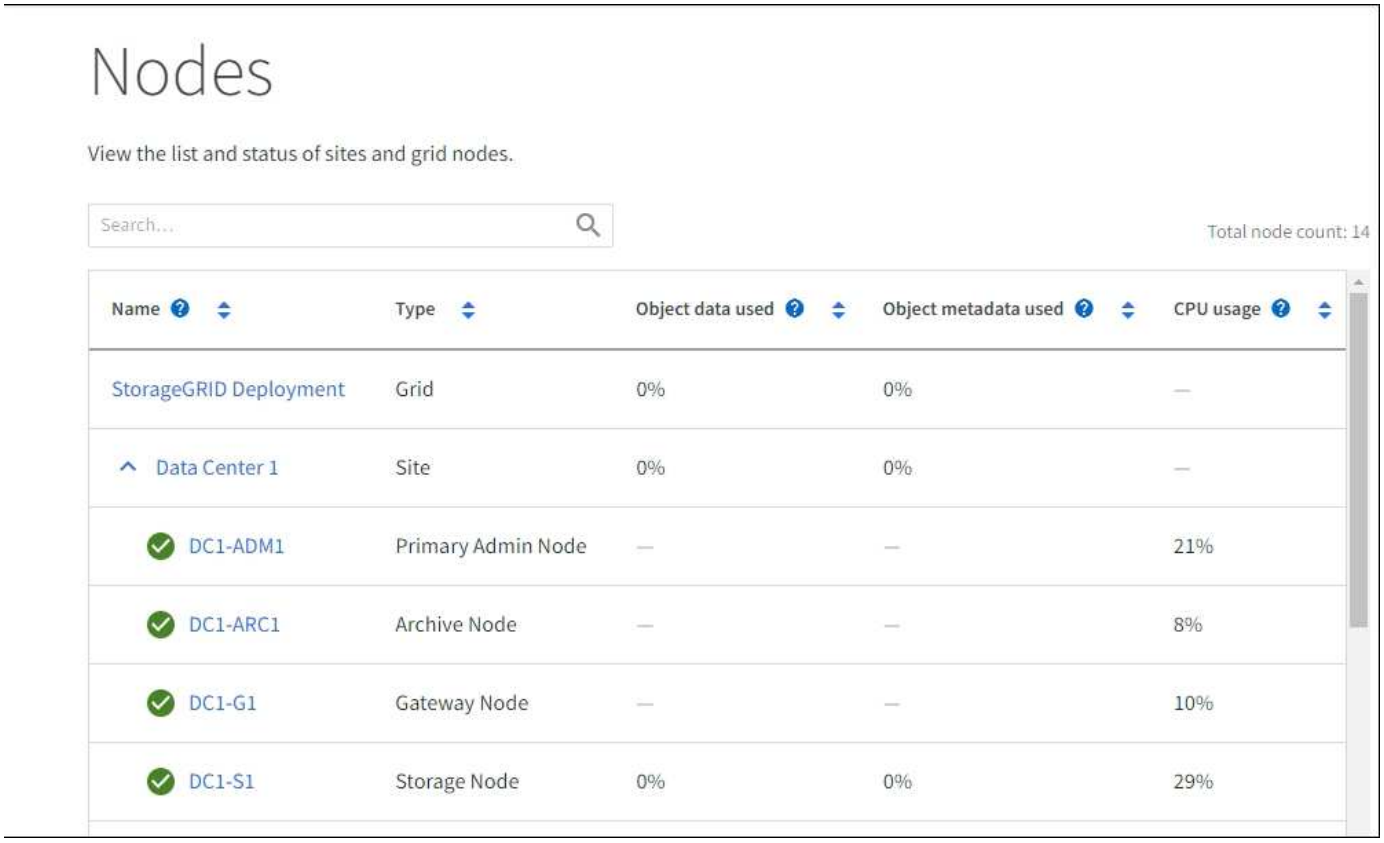
Im Menü „Alarme“ können Sie Folgendes tun:"Benachrichtigungen verwalten" :

- Aktuelle Warnungen überprüfen
- Überprüfen gelöster Warnungen
- Konfigurieren Sie Stummschaltungen, um Warnbenachrichtigungen zu unterdrücken
- Definieren Sie Warnregeln für Bedingungen, die Warnmeldungen auslösen
- Konfigurieren Sie den E-Mail-Server für Warnbenachrichtigungen

Knotenseite

Der"Knotenseite" zeigt Informationen zum gesamten Raster, zu jedem Standort im Raster und zu jedem Knoten an einem Standort an.

Auf der Nodes-Startseite werden kombinierte Metriken für das gesamte Raster angezeigt. Um Informationen zu einer bestimmten Site oder einem bestimmten Knoten anzuzeigen, wählen Sie die Site oder den Knoten aus.

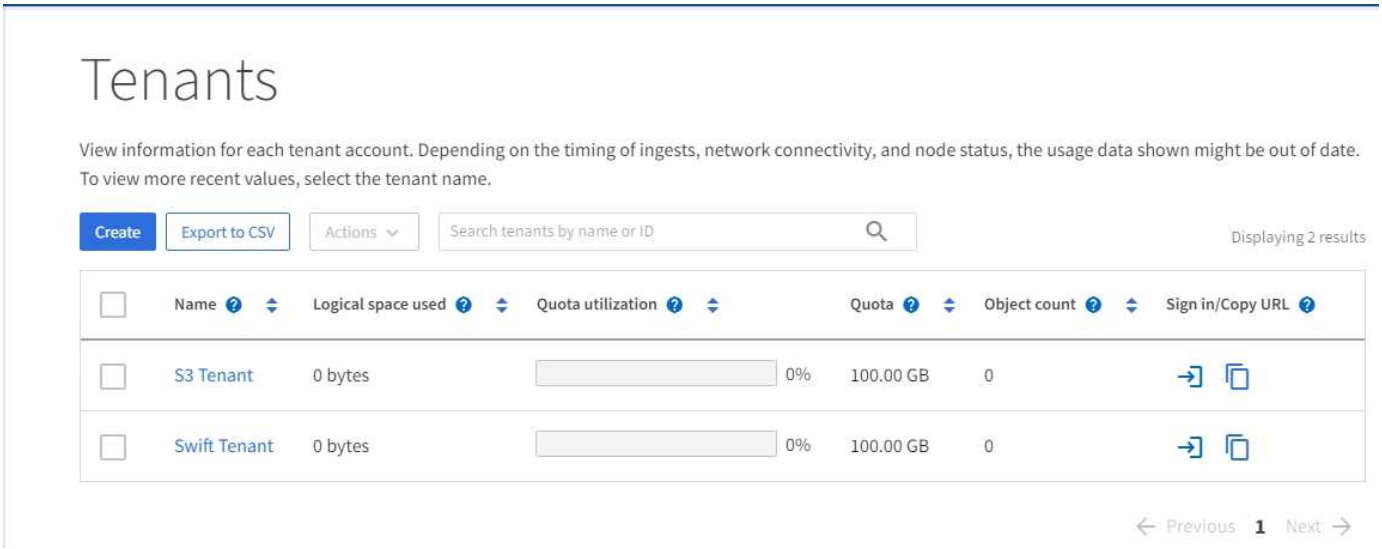


Mieterseite

Der"Mieterseite" ermöglicht es Ihnen,"Erstellen und Überwachen der Speichermandantenkonten" für Ihr StorageGRID System. Sie müssen mindestens ein Mandantenkonto erstellen, um festzulegen, wer Objekte

speichern und abrufen kann und welche Funktionen ihm zur Verfügung stehen.

Auf der Seite „Mandanten“ werden auch Nutzungsdetails für jeden Mandanten bereitgestellt, einschließlich der Menge des verwendeten Speichers und der Anzahl der Objekte. Wenn Sie beim Erstellen des Mandanten ein Kontingent festgelegt haben, können Sie sehen, wie viel von diesem Kontingent verwendet wurde.



ILM-Menü

Der"ILM-Menü" ermöglicht es Ihnen,"Konfigurieren Sie die Regeln und Richtlinien für das Information Lifecycle Management (ILM)." die die Haltbarkeit und Verfügbarkeit der Daten regeln. Sie können auch eine Objektkennung eingeben, um die Metadaten für dieses Objekt anzuzeigen.

Über das ILM-Menü können Sie ILM anzeigen und verwalten:

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

Konfigurationsmenü

Im Konfigurationsmenü können Sie Netzwerkeinstellungen, Sicherheitseinstellungen, Systemeinstellungen, Überwachungsoptionen und Zugriffskontrolloptionen festlegen.

Netzwerkaufgaben

Zu den Netzwerkaufgaben gehören:

- "Verwalten von Hochverfügbarkeitsgruppen"
- "Verwalten von Load Balancer-Endpunkten"
- "Konfigurieren von S3-Endpunktdomänennamen"

- "Verwalten von Richtlinien zur Verkehrsklassifizierung"
- "Konfigurieren von VLAN-Schnittstellen"

Sicherheitsaufgaben

Zu den Sicherheitsaufgaben gehören:

- "Sicherheitszertifikate verwalten"
- "Verwalten interner Firewall-Kontrollen"
- "Konfigurieren von Schlüsselverwaltungsservern"
- Konfigurieren von Sicherheitseinstellungen, einschließlich der"TLS- und SSH-Richtlinie" ,"Netzwerk- und Objektsicherheitsoptionen" , Und"Schnittstellensicherheitseinstellungen" .
- Konfigurieren der Einstellungen für eine"Speicherproxy" oder ein"Administrator-Proxy"

Systemaufgaben

Zu den Systemaufgaben gehören:

- Verwenden"Netzverbund" um Mandantenkontoinformationen zu klonen und Objektdaten zwischen zwei StorageGRID Systemen zu replizieren.
- Optional: Aktivieren Sie die"Gespeicherte Objekte komprimieren" Option.
- "Verwalten der S3-Objektsperre"
- Verstehen von Speicheroptionen wie"Objektsegmentierung" Und"Speichervolumen-Wasserzeichen" .
- "Verwalten von Erasure-Coding-Profilen" .

Überwachungsaufgaben

Zu den Überwachungsaufgaben gehören:

- "Konfigurieren von Prüfmeldungen und Protokollzielen"
- "Verwenden der SNMP-Überwachung"

Zugriffskontrollaufgaben

Zu den Aufgaben der Zugriffskontrolle gehören:

- "Verwalten von Administratorgruppen"
- "Verwalten von Administratorbenutzern"
- Ändern der"Bereitstellungspassphrase" oder"Passwörter für die Knotenkonsole"
- "Verwenden der Identitätsföderation"
- "Konfigurieren von SSO"

Wartungsmenü

Über das Wartungsmenü können Sie Wartungsaufgaben, Systemwartung und Netzwerkwartung durchführen.

Aufgaben

Zu den Wartungsaufgaben gehören:

- "Stilllegungsarbeiten"ungenutzte Netzknoten und Standorte zu entfernen
- "Expansionsvorgänge"um neue Grid-Knoten und Sites hinzuzufügen
- "Verfahren zur Wiederherstellung von Grid-Knoten"um einen ausgefallenen Knoten zu ersetzen und Daten wiederherzustellen
- "Prozeduren umbenennen"um die Anzeigenamen Ihres Rasters, Ihrer Sites und Knoten zu ändern
- "Operationen zur Objektexistenzprüfung"um die Existenz (jedoch nicht die Richtigkeit) von Objektdaten zu überprüfen
- Durchführen einer"Rollierender Neustart" um mehrere Grid-Knoten neu zu starten
- "Volume-Wiederherstellungsvorgänge"

System

Zu den Aufgaben der Systemwartung, die Sie durchführen können, gehören:

- "Anzeigen von StorageGRID -Lizenzinformationen"oder"Aktualisieren der Lizenzinformationen"
- Generieren und Herunterladen der"Wiederherstellungspaket"
- Durchführen von StorageGRID -Softwareupdates, einschließlich Software-Upgrades, Hotfixes und Updates der SANtricity OS-Software auf ausgewählten Geräten
  - "Upgrade-Verfahren"
  - "Hotfix-Verfahren"
  - "Aktualisieren Sie SANtricity OS auf SG6000-Speichercontrollern mit Grid Manager"
  - "Aktualisieren Sie SANtricity OS auf SG5700-Speichercontrollern mit Grid Manager"

Netzwerk

Zu den Aufgaben, die Sie zur Netzwerkwartung durchführen können, gehören:

- "Konfigurieren von DNS-Servern"
- "Aktualisieren von Grid-Netzwerk-Subnetzen"
- "Verwalten von NTP-Servern"

Support-Menü

Das Support-Menü bietet Optionen, die dem technischen Support bei der Analyse und Fehlerbehebung Ihres Systems helfen.

Tools

Im Abschnitt „Tools“ des Support-Menüs können Sie:

- "Konfigurieren Sie AutoSupport"
- "Diagnose ausführen"zum aktuellen Zustand des Netzes
- "Zugriff auf den Grid-Topologie-Baum"um detaillierte Informationen zu Grid-Knoten, Diensten und Attributen anzuzeigen

- "Erfassen von Protokolldateien und Systemdaten"
- "Überprüfen der Supportmetriken"

> Die über die Option **Metriken** verfügbaren Tools sind für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig.

Alarme (alt)

Die Informationen zu Legacy-Alarmen wurden aus dieser Version der Dokumentation entfernt. Siehe "Verwalten von Warnungen und Alarmen (StorageGRID 11.8-Dokumentation)" .

Sonstige

Im Abschnitt „Sonstiges“ des Support-Menüs können Sie:

- Verwalten"Linkkosten"
- Sicht"Netzwerkmanagementsystem (NMS)" Einträge
- Verwalten"Speicherwasserzeichen"

Entdecken Sie den Tenant Manager

Der"Mietermanager" ist die browserbasierte grafische Benutzeroberfläche, auf die Mandantenbenutzer zugreifen, um ihre Speicherkonten zu konfigurieren, zu verwalten und zu überwachen.

> Der Tenant Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispiel-Screenshots auf dieser Seite überein.

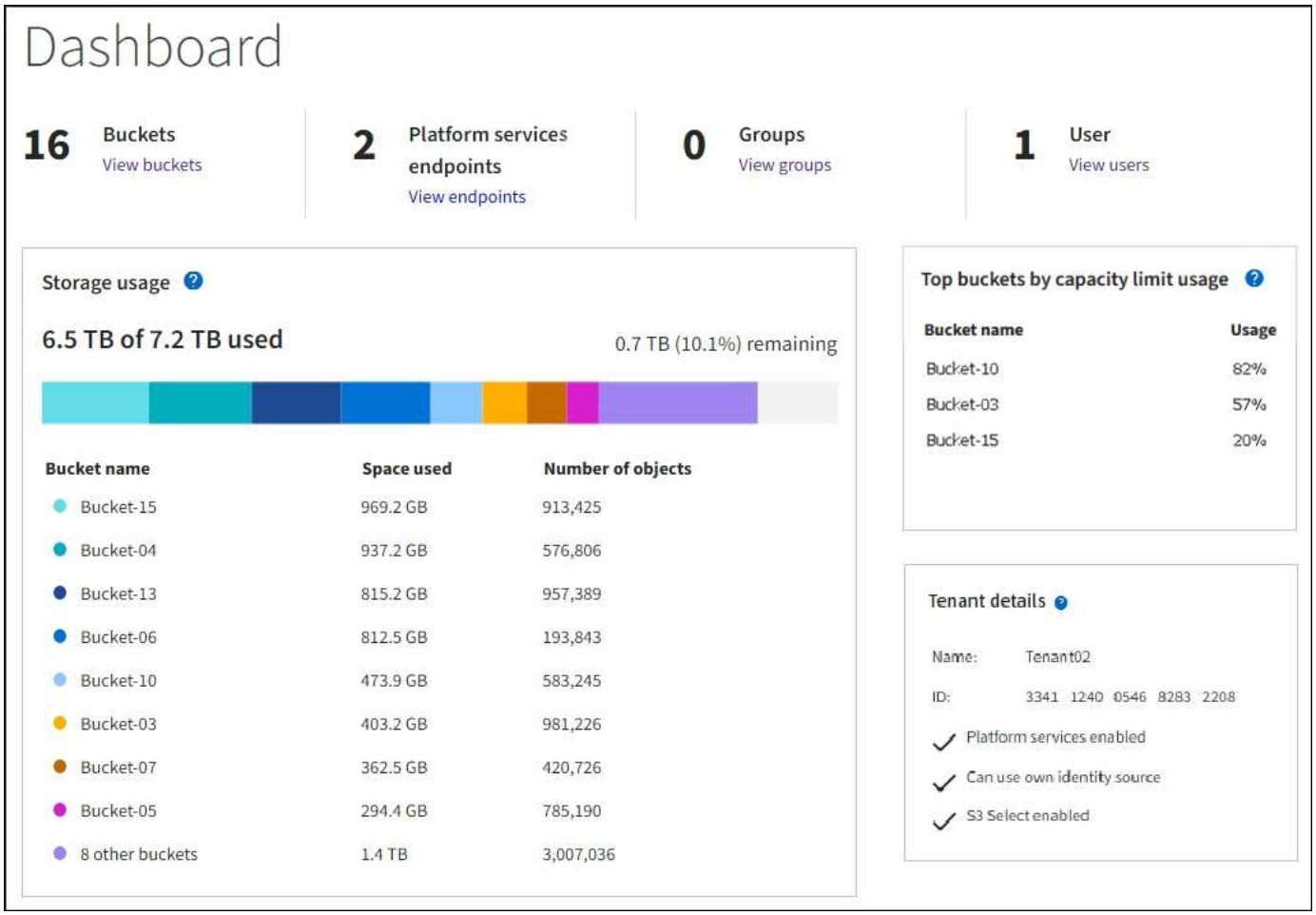
Wenn sich Mandantenbenutzer beim Mandantenmanager anmelden, stellen sie eine Verbindung zu einem Admin-Knoten her.

Mandantenmanager-Dashboard

Nachdem ein Grid-Administrator mithilfe des Grid Managers oder der Grid Management API ein Mandantenkonto erstellt hat, können sich Mandantenbenutzer beim Mandanten-Manager anmelden.

Über das Tenant Manager-Dashboard können Mandantenbenutzer die Speichernutzung auf einen Blick überwachen. Das Speichernutzungsfenster enthält eine Liste der größten Buckets (S3) oder Container (Swift) für den Mandanten. Der Wert „Benutzter Speicherplatz“ ist die Gesamtmenge der Objektdaten im Bucket oder Container. Das Balkendiagramm stellt die relativen Größen dieser Eimer oder Behälter dar.

Der über dem Balkendiagramm angezeigte Wert ist die Summe des für alle Buckets oder Container des Mandanten verwendeten Speicherplatzes. Wenn bei der Kontoerstellung die für den Mandanten maximal verfügbare Anzahl an Gigabyte, Terabyte oder Petabyte angegeben wurde, werden auch die Menge des verwendeten und verbleibenden Kontingents angezeigt.



Speichermenü (S3)

Das Speichermenü wird nur für S3-Mandantenkonten bereitgestellt. Über dieses Menü können S3-Benutzer Zugriffsschlüssel verwalten, Buckets erstellen, verwalten und löschen, Plattformdienst-Endpunkte verwalten und alle Grid-Föderationsverbindungen anzeigen, die sie verwenden dürfen.

Meine Zugriffsschlüssel

S3-Mandantenbenutzer können Zugriffsschlüssel wie folgt verwalten:

- Benutzer mit der Berechtigung „Eigene S3-Anmeldeinformationen verwalten“ können ihre eigenen S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit der Berechtigung „Root-Zugriff“ können die Zugriffsschlüssel für das S3-Root-Konto, ihr eigenes Konto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel bieten außerdem vollständigen Zugriff auf die Buckets und Objekte des Mandanten, sofern dies nicht ausdrücklich durch eine Bucket-Richtlinie deaktiviert wird.

> Die Verwaltung der Zugriffsschlüssel für andere Benutzer erfolgt über das Menü „Zugriffsverwaltung“.

Eimer

S3-Tenant-Benutzer mit den entsprechenden Berechtigungen können die folgenden Aufgaben für ihre Buckets ausführen:

- Buckets erstellen
- Aktivieren Sie S3 Object Lock für einen neuen Bucket (setzt voraus, dass S3 Object Lock für das StorageGRID -System aktiviert ist).
- Konsistenzwerte aktualisieren
- Aktivieren und Deaktivieren der Aktualisierung der letzten Zugriffszeit
- Aktivieren oder Aussetzen der Objektversionierung
- Standardaufbewahrung für S3 Object Lock aktualisieren
- Konfigurieren Sie Cross-Origin Resource Sharing (CORS)
- Alle Objekte in einem Bucket löschen
- Leere Buckets löschen
- Verwenden Sie die"S3-Konsole" zum Verwalten von Bucket-Objekten

Wenn ein Grid-Administrator die Verwendung von Plattformdiensten für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit den entsprechenden Berechtigungen auch diese Aufgaben ausführen:

- Konfigurieren Sie S3-Ereignisbenachrichtigungen, die an einen Zieldienst gesendet werden können, der den Amazon Simple Notification Service unterstützt.
- Konfigurieren Sie die CloudMirror-Replikation, die es dem Mandanten ermöglicht, Objekte automatisch in einen externen S3-Bucket zu replizieren.
- Konfigurieren Sie die Suchintegration, die Objektmetadaten an einen Zielsuchindex sendet, wenn ein Objekt erstellt oder gelöscht wird oder seine Metadaten oder Tags aktualisiert werden.

Plattformdienst-Endpunkte

Wenn ein Grid-Administrator die Verwendung von Plattformdiensten für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit der Berechtigung „Endpunkte verwalten“ für jeden Plattformdienst einen Zielendpunkt konfigurieren.

Grid-Föderation-Verbindungen

Wenn ein Grid-Administrator die Verwendung einer Grid-Föderationsverbindung für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit Root-Zugriffsberechtigung den Verbindungsnamen anzeigen, auf die Bucket-Detailseite für jeden Bucket zugreifen, für den die Cross-Grid-Replikation aktiviert ist, und den letzten Fehler anzeigen, der aufgetreten ist, als Bucket-Daten in das andere Grid in der Verbindung repliziert wurden. Sehen "Grid-Föderation-Verbindungen anzeigen" .

Menü „Zugriffsverwaltung“

Über das Menü „Zugriffsverwaltung“ können StorageGRID Mandanten Benutzergruppen aus einer föderierten Identitätsquelle importieren und Verwaltungsberechtigungen zuweisen. Mandanten können auch lokale Mandantengruppen und Benutzer verwalten, sofern nicht Single Sign-On (SSO) für das gesamte StorageGRID System aktiviert ist.

Netzwerkrichtlinien

Netzwerkrichtlinien

Verwenden Sie diese Richtlinien, um mehr über die Architektur und Netzwerktopologien

von StorageGRID zu erfahren und die Anforderungen für die Netzwerkkonfiguration und -bereitstellung kennenzulernen.

Zu dieser Anleitung

Diese Richtlinien enthalten Informationen, die Sie zum Erstellen der StorageGRID Netzwerkinfrastruktur verwenden können, bevor Sie StorageGRID -Knoten bereitstellen und konfigurieren. Verwenden Sie diese Richtlinien, um sicherzustellen, dass die Kommunikation zwischen allen Knoten im Grid und zwischen dem Grid und externen Clients und Diensten stattfinden kann.

Externe Clients und externe Dienste müssen eine Verbindung zu StorageGRID -Netzwerken herstellen, um Funktionen wie die folgenden auszuführen:

- Speichern und Abrufen von Objektdaten
- Erhalten Sie E-Mail-Benachrichtigungen
- Greifen Sie auf die StorageGRID -Verwaltungsschnittstelle (Grid Manager und Tenant Manager) zu.
- Zugriff auf die Audit-Freigabe (optional)
- Bieten Sie Dienstleistungen an wie:
  - Netzwerkzeitprotokoll (NTP)
  - Domänennamensystem (DNS)
  - Schlüsselverwaltungsserver (KMS)

Das StorageGRID -Netzwerk muss entsprechend konfiguriert werden, um den Datenverkehr für diese und weitere Funktionen zu bewältigen.

Bevor Sie beginnen

Die Netzwerkkonfiguration für ein StorageGRID -System erfordert ein hohes Maß an Erfahrung mit Ethernet-Switching, TCP/IP-Netzwerken, Subnetzen, Netzwerkrouting und Firewalls.

Machen Sie sich vor der Netzwerkkonfiguration mit der StorageGRID -Architektur vertraut, wie in"Erfahren Sie mehr über StorageGRID" .

Nachdem Sie festgelegt haben, welche StorageGRID -Netzwerke Sie verwenden möchten und wie diese Netzwerke konfiguriert werden, können Sie die StorageGRID -Knoten installieren und konfigurieren, indem Sie den entsprechenden Anweisungen folgen.

Installieren von Appliance-Knoten

- "Installieren der Appliance-Hardware"

Installieren Sie softwarebasierte Knoten

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"

Konfigurieren und Verwalten der StorageGRID -Software

- "StorageGRID verwalten"
- "Versionshinweise"

StorageGRID -Netzwerktypen

Die Grid-Knoten in einem StorageGRID -System verarbeiten *Grid-Verkehr*, *Admin-Verkehr* und *Client-Verkehr*. Sie müssen das Netzwerk entsprechend konfigurieren, um diese drei Arten von Datenverkehr zu verwalten und Kontrolle und Sicherheit zu gewährleisten.

Verkehrsarten

Verkehrsart	Beschreibung	Netzwerktyp
Netzverkehr	Der interne StorageGRID -Verkehr, der zwischen allen Knoten im Grid stattfindet. Alle Grid-Knoten müssen über dieses Netzwerk mit allen anderen Grid-Knoten kommunizieren können.	Grid-Netzwerk (erforderlich)
Admin-Verkehr	Der für die Systemadministration und -wartung verwendete Datenverkehr.	Admin-Netzwerk (optional),VLAN-Netzwerk (optional)
Client-Verkehr	Der Datenverkehr zwischen externen Clientanwendungen und dem Grid, einschließlich aller Objektspeicheranforderungen von S3-Clients.	Client-Netzwerk (optional),VLAN-Netzwerk (optional)

Sie können das Netzwerk auf folgende Arten konfigurieren:

- Nur Grid-Netzwerk
- Grid- und Admin-Netzwerke
- Grid- und Client-Netzwerke
- Grid-, Admin- und Client-Netzwerke

Das Grid-Netzwerk ist obligatorisch und kann den gesamten Grid-Verkehr verwalten. Die Admin- und Client-Netzwerke können zum Zeitpunkt der Installation einbezogen oder später hinzugefügt werden, um sich an geänderte Anforderungen anzupassen. Obwohl das Admin-Netzwerk und das Client-Netzwerk optional sind, kann das Grid-Netzwerk isoliert und sicher gemacht werden, wenn Sie diese Netzwerke zur Abwicklung des Verwaltungs- und Client-Verkehrs verwenden.

Interne Ports sind nur über das Grid-Netzwerk zugänglich. Externe Ports sind von allen Netzwerktypen aus zugänglich. Diese Flexibilität bietet mehrere Optionen für die Gestaltung einer StorageGRID -Bereitstellung und die Einrichtung externer IP- und Portfilter in Switches und Firewalls. Sehen"interne Grid-Knoten-Kommunikation" Und"Externe Kommunikation" .

Netzwerkschnittstellen

StorageGRID -Knoten sind über die folgenden spezifischen Schnittstellen mit jedem Netzwerk verbunden:

Netzwerk	Schnittstellenname
Grid-Netzwerk (erforderlich)	eth0

Netzwerk	Schnittstellenname
Admin-Netzwerk (optional)	eth1
Client-Netzwerk (optional)	eth2

Einzelheiten zum Zuordnen virtueller oder physischer Ports zu Knotennetzwerkschnittstellen finden Sie in den Installationsanweisungen:

Softwarebasierte Knoten

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"

Appliance-Knoten

- "SG6160 Speichergerät"
- "SGF6112 Speichergerät"
- "SG6000-Speichergerät"
- "SG5800 Speichergerät"
- "SG5700 Speichergerät"
- "SG110 und SG1100 Servicegeräte"
- "SG100 und SG1000 Servicegeräte"

Netzwerkinformationen für jeden Knoten

Sie müssen für jedes Netzwerk, das Sie auf einem Knoten aktivieren, Folgendes konfigurieren:

- IP-Adresse
- Subnetzmaske
- Gateway-IP-Adresse

Sie können für jedes der drei Netzwerke auf jedem Grid-Knoten nur eine IP-Adresse/Maske/Gateway-Kombination konfigurieren. Wenn Sie kein Gateway für ein Netzwerk konfigurieren möchten, sollten Sie die IP-Adresse als Gateway-Adresse verwenden.

Hochverfügbarkeitsgruppen

Hochverfügbarkeitsgruppen (HA) bieten die Möglichkeit, virtuelle IP-Adressen (VIP) zur Grid- oder Client-Netzwerkschnittstelle hinzuzufügen. Weitere Informationen finden Sie unter "Verwalten von Hochverfügbarkeitsgruppen" .

Netznetzwerk

Das Grid-Netzwerk ist erforderlich. Es wird für den gesamten internen StorageGRID Verkehr verwendet. Das Grid-Netzwerk bietet Konnektivität zwischen allen Knoten im Grid, über alle Standorte und Subnetze hinweg. Alle Knoten im Grid-Netzwerk müssen mit allen anderen Knoten kommunizieren können. Das Grid-Netzwerk kann aus mehreren Subnetzen bestehen. Netzwerke, die kritische Grid-Dienste wie NTP enthalten, können auch als Grid-Subnetze hinzugefügt werden.

StorageGRID unterstützt keine Netzwerkadressübersetzung (NAT) zwischen Knoten.

Das Grid-Netzwerk kann für den gesamten Admin-Verkehr und den gesamten Client-Verkehr verwendet werden, auch wenn das Admin-Netzwerk und das Client-Netzwerk konfiguriert sind. Das Grid-Netzwerk-Gateway ist das Standard-Gateway des Knotens, sofern für den Knoten nicht das Client-Netzwerk konfiguriert ist.

Beim Konfigurieren des Grid-Netzwerks müssen Sie sicherstellen, dass das Netzwerk vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt ist.

Beachten Sie die folgenden Anforderungen und Details für das Grid Network Gateway:

- Das Grid-Netzwerk-Gateway muss konfiguriert werden, wenn mehrere Grid-Subnetze vorhanden sind.
- Das Grid-Netzwerk-Gateway ist das Standard-Gateway des Knotens, bis die Grid-Konfiguration abgeschlossen ist.
- Statische Routen werden automatisch für alle Knoten zu allen in der globalen Grid-Netzwerk-Subnetzliste konfigurierten Subnetzen generiert.
- Wenn ein Client-Netzwerk hinzugefügt wird, wechselt das Standard-Gateway vom Grid-Netzwerk-Gateway zum Client-Netzwerk-Gateway, wenn die Grid-Konfiguration abgeschlossen ist.

Admin-Netzwerk

Das Admin-Netzwerk ist optional. Nach der Konfiguration kann es für den Systemadministrations- und Wartungsverkehr verwendet werden. Das Admin-Netzwerk ist normalerweise ein privates Netzwerk und muss nicht zwischen Knoten geroutet werden können.

Sie können auswählen, für welche Grid-Knoten das Admin-Netzwerk aktiviert werden soll.

Wenn Sie das Admin-Netzwerk verwenden, muss der Verwaltungs- und Wartungsverkehr nicht über das Grid-Netzwerk laufen. Typische Verwendungszwecke des Admin-Netzwerks sind unter anderem:

- Zugriff auf die Benutzeroberflächen von Grid Manager und Tenant Manager.
- Zugriff auf kritische Dienste wie NTP-Server, DNS-Server, externe Schlüsselverwaltungsserver (KMS) und Lightweight Directory Access Protocol (LDAP)-Server.
- Zugriff auf Prüfprotokolle auf Admin-Knoten.
- Secure Shell Protocol (SSH)-Zugriff für Wartung und Support.

Das Admin-Netzwerk wird niemals für internen Grid-Verkehr verwendet. Es wird ein Admin-Netzwerk-Gateway bereitgestellt, das dem Admin-Netzwerk die Kommunikation mit mehreren externen Subnetzen ermöglicht. Das Admin-Netzwerk-Gateway wird jedoch nie als Standard-Gateway des Knotens verwendet.

Beachten Sie die folgenden Anforderungen und Details für das Admin-Netzwerk-Gateway:

- Das Admin-Netzwerk-Gateway ist erforderlich, wenn Verbindungen von außerhalb des Admin-Netzwerk-Subnetzes hergestellt werden oder wenn mehrere Admin-Netzwerk-Subnetze konfiguriert sind.
- Für jedes in der Admin-Netzwerk-Subnetzliste des Knotens konfigurierte Subnetz werden statische Routen erstellt.

Kundennetzwerk

Das Client-Netzwerk ist optional. Wenn es konfiguriert ist, wird es verwendet, um Clientanwendungen wie S3 Zugriff auf Grid-Dienste zu gewähren. Wenn Sie StorageGRID Daten einer externen Ressource zugänglich machen möchten (z. B. einem Cloud Storage Pool oder dem StorageGRID CloudMirror-Replikationsdienst), kann die externe Ressource auch das Client-Netzwerk verwenden. Grid-Knoten können mit jedem Subnetz kommunizieren, das über das Client-Netzwerk-Gateway erreichbar ist.

Sie können auswählen, auf welchen Grid-Knoten das Client-Netzwerk aktiviert werden soll. Es müssen sich nicht alle Knoten im selben Client-Netzwerk befinden und die Knoten kommunizieren niemals über das Client-Netzwerk miteinander. Das Client-Netzwerk ist erst betriebsbereit, wenn die Grid-Installation abgeschlossen ist.

Zur Erhöhung der Sicherheit können Sie festlegen, dass die Client-Netzwerkschnittstelle eines Knotens nicht vertrauenswürdig ist, sodass das Client-Netzwerk hinsichtlich der zulässigen Verbindungen restriktiver ist. Wenn die Client-Netzwerkschnittstelle eines Knotens nicht vertrauenswürdig ist, akzeptiert die Schnittstelle ausgehende Verbindungen, wie sie beispielsweise von der CloudMirror-Replikation verwendet werden, akzeptiert jedoch nur eingehende Verbindungen auf Ports, die explizit als Endpunkte des Lastenausgleichs konfiguriert wurden. Sehen"Verwalten von Firewall-Steuerelementen" Und"Konfigurieren von Load Balancer-Endpunkten" .

Wenn Sie ein Client-Netzwerk verwenden, muss der Client-Verkehr nicht über das Grid-Netzwerk laufen. Der Grid-Netzwerkverkehr kann auf ein sicheres, nicht routingfähiges Netzwerk aufgeteilt werden. Die folgenden Knotentypen werden häufig mit einem Client-Netzwerk konfiguriert:

- Gateway-Knoten, da diese Knoten Zugriff auf den StorageGRID Load Balancer-Dienst und S3-Client-Zugriff auf das Grid bieten.
- Speicherknoten, da diese Knoten Zugriff auf das S3-Protokoll sowie auf Cloud-Speicherpools und den CloudMirror-Replikationsdienst bieten.
- Admin-Knoten, um sicherzustellen, dass Mandantenbenutzer eine Verbindung zum Mandantenmanager herstellen können, ohne das Admin-Netzwerk verwenden zu müssen.

Beachten Sie Folgendes für das Client-Netzwerk-Gateway:

- Das Client-Netzwerk-Gateway ist erforderlich, wenn das Client-Netzwerk konfiguriert ist.
- Das Client-Netzwerk-Gateway wird zur Standardroute für den Grid-Knoten, wenn die Grid-Konfiguration abgeschlossen ist.

Optionale VLAN-Netzwerke

Bei Bedarf können Sie optional virtuelle LAN-Netzwerke (VLAN) für den Client-Verkehr und für einige Arten von Admin-Verkehr verwenden. Grid-Verkehr kann jedoch keine VLAN-Schnittstelle verwenden. Der interne StorageGRID Verkehr zwischen Knoten muss immer das Grid-Netzwerk auf eth0 verwenden.

Um die Verwendung von VLANs zu unterstützen, müssen Sie eine oder mehrere Schnittstellen auf einem Knoten als Trunk-Schnittstellen am Switch konfigurieren. Sie können die Grid-Netzwerkschnittstelle (eth0) oder die Client-Netzwerkschnittstelle (eth2) als Trunk konfigurieren oder dem Knoten Trunk-Schnittstellen hinzufügen.

Wenn eth0 als Trunk konfiguriert ist, fließt der Grid-Netzwerkverkehr über die native Trunk-Schnittstelle, wie auf dem Switch konfiguriert. Wenn eth2 als Trunk konfiguriert ist und das Client-Netzwerk ebenfalls auf demselben Knoten konfiguriert ist, verwendet das Client-Netzwerk das native VLAN des Trunk-Ports, wie es auf dem Switch konfiguriert ist.

Über VLAN-Netzwerke wird nur eingehender Administratorverkehr unterstützt, wie er beispielsweise für SSH-, Grid Manager- oder Tenant Manager-Verkehr verwendet wird. Ausgehender Datenverkehr, wie er beispielsweise für NTP, DNS, LDAP, KMS und Cloud Storage Pools verwendet wird, wird über VLAN-Netzwerke nicht unterstützt.

> ⓘ VLAN-Schnittstellen können nur zu Admin-Knoten und Gateway-Knoten hinzugefügt werden. Sie können keine VLAN-Schnittstelle für den Client- oder Administratorzugriff auf Speicherknoten verwenden.

Sehen"Konfigurieren von VLAN-Schnittstellen" für Anweisungen und Richtlinien.

VLAN-Schnittstellen werden nur in HA-Gruppen verwendet und erhalten VIP-Adressen auf dem aktiven Knoten. Sehen"Verwalten von Hochverfügbarkeitsgruppen" für Anweisungen und Richtlinien.

Beispiele für Netzwerktopologien

Grid-Netzwerktopologie

Die einfachste Netzwerktopologie wird erstellt, indem nur das Grid-Netzwerk konfiguriert wird.

Wenn Sie das Grid-Netzwerk konfigurieren, legen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle für jeden Grid-Knoten fest.

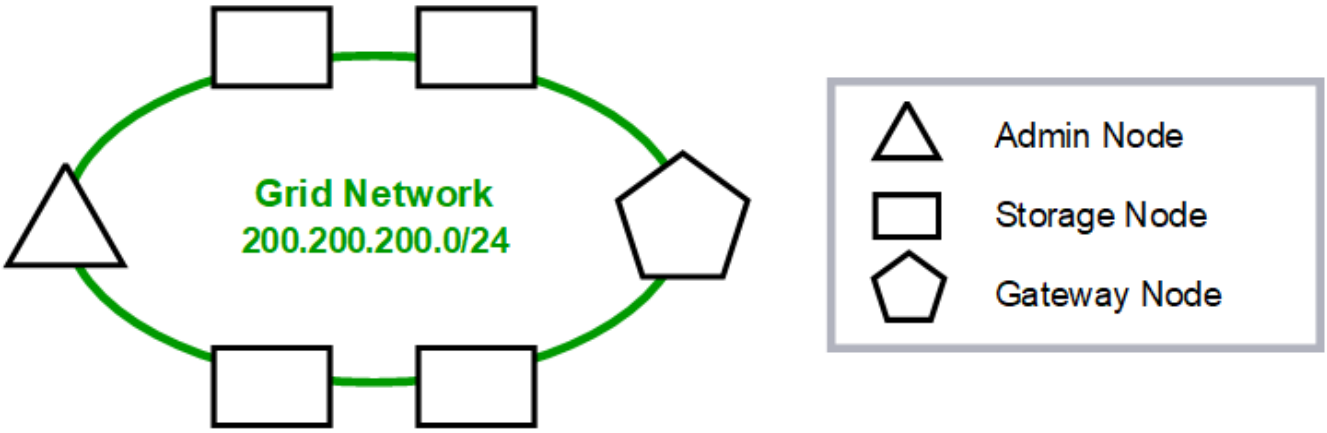
Während der Konfiguration müssen Sie alle Grid Network-Subnetze zur Grid Network Subnet List (GNSL) hinzufügen. Diese Liste enthält alle Subnetze für alle Sites und kann auch externe Subnetze enthalten, die Zugriff auf kritische Dienste wie NTP, DNS oder LDAP bieten.

Bei der Installation wendet die Grid Network-Schnittstelle statische Routen für alle Subnetze im GNSL an und legt die Standardroute des Knotens zum Grid Network-Gateway fest, sofern eines konfiguriert ist. Das GNSL ist nicht erforderlich, wenn kein Client-Netzwerk vorhanden ist und das Grid-Netzwerk-Gateway die Standardroute des Knotens ist. Außerdem werden Hostrouten zu allen anderen Knoten im Grid generiert.

In diesem Beispiel wird der gesamte Datenverkehr über dasselbe Netzwerk abgewickelt, einschließlich des Datenverkehrs im Zusammenhang mit S3-Clientanforderungen sowie Verwaltungs- und Wartungsfunktionen.

> ⓘ Diese Topologie eignet sich für Einzelstandortbereitstellungen, die nicht extern verfügbar sind, für Proof-of-Concept- oder Testbereitstellungen oder wenn ein Lastenausgleich eines Drittanbieters als Clientzugriffsgrenze fungiert. Wenn möglich, sollte das Grid-Netzwerk ausschließlich für den internen Verkehr verwendet werden. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk unterliegen zusätzlichen Firewall-Einschränkungen, die den externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Verkehr wird unterstützt, diese Verwendung bietet jedoch weniger Schutzebenen.

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

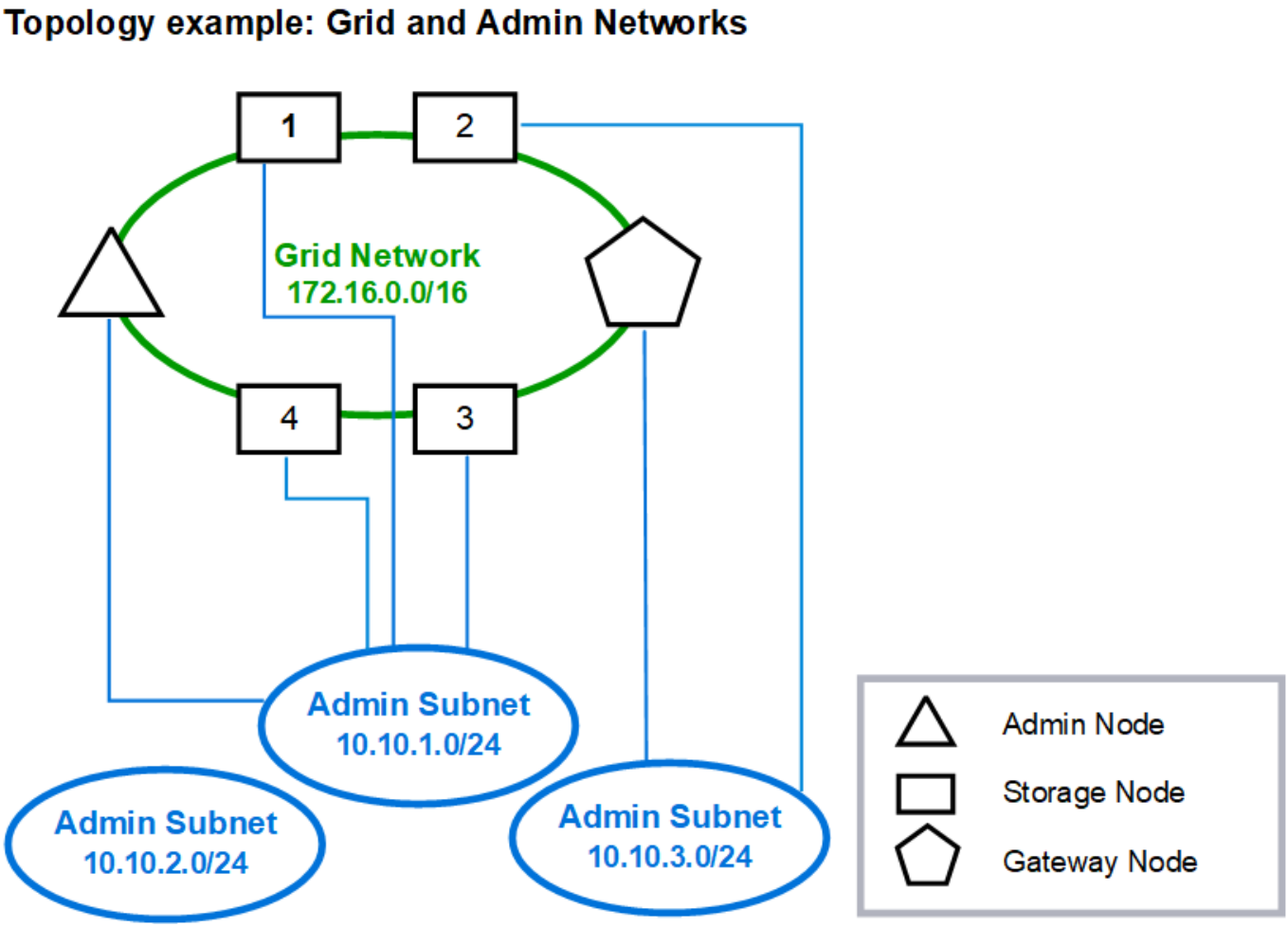
Admin-Netzwerktopologie

Ein Admin-Netzwerk ist optional. Eine Möglichkeit, ein Admin-Netzwerk und ein Grid-Netzwerk zu verwenden, besteht darin, für jeden Knoten ein routingfähiges Grid-Netzwerk und ein begrenztes Admin-Netzwerk zu konfigurieren.

Wenn Sie das Admin-Netzwerk konfigurieren, legen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth1-Schnittstelle für jeden Grid-Knoten fest.

Das Admin-Netzwerk kann für jeden Knoten eindeutig sein und aus mehreren Subnetzen bestehen. Jeder Knoten kann mit einer Admin External Subnet List (AESL) konfiguriert werden. Die AESL listet die über das Admin-Netzwerk erreichbaren Subnetze für jeden Knoten auf. Die AESL muss auch die Subnetze aller Dienste enthalten, auf die das Grid über das Admin-Netzwerk zugreift, z. B. NTP, DNS, KMS und LDAP. Für jedes Subnetz in der AESL werden statische Routen angewendet.

In diesem Beispiel wird das Grid-Netzwerk für den Datenverkehr im Zusammenhang mit S3-Clientanforderungen und Objektverwaltung verwendet, während das Admin-Netzwerk für Verwaltungsfunktionen verwendet wird.



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

Client-Netzwerktopologie

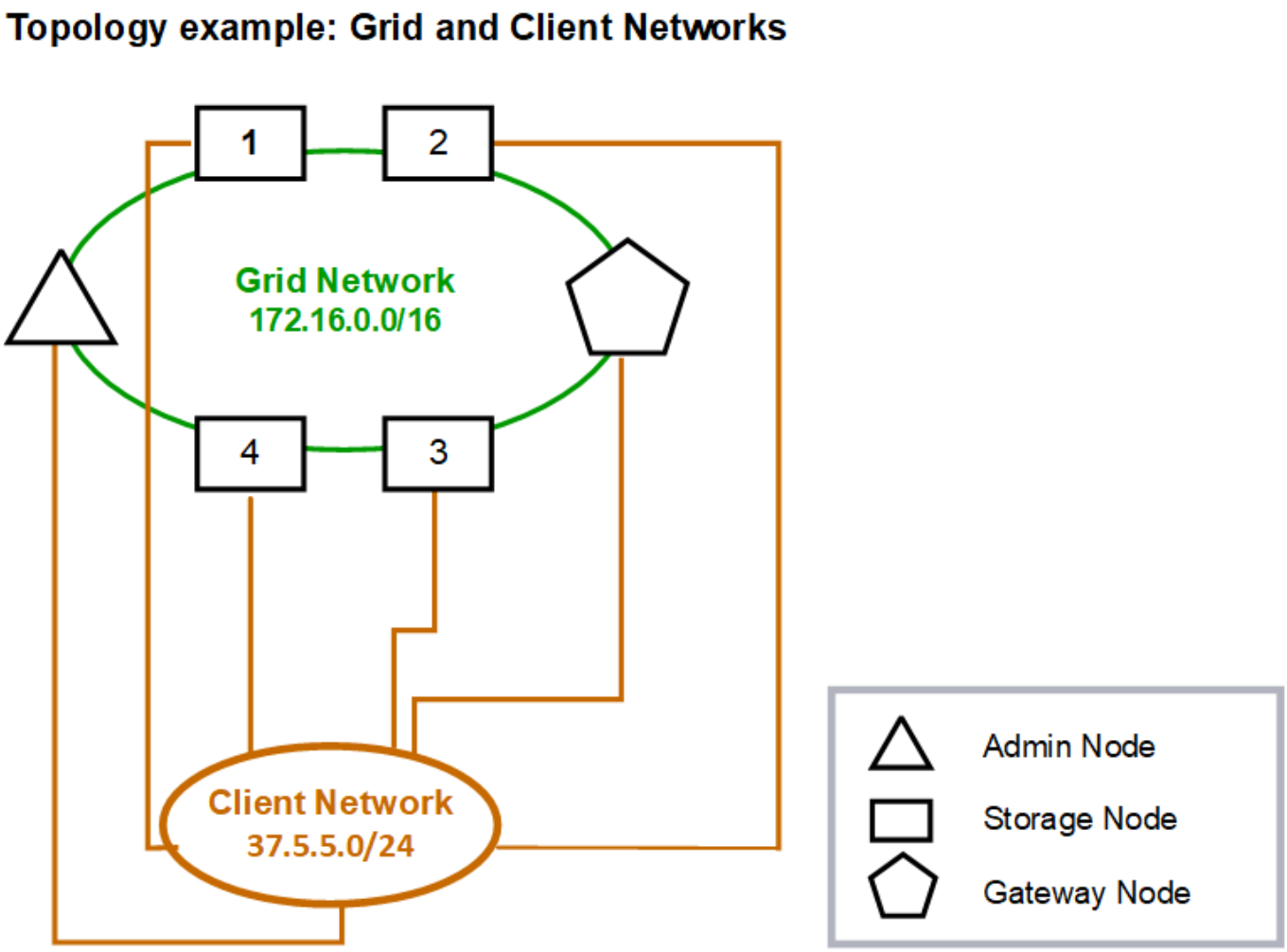
Ein Client-Netzwerk ist optional. Durch die Verwendung eines Client-Netzwerks kann der Client-Netzwerkverkehr (z. B. S3) vom internen Grid-Verkehr getrennt werden, wodurch die Grid-Vernetzung sicherer wird. Der Verwaltungsverkehr kann entweder vom Client- oder vom Grid-Netzwerk abgewickelt werden, wenn das Admin-Netzwerk nicht konfiguriert ist.

Wenn Sie das Client-Netzwerk konfigurieren, legen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth2-Schnittstelle für den konfigurierten Knoten fest. Das Client-Netzwerk jedes Knotens kann unabhängig vom Client-Netzwerk auf jedem anderen Knoten sein.

Wenn Sie während der Installation ein Client-Netzwerk für einen Knoten konfigurieren, wechselt das Standard-Gateway des Knotens nach Abschluss der Installation vom Grid-Netzwerk-Gateway zum Client-Netzwerk-Gateway. Wenn später ein Client-Netzwerk hinzugefügt wird, wechselt das Standard-Gateway des Knotens auf die gleiche Weise.

In diesem Beispiel wird das Client-Netzwerk für S3-Client-Anfragen und für Verwaltungsfunktionen verwendet,

während das Grid-Netzwerk für interne Objektverwaltungsvorgänge vorgesehen ist.



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

Ähnliche Informationen

"Knotennetzwerkkonfiguration ändern"

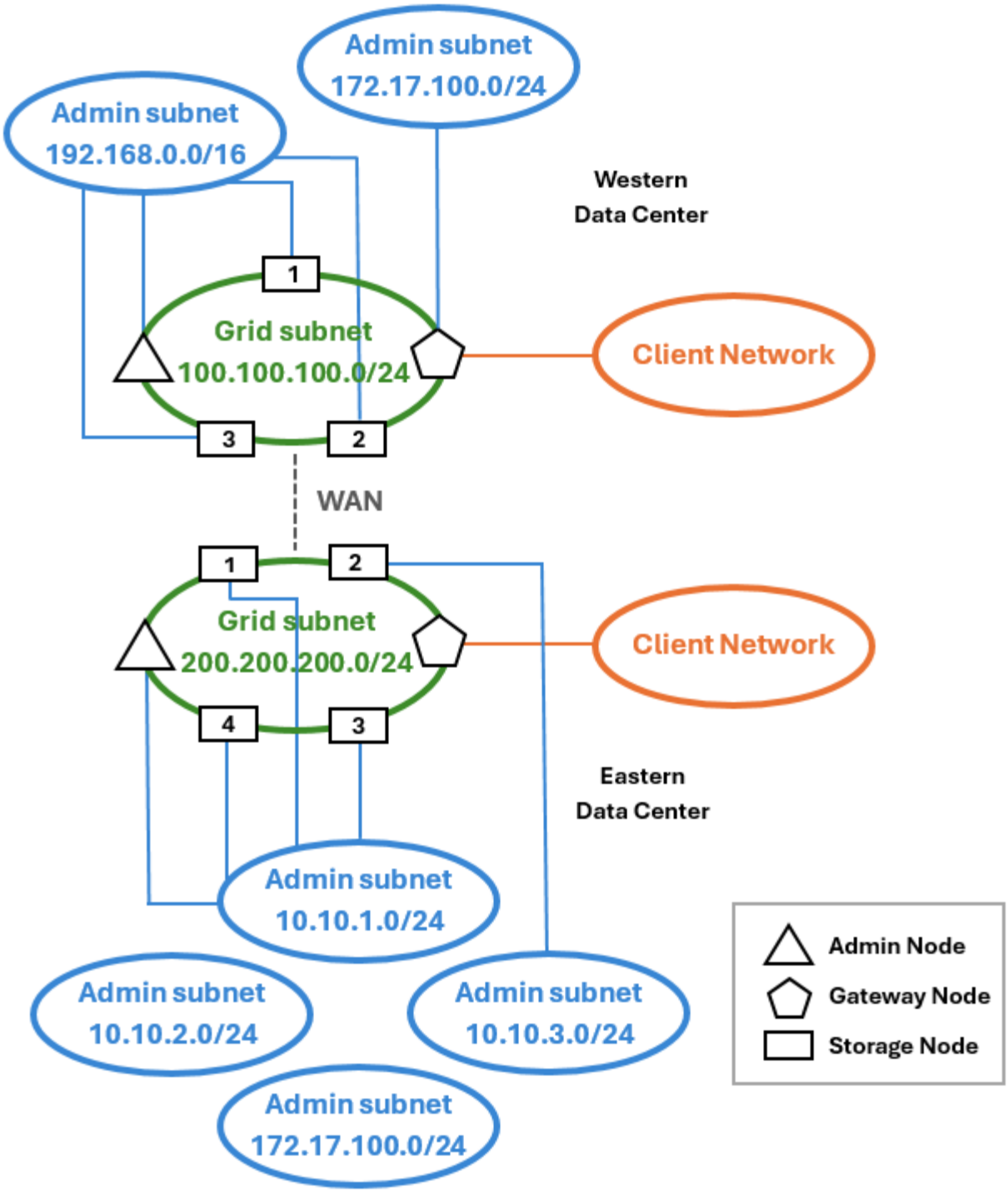
Topologie für alle drei Netzwerke

Sie können alle drei Netzwerke in einer Netzwerktopologie konfigurieren, die aus einem privaten Grid-Netzwerk, begrenzten standortspezifischen Admin-Netzwerken und offenen Client-Netzwerken besteht. Die Verwendung von Load Balancer-Endpunkten und nicht vertrauenswürdigen Client-Netzwerken kann bei Bedarf zusätzliche Sicherheit bieten.

In diesem Beispiel:

- Das Grid-Netzwerk wird für den Netzwerkverkehr im Zusammenhang mit internen Objektverwaltungsvorgängen verwendet.
- Das Admin-Netzwerk wird für den Datenverkehr im Zusammenhang mit Verwaltungsfunktionen verwendet.
- Das Client-Netzwerk wird für den Datenverkehr im Zusammenhang mit S3-Client-Anfragen verwendet.

Topologiebeispiel: Grid-, Admin- und Client-Netzwerke



Netzwerkanforderungen

Sie müssen überprüfen, ob die aktuelle Netzwerkinfrastruktur und -konfiguration das geplante StorageGRID Netzwerkdesign unterstützen kann.

Allgemeine Netzwerkanforderungen

Alle StorageGRID Bereitstellungen müssen die folgenden Verbindungen unterstützen können.

Diese Verbindungen können über das Grid-, Admin- oder Client-Netzwerk oder über Kombinationen dieser Netzwerke erfolgen, wie in den Beispielen zur Netzwerktopologie dargestellt.

- **Verwaltungsverbindungen**: Eingehende Verbindungen von einem Administrator zum Knoten, normalerweise über SSH. Webbrowser-Zugriff auf den Grid Manager, den Tenant Manager und den StorageGRID Appliance Installer.
- **NTP-Serververbindungen**: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.

  Mindestens ein NTP-Server muss vom primären Admin-Knoten aus erreichbar sein.
- **DNS-Serververbindungen**: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.
- **LDAP/Active Directory-Serververbindungen**: Ausgehende TCP-Verbindung vom Identitätsdienst auf Speicherknoten.
- * AutoSupport*: Ausgehende TCP-Verbindung von den Admin-Knoten zu entweder `support.netapp.com` oder ein vom Kunden konfigurierter Proxy.
- **Externer Schlüsselverwaltungsserver**: Ausgehende TCP-Verbindung von jedem Appliance-Knoten mit aktivierter Knotenverschlüsselung.
- Eingehende TCP-Verbindungen von S3-Clients.
- Ausgehende Anfragen von StorageGRID Plattformdiensten wie CloudMirror-Replikation oder von Cloud Storage Pools.

Wenn StorageGRID mithilfe der Standardroutingregeln keinen der bereitgestellten NTP- oder DNS-Server kontaktieren kann, versucht es automatisch, in allen Netzwerken (Grid, Admin und Client) Kontakt aufzunehmen, sofern die IP-Adressen der DNS- und NTP-Server angegeben sind. Wenn die NTP- oder DNS-Server in einem beliebigen Netzwerk erreichbar sind, erstellt StorageGRID automatisch zusätzliche Routing-Regeln, um sicherzustellen, dass dieses Netzwerk für alle zukünftigen Verbindungsversuche verwendet wird.

Obwohl Sie diese automatisch erkannten Hostrouten verwenden können, sollten Sie die DNS- und NTP-Routen im Allgemeinen manuell konfigurieren, um die Konnektivität sicherzustellen, falls die automatische Erkennung fehlschlägt.

Wenn Sie während der Bereitstellung noch nicht bereit sind, die optionalen Admin- und Client-Netzwerke zu konfigurieren, können Sie diese Netzwerke konfigurieren, wenn Sie während der Konfigurationsschritte Grid-Knoten genehmigen. Darüber hinaus können Sie diese Netzwerke nach der Installation mit dem Tool „IP ändern“ konfigurieren (siehe"Konfigurieren von IP-Adressen").

Über VLAN-Schnittstellen werden nur S3-Clientverbindungen und SSH-, Grid Manager- und Tenant Manager-Verwaltungsverbindungen unterstützt. Ausgehende Verbindungen, beispielsweise zu NTP-, DNS-, LDAP-, AutoSupport und KMS-Servern, müssen direkt über die Client-, Admin- oder Grid-Netzwerkschnittstellen erfolgen. Wenn die Schnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, fließt dieser Datenverkehr über das native VLAN der Schnittstelle, wie am Switch konfiguriert.

Wide Area Networks (WANs) für mehrere Standorte

Bei der Konfiguration eines StorageGRID -Systems mit mehreren Standorten muss die WAN-Verbindung zwischen den Standorten eine Mindestbandbreite von 25 Mbit/Sekunde in jede Richtung aufweisen, bevor der Client-Verkehr berücksichtigt wird. Für die Datenreplikation oder Erasure Coding zwischen Standorten, die Erweiterung von Knoten oder Standorten, die Wiederherstellung von Knoten und andere Vorgänge oder Konfigurationen ist zusätzliche Bandbreite erforderlich.

Die tatsächlichen Mindestanforderungen an die WAN-Bandbreite hängen von der Clientaktivität und dem ILM-Schutzschema ab. Wenn Sie Hilfe bei der Schätzung der Mindestanforderungen für die WAN-Bandbreite

benötigen, wenden Sie sich an Ihren NetApp Professional Services-Berater.

Verbindungen für Admin-Knoten und Gateway-Knoten

Admin-Knoten müssen immer vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt werden. Sie müssen sicherstellen, dass kein nicht vertrauenswürdiger Client auf einen Admin-Knoten im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk zugreifen kann.

Admin-Knoten und Gateway-Knoten, die Sie zu Hochverfügbarkeitsgruppen hinzufügen möchten, müssen mit einer statischen IP-Adresse konfiguriert werden. Weitere Informationen finden Sie unter "Verwalten von Hochverfügbarkeitsgruppen" .

Verwenden der Netzwerkadressübersetzung (NAT)

Verwenden Sie keine Netzwerkadressübersetzung (NAT) im Grid-Netzwerk zwischen Grid-Knoten oder zwischen StorageGRID Sites. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt geroutet werden können. Bei Bedarf können Sie jedoch NAT zwischen externen Clients und Grid-Knoten verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway-Knoten bereitzustellen. Die Verwendung von NAT zum Überbrücken eines öffentlichen Netzwerksegments wird nur unterstützt, wenn Sie eine Tunnelanwendung verwenden, die für alle Knoten im Grid transparent ist, d. h. die Grid-Knoten benötigen keine Kenntnis der öffentlichen IP-Adressen.

Netzwerkspezifische Anforderungen

Befolgen Sie die Anforderungen für jeden StorageGRID Netzwerktyp.

Netzwerk-Gateways und Router

- Wenn festgelegt, muss sich das Gateway für ein bestimmtes Netzwerk innerhalb des Subnetzes des jeweiligen Netzwerks befinden.
- Wenn Sie eine Schnittstelle mit statischer Adressierung konfigurieren, müssen Sie eine andere Gateway-Adresse als 0.0.0.0 angeben.
- Wenn Sie kein Gateway haben, empfiehlt es sich, die Gateway-Adresse auf die IP-Adresse der Netzwerkschnittstelle festzulegen.

Subnetze

Jedes Netzwerk muss mit seinem eigenen Subnetz verbunden sein, das sich nicht mit anderen Netzwerken auf dem Knoten überschneidet.

Die folgenden Einschränkungen werden vom Grid Manager während der Bereitstellung erzwungen. Sie werden hier bereitgestellt, um bei der Netzwerkplanung vor der Bereitstellung zu helfen.

- Die Subnetzmaske für eine Netzwerk-IP-Adresse kann nicht 255.255.255.254 oder 255.255.255.255 (/31 oder /32 in der CIDR-Notation) sein.
- Das durch die IP-Adresse und Subnetzmaske (CIDR) einer Netzwerkschnittstelle definierte Subnetz darf sich nicht mit dem Subnetz einer anderen auf demselben Knoten konfigurierten Schnittstelle überschneiden.
- Verwenden Sie keine Subnetze, die die folgenden IPv4-Adressen für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens enthalten:
  - 192.168.130.101

- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

  Verwenden Sie beispielsweise nicht die folgenden Subnetzbereiche für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens:

- 192.168.130.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.130.101 und 192.168.130.102 enthält
- 192.168.131.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.131.101 und 192.168.131.102 enthält
- 198.51.100.0/24, da dieser Subnetzbereich die IP-Adressen 198.51.100.2 und 198.51.100.4 enthält

- Das Grid-Netzwerk-Subnetz für jeden Knoten muss in der GNSL enthalten sein.
- Das Admin-Netzwerk-Subnetz darf sich nicht mit dem Grid-Netzwerk-Subnetz, dem Client-Netzwerk-Subnetz oder einem anderen Subnetz in der GNSL überschneiden.
- Die Subnetze in der AESL dürfen sich nicht mit Subnetzen in der GNSL überschneiden.
- Das Client-Netzwerk-Subnetz darf sich nicht mit dem Grid-Netzwerk-Subnetz, dem Admin-Netzwerk-Subnetz, einem anderen Subnetz in der GNSL oder einem anderen Subnetz in der AESL überschneiden.

Netznetzwerk

- Zum Zeitpunkt der Bereitstellung muss jeder Grid-Knoten an das Grid-Netzwerk angeschlossen sein und über die Netzwerkkonfiguration, die Sie bei der Bereitstellung des Knotens angeben, mit dem primären Admin-Knoten kommunizieren können.
- Während des normalen Netzbetriebs muss jeder Netzknoten in der Lage sein, über das Netznetzwerk mit allen anderen Netzknoten zu kommunizieren.

> Das Grid-Netzwerk muss zwischen den einzelnen Knoten direkt routebar sein. Die Netzwerkadressübersetzung (NAT) zwischen Knoten wird nicht unterstützt.

- Wenn das Grid-Netzwerk aus mehreren Subnetzen besteht, fügen Sie diese der Grid-Netzwerk-Subnetzliste (GNSL) hinzu. Für jedes Subnetz im GNSL werden auf allen Knoten statische Routen erstellt.
- Wenn die Grid-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, muss das native Trunk-VLAN das für den Grid-Netzwerkverkehr verwendete VLAN sein. Alle Grid-Knoten müssen über das native Trunk-VLAN zugänglich sein.

Admin-Netzwerk

Das Admin-Netzwerk ist optional. Wenn Sie ein Admin-Netzwerk konfigurieren möchten, befolgen Sie diese Anforderungen und Richtlinien.

Zu den typischen Verwendungszwecken des Admin-Netzwerks gehören Verwaltungsverbindungen, AutoSupport, KMS und Verbindungen zu kritischen Servern wie NTP, DNS und LDAP, wenn diese Verbindungen nicht über das Grid-Netzwerk oder das Client-Netzwerk bereitgestellt werden.

Das Admin-Netzwerk und die AESL können für jeden Knoten eindeutig sein, solange die gewünschten Netzwerkdienste und Clients erreichbar sind.

Sie müssen mindestens ein Subnetz im Admin-Netzwerk definieren, um eingehende Verbindungen von externen Subnetzen zu ermöglichen. Auf jedem Knoten werden für jedes Subnetz in der AESL automatisch statische Routen generiert.

Kundennetzwerk

Das Client-Netzwerk ist optional. Wenn Sie die Konfiguration eines Client-Netzwerks planen, beachten Sie die folgenden Überlegungen.

- Das Client-Netzwerk ist für die Unterstützung des Datenverkehrs von S3-Clients ausgelegt. Wenn konfiguriert, wird das Client-Netzwerk-Gateway zum Standard-Gateway des Knotens.
- Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur an explizit konfigurierten Load Balancer-Endpunkten akzeptieren. Sehen "Konfigurieren von Load Balancer-Endpunkten" .
- Wenn die Client-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, überlegen Sie, ob die Konfiguration der Client-Netzwerkschnittstelle (eth2) erforderlich ist. Wenn dies konfiguriert ist, fließt der Client-Netzwerkverkehr über das native Trunk-VLAN, wie im Switch konfiguriert.

Ähnliche Informationen

"Knotennetzwerkkonfiguration ändern"

Bereitstellungsspezifische Netzwerküberlegungen

Linux-Bereitstellungen

Aus Gründen der Effizienz, Zuverlässigkeit und Sicherheit läuft das StorageGRID -System unter Linux als Sammlung von Container-Engines. Eine Container-Engine-bezogene Netzwerkkonfiguration ist in einem StorageGRID System nicht erforderlich.

Verwenden Sie für die Container-Netzwerkschnittstelle ein nicht gebundenes Gerät, z. B. ein VLAN oder ein virtuelles Ethernet-Paar (veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Knotenkonfigurationsdatei an.

Verwenden Sie Bond- oder Bridge-Geräte nicht direkt als Container-Netzwerkschnittstelle. Dies könnte den Start des Knotens aufgrund eines Kernelproblems bei der Verwendung von Macvlan mit Bond- und Bridge-Geräten im Container-Namespace verhindern.

Siehe die Installationsanweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" Bereitstellungen.

Host-Netzwerkkonfiguration für Container-Engine-Bereitstellungen

Bevor Sie mit der StorageGRID -Bereitstellung auf einer Container-Engine-Plattform beginnen, legen Sie fest, welche Netzwerke (Grid, Admin, Client) jeder Knoten verwenden wird. Sie müssen sicherstellen, dass die Netzwerkschnittstelle jedes Knotens auf der richtigen virtuellen oder physischen Hostschnittstelle konfiguriert ist und dass jedes Netzwerk über ausreichend Bandbreite verfügt.

Physische Hosts

Wenn Sie physische Hosts zur Unterstützung von Grid-Knoten verwenden:

- Stellen Sie sicher, dass alle Hosts für jede Knotenschnittstelle dieselbe Hostschnittstelle verwenden. Diese Strategie vereinfacht die Hostkonfiguration und ermöglicht eine zukünftige Knotenmigration.
- Besorgen Sie sich eine IP-Adresse für den physischen Host selbst.

> Eine physische Schnittstelle auf dem Host kann vom Host selbst und einem oder mehreren auf dem Host laufenden Knoten verwendet werden. Alle dem Host oder den Knoten, die diese Schnittstelle verwenden, zugewiesenen IP-Adressen müssen eindeutig sein. Der Host und der Knoten können keine IP-Adressen gemeinsam nutzen.

- Öffnen Sie die erforderlichen Ports zum Host.
- Wenn Sie VLAN-Schnittstellen in StorageGRID verwenden möchten, muss der Host über eine oder mehrere Trunk-Schnittstellen verfügen, die Zugriff auf die gewünschten VLANs bieten. Diese Schnittstellen können als eth0, eth2 oder als zusätzliche Schnittstellen an den Knotencontainer übergeben werden. Informationen zum Hinzufügen von Trunk- oder Zugriffsschnittstellen finden Sie im Folgenden:
  - **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"

Empfehlungen zur Mindestbandbreite

Die folgende Tabelle enthält Empfehlungen zur minimalen LAN-Bandbreite für jeden StorageGRID Knotentyp und jeden Netzwerktyp. Sie müssen jedem physischen oder virtuellen Host eine ausreichende Netzwerkbandbreite bereitstellen, um die aggregierten Mindestbandbreitenanforderungen für die Gesamtzahl und den Typ der StorageGRID Knoten zu erfüllen, die Sie auf diesem Host ausführen möchten.

Knotentyp	**Netzwerktyp**		
	Netz	Administrator	Kunde
	Mindest-LAN-Bandbreite	Administrator	10 Gbit/s
1 Gbit/s	1 Gbit/s	Tor	10 Gbit/s
1 Gbit/s	10 Gbit/s	Storage	10 Gbit/s
1 Gbit/s	10 Gbit/s	Archiv	10 Gbit/s

> Diese Tabelle enthält nicht die SAN-Bandbreite, die für den Zugriff auf gemeinsam genutzten Speicher erforderlich ist. Wenn Sie gemeinsam genutzten Speicher verwenden, auf den über Ethernet (iSCSI oder FCoE) zugegriffen wird, sollten Sie auf jedem Host separate physische Schnittstellen bereitstellen, um ausreichend SAN-Bandbreite bereitzustellen. Um Engpässe zu vermeiden, sollte die SAN-Bandbreite für einen bestimmten Host in etwa der aggregierten Netzwerkbandbreite aller auf diesem Host ausgeführten Speicherknoten entsprechen.

Verwenden Sie die Tabelle, um die Mindestanzahl der auf jedem Host bereitzustellenden Netzwerkschnittstellen zu bestimmen, basierend auf der Anzahl und dem Typ der StorageGRID -Knoten, die Sie auf diesem Host ausführen möchten.

So führen Sie beispielsweise einen Admin-Knoten, einen Gateway-Knoten und einen Speicherknoten auf einem einzelnen Host aus:

- Verbinden Sie das Grid und die Admin-Netzwerke auf dem Admin-Knoten (erfordert 10 + 1 = 11 Gbit/s)
- Verbinden Sie das Grid und die Client-Netzwerke mit dem Gateway-Knoten (erfordert 10 + 10 = 20 Gbit/s)
- Verbinden Sie das Grid-Netzwerk mit dem Speicherknoten (erfordert 10 Gbit/s)

In diesem Szenario sollten Sie mindestens 11 + 20 + 10 = 41 Gbit/s Netzwerkbandbreite bereitstellen. Diese kann durch zwei 40-Gbit/s-Schnittstellen oder fünf 10-Gbit/s-Schnittstellen erreicht werden, die möglicherweise zu Trunks zusammengefasst und dann von den drei oder mehr VLANs gemeinsam genutzt werden, die die Grid-, Admin- und Client-Subnetze lokal zum physischen Rechenzentrum mit dem Host übertragen.

Einige empfohlene Methoden zum Konfigurieren physischer und Netzwerkressourcen auf den Hosts in Ihrem StorageGRID Cluster zur Vorbereitung Ihrer StorageGRID Bereitstellung finden Sie im Folgenden:

- "Konfigurieren des Hostnetzwerks (Red Hat Enterprise Linux)"
- "Konfigurieren Sie das Hostnetzwerk (Ubuntu oder Debian)."

Vernetzung und Ports für Plattformdienste und Cloud-Speicherpools

Wenn Sie StorageGRID -Plattformdienste oder Cloud Storage Pools verwenden möchten, müssen Sie Grid-Netzwerke und Firewalls konfigurieren, um sicherzustellen, dass die Zielendpunkte erreicht werden können.

Vernetzung für Plattformdienste

Wie beschrieben in"Plattformdienste für Mandanten verwalten" Und"Plattformdienste verwalten" Zu den Plattformdiensten gehören externe Dienste, die Suchintegration, Ereignisbenachrichtigung und CloudMirror-Replikation bereitstellen.

Plattformdienste erfordern Zugriff von Speicherknoten, die den StorageGRID ADC-Dienst hosten, auf die externen Dienstendpunkte. Beispiele für die Bereitstellung des Zugriffs sind:

- Konfigurieren Sie auf den Speicherknoten mit ADC-Diensten eindeutige Admin-Netzwerke mit AESL-Einträgen, die zu den Zielendpunkten weiterleiten.
- Verlassen Sie sich auf die Standardroute, die von einem Client-Netzwerk bereitgestellt wird. Wenn Sie die Standardroute verwenden, können Sie die"nicht vertrauenswürdige Client-Netzwerkfunktion" um eingehende Verbindungen einzuschränken.

Vernetzung für Cloud-Speicherpools

Cloud-Speicherpools erfordern außerdem Zugriff von Speicherknoten auf die Endpunkte, die vom verwendeten externen Dienst bereitgestellt werden, z. B. Amazon S3 Glacier oder Microsoft Azure Blob Storage. Weitere Informationen finden Sie unter"Was ist ein Cloud-Speicherpool?" .

Ports für Plattformdienste und Cloud Storage Pools

Standardmäßig verwenden Plattformdienste und die Cloud Storage Pool-Kommunikation die folgenden Ports:

- **80**: Für Endpunkt-URIs, die mit beginnen `http`
- **443**: Für Endpunkt-URIs, die mit beginnen `https`

Beim Erstellen oder Bearbeiten des Endpunkts kann ein anderer Port angegeben werden. Sehen "Netzwerkportreferenz" .

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.

VLANs und Plattformdienste und Cloud-Speicherpools

Sie können keine VLAN-Netzwerke für Plattformdienste oder Cloud-Speicherpools verwenden. Die Zielendpunkte müssen über das Grid-, Admin- oder Client-Netzwerk erreichbar sein.

Appliance-Knoten

Sie können die Netzwerkports auf StorageGRID -Geräten so konfigurieren, dass sie die Port-Bond-Modi verwenden, die Ihren Anforderungen an Durchsatz, Redundanz und Failover entsprechen.

Die 10/25-GbE-Ports auf den StorageGRID -Geräten können für Verbindungen zum Grid-Netzwerk und Client-Netzwerk im Fixed- oder Aggregate-Bond-Modus konfiguriert werden.

Die 1-GbE-Admin-Netzwerkports können für Verbindungen zum Admin-Netzwerk im unabhängigen oder aktiven Backup-Modus konfiguriert werden.

Informieren Sie sich über die Port-Bond-Modi für Ihr Gerät:

- "Port-Bond-Modi (SG6160)"
- "Port-Bond-Modi (SGF6112)"
- "Port-Bond-Modi (SG6000-CN-Controller)"
- "Port-Bond-Modi (SG5800-Controller)"
- "Port-Bond-Modi (E5700SG-Controller)"
- "Port-Bond-Modi (SG110 und SG1100)"
- "Port-Bond-Modi (SG100 und SG1000)"

Netzwerkinstallation und -bereitstellung

Sie müssen verstehen, wie das Grid-Netzwerk und die optionalen Admin- und Client-Netzwerke während der Knotenbereitstellung und Grid-Konfiguration verwendet werden.

Erstmalige Bereitstellung eines Knotens

Wenn Sie einen Knoten zum ersten Mal bereitstellen, müssen Sie den Knoten an das Grid-Netzwerk anschließen und sicherstellen, dass er Zugriff auf den primären Admin-Knoten hat. Wenn das Grid-Netzwerk isoliert ist, können Sie das Admin-Netzwerk auf dem primären Admin-Knoten für den Konfigurations- und Installationszugriff von außerhalb des Grid-Netzwerks konfigurieren.

Ein Grid-Netzwerk mit konfiguriertem Gateway wird während der Bereitstellung zum Standard-Gateway für

einen Knoten. Das Standard-Gateway ermöglicht Grid-Knoten in separaten Subnetzen die Kommunikation mit dem primären Admin-Knoten, bevor das Grid konfiguriert wurde.

Bei Bedarf können auch Subnetze, die NTP-Server enthalten oder Zugriff auf den Grid Manager oder die API benötigen, als Grid-Subnetze konfiguriert werden.

Automatische Knotenregistrierung mit primärem Admin-Knoten

Nachdem die Knoten bereitgestellt wurden, registrieren sie sich über das Grid-Netzwerk beim primären Admin-Knoten. Anschließend können Sie den Grid Manager, den `configure-storagegrid.py` Python-Skript oder die Installations-API zum Konfigurieren des Rasters und Genehmigen der registrierten Knoten. Während der Grid-Konfiguration können Sie mehrere Grid-Subnetze konfigurieren. Wenn Sie die Grid-Konfiguration abschließen, werden auf jedem Knoten statische Routen zu diesen Subnetzen über das Grid-Netzwerk-Gateway erstellt.

Deaktivieren des Admin-Netzwerks oder Client-Netzwerks

Wenn Sie das Admin-Netzwerk oder das Client-Netzwerk deaktivieren möchten, können Sie die Konfiguration während des Knotengenehmigungsprozesses entfernen oder nach Abschluss der Installation das Tool „IP ändern“ verwenden (siehe"Konfigurieren von IP-Adressen").

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Bereitstellung und Konfiguration des Grid-Knotens diese Richtlinien für DHCP-Adressierung und Netzwerkkonfigurationsänderungen.

- Wenn DHCP zum Zuweisen von IP-Adressen verwendet wurde, konfigurieren Sie eine DHCP-Reservierung für jede IP-Adresse in den verwendeten Netzwerken.

  Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten.

  > Knoten werden neu gestartet, wenn die Grid-Netzwerkkonfiguration per DHCP geändert wird. Dies kann zu Ausfällen führen, wenn eine DHCP-Änderung mehrere Knoten gleichzeitig betrifft.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmasken und Standard-Gateways für einen Grid-Knoten ändern möchten. Sehen "Konfigurieren von IP-Adressen" .
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin-Knoten und anderen Grid-Knoten verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Netzwerkportreferenz

Interne Grid-Knoten-Kommunikation

Die interne Firewall von StorageGRID ermöglicht eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk. Verbindungen werden auch auf Ports akzeptiert, die von Load Balancer-Endpunkten definiert werden.

NetApp empfiehlt, den ICMP-Verkehr (Internet Control Message Protocol) zwischen Grid-Knoten zu aktivieren. Das Zulassen von ICMP-Verkehr kann die Failover-Leistung verbessern, wenn ein Grid-Knoten nicht erreicht werden kann.

Zusätzlich zu ICMP und den in der Tabelle aufgeführten Ports verwendet StorageGRID das Virtual Router Redundancy Protocol (VRRP). VRRP ist ein Internetprotokoll, das die IP-Protokollnummer 112 verwendet. StorageGRID verwendet VRRP nur im Unicast-Modus. VRRP ist nur erforderlich, wenn"Hochverfügbarkeitsgruppen" konfiguriert sind.

Richtlinien für Linux-basierte Knoten

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports zum Zeitpunkt der Bereitstellung mithilfe eines Bereitstellungskonfigurationsparameters neu zuordnen. Weitere Informationen zur Portneuzuordnung und zu den Bereitstellungskonfigurationsparametern finden Sie unter:

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"

Richtlinien für VMware-basierte Knoten

Konfigurieren Sie die folgenden Ports nur, wenn Sie Firewall-Einschränkungen definieren müssen, die außerhalb des VMware-Netzwerks liegen.

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports neu zuordnen, wenn Sie Knoten mithilfe des VMware vSphere Web Client bereitstellen oder indem Sie bei der Automatisierung der Grid-Knotenbereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen zur Portneuzuordnung und zu den Bereitstellungskonfigurationsparametern finden Sie unter"Installieren Sie StorageGRID auf VMware" .

Richtlinien für Appliance-Knoten

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Sehen "Optional: Netzwerkports für das Gerät neu zuordnen" .

Interne StorageGRID Ports

Hafen	TCP oder UDP	Aus	Zu	Details
22	TCP	Primärer Admin-Knoten	Alle Knoten	Für Wartungsverfahren muss der primäre Admin-Knoten in der Lage sein, über SSH auf Port 22 mit allen anderen Knoten zu kommunizieren. Das Zulassen von SSH-Verkehr von anderen Knoten ist optional.
80	TCP	Geräte	Primärer Admin-Knoten	Wird von StorageGRID -Geräten verwendet, um mit dem primären Admin-Knoten zu kommunizieren und die Installation zu starten.

Hafen	TCP oder UDP	Aus	Zu	Details
123	UDP	Alle Knoten	Alle Knoten	Netzwerkzeitprotokolldienst. Jeder Knoten synchronisiert seine Zeit mit jedem anderen Knoten über NTP.
443	TCP	Alle Knoten	Primärer Admin-Knoten	Wird verwendet, um während der Installation und anderer Wartungsvorgänge den Status an den primären Admin-Knoten zu übermitteln.
1055	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
1139	TCP	Speicherknoten	Speicherknoten	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Knoten	Speicherknoten mit ADC	Berichterstellung, Prüfung und Konfiguration des internen Datenverkehrs.
1502	TCP	Alle Knoten	Speicherknoten	S3- und Swift-bezogener interner Datenverkehr.
1504	TCP	Alle Knoten	Admin-Knoten	NMS-Dienstberichterstattung und Konfiguration des internen Datenverkehrs.
1505	TCP	Alle Knoten	Admin-Knoten	AMS-Service-interner Verkehr.
1506	TCP	Alle Knoten	Alle Knoten	Serverstatus interner Datenverkehr.
1507	TCP	Alle Knoten	Gateway-Knoten	Interner Datenverkehr des Load Balancers.
1508	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr des Konfigurationsmanagements.
1511	TCP	Alle Knoten	Speicherknoten	Metadaten des internen Datenverkehrs.
5353	UDP	Alle Knoten	Alle Knoten	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird.

Hafen	TCP oder UDP	Aus	Zu	Details
7001	TCP	Speicherknoten	Speicherknoten	Cassandra TLS-Clusterkommunikation zwischen Knoten.
7443	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
8443	TCP	Primärer Admin-Knoten	Appliance-Knoten	Interner Verkehr im Zusammenhang mit dem Wartungsmodusverfahren.
9042	TCP	Speicherknoten	Speicherknoten	Cassandra-Client-Port.
9999	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr für mehrere Dienste. Beinhaltet Wartungsverfahren, Metriken und Netzwerkupdates.
10226	TCP	Speicherknoten	Primärer Admin-Knoten	Wird von StorageGRID -Geräten zum Weiterleiten von AutoSupport Paketen vom E-Series SANtricity System Manager an den primären Admin-Knoten verwendet.
10342	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
18000	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Datenverkehr des Kontodienstes.
18001	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Datenverkehr der Identity Federation.
18002	TCP	Admin-/Speicherknoten	Speicherknoten	Interner API-Verkehr im Zusammenhang mit Objektprotokollen.
18003	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Die Plattform bedient den internen Datenverkehr.

Hafen	TCP oder UDP	Aus	Zu	Details
18017	TCP	Admin-/Speicherknoten	Speicherknoten	Interner Datenverkehr des Data Mover-Dienstes für Cloud Storage Pools.
18019	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr des Chunk-Dienstes für Erasure Coding und Replikation
18082	TCP	Admin-/Speicherknoten	Speicherknoten	S3-bezogener interner Datenverkehr.
18083	TCP	Alle Knoten	Speicherknoten	Swift-bezogener interner Verkehr.
18086	TCP	Alle Knoten	Speicherknoten	Interner Verkehr im Zusammenhang mit dem LDR-Dienst.
18200	TCP	Admin-/Speicherknoten	Speicherknoten	Zusätzliche Statistiken zu Clientanfragen.
19000	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Verkehr des Keystone -Dienstes.

Ähnliche Informationen

"Externe Kommunikation"

Externe Kommunikation

Clients müssen mit Grid-Knoten kommunizieren, um Inhalte aufzunehmen und abzurufen. Die verwendeten Ports hängen von den gewählten Objektspeicherprotokollen ab. Diese Ports müssen für den Client zugänglich sein.

Eingeschränkter Zugang zu Häfen

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen der Ports einschränken, können Sie Folgendes tun:

- Verwenden"Load Balancer-Endpunkte" um den Zugriff auf benutzerdefinierte Ports zu ermöglichen.
- Ordnen Sie die Ports beim Bereitstellen von Knoten neu zu. Sie sollten die Endpunkte des Lastenausgleichs jedoch nicht neu zuordnen. Sehen Sie sich die Informationen zur Portneuzuordnung für Ihren StorageGRID Knoten an:
  - "Port-Neuzuordnungsschlüssel für StorageGRID unter Red Hat Enterprise Linux"
  - "Port-Neuzuordnungsschlüssel für StorageGRID unter Ubuntu oder Debian"

- "Ports für StorageGRID auf VMware neu zuordnen"
- "Optional: Netzwerkports für das Gerät neu zuordnen"

Für die externe Kommunikation verwendete Ports

Die folgende Tabelle zeigt die für den Datenverkehr in die Knoten verwendeten Ports.

> Diese Liste enthält keine Ports, die möglicherweise konfiguriert sind als"Load Balancer-Endpunkte" .

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
22	TCP	SSH	Service-Laptop	Alle Knoten	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 2022 anstelle von 22 verwenden.
25	TCP	SMTP	Admin-Knoten	E-Mail-Server	Wird für Warnungen und E-Mail-basierten AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 auf der Seite „E-Mail-Server“ überschreiben.
53	TCP/UDP	DNS	Alle Knoten	DNS-Server	Wird für DNS verwendet.
67	UDP	DHCP	Alle Knoten	DHCP-Dienst	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient-Dienst wird für statisch konfigurierte Grids nicht ausgeführt.
68	UDP	DHCP	DHCP-Dienst	Alle Knoten	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient-Dienst wird nicht für Grids ausgeführt, die statische IP-Adressen verwenden.
80	TCP	HTTP	Browser	Admin-Knoten	Port 80 leitet für die Benutzeroberfläche des Admin-Knotens auf Port 443 um.
80	TCP	HTTP	Browser	Geräte	Port 80 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
80	TCP	HTTP	Speicherknoten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTP verwenden. Mandanten können die Standard-HTTP-Porteinstellung von 80 beim Erstellen eines Endpunkts überschreiben.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
80	TCP	HTTP	Speicherknoten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTP verwenden. Grid-Administratoren können die Standard-HTTP-Porteinstellung von 80 beim Konfigurieren eines Cloud-Speicherpools überschreiben.
111	TCP/UDP	RPCBind	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export (Portmap) verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
123	UDP	NTP	Primäre NTP-Knoten	Externes NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Knoten synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.
161	TCP/UDP	SNMP	SNMP-Client	Alle Knoten	Wird für SNMP-Polling verwendet. Alle Knoten stellen grundlegende Informationen bereit; Admin-Knoten stellen auch Warndaten bereit. Bei Konfiguration wird standardmäßig der UDP-Port 161 verwendet. **Hinweis:** Dieser Port ist nur erforderlich und wird nur in der Knoten-Firewall geöffnet, wenn SNMP konfiguriert ist. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.
162	TCP/UDP	SNMP-Benachrichtigungen	Alle Knoten	Benachrichtigungsziele	Ausgehende SNMP-Benachrichtigungen und Traps werden standardmäßig an UDP-Port 162 gesendet. **Hinweis:** Dieser Port ist nur erforderlich, wenn SNMP aktiviert und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
389	TCP/UDP	LDAP	Speicherknoten mit ADC	Active Directory/LDAP	Wird zum Herstellen einer Verbindung mit einem Active Directory- oder LDAP-Server für die Identitätsföderation verwendet.
443	TCP	HTTPS	Browser	Admin-Knoten	Wird von Webbrowsern und Management-API-Clients verwendet, um auf den Grid Manager und den Tenant Manager zuzugreifen. **Hinweis**: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.
443	TCP	HTTPS	Admin-Knoten	Active Directory	Wird von Admin-Knoten verwendet, die eine Verbindung zu Active Directory herstellen, wenn Single Sign-On (SSO) aktiviert ist.
443	TCP	HTTPS	Speicherknoten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTPS verwenden. Mandanten können die Standard-HTTP-Porteinstellung 443 beim Erstellen eines Endpunkts überschreiben.
443	TCP	HTTPS	Speicherknoten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTPS verwenden. Grid-Administratoren können die Standard-HTTPS-Porteinstellung 443 beim Konfigurieren eines Cloud-Speicherpools überschreiben.
903	TCP	NFS	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export verwendet(`rpc.mountd`). **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
2022	TCP	SSH	Service-Laptop	Alle Knoten	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 22 anstelle von 2022 verwenden.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
2049	TCP	NFS	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export (NFS) verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
5353	UDP	mDNS	Alle Knoten	Alle Knoten	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird.
5696	TCP	KMIP	Gerät	KMS	Externer Datenverkehr des Key Management Interoperability Protocol (KMIP) von für die Knotenverschlüsselung konfigurierten Geräten zum Key Management Server (KMS), sofern auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer kein anderer Port angegeben ist.
8022	TCP	SSH	Service-Laptop	Alle Knoten	SSH auf Port 8022 gewährt Zugriff auf das Basisbetriebssystem auf Appliance- und virtuellen Knotenplattformen für Support und Fehlerbehebung. Dieser Port wird nicht für Linux-basierte (Bare-Metal-)Knoten verwendet und muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.
8443	TCP	HTTPS	Browser	Admin-Knoten	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen. **Hinweis**: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
8443	TCP	HTTPS	Browser	Geräte	Wird von Webbrowsern und Verwaltungs-API-Clients verwendet, um auf das StorageGRID Appliance Installer zuzugreifen. **Hinweis**: Port 443 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
9022	TCP	SSH	Service-Laptop	Geräte	Gewährt Zugriff auf StorageGRID -Geräte im Vorkonfigurationsmodus für Support und Fehlerbehebung. Dieser Port muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.
9091	TCP	HTTPS	Externer Grafana-Dienst	Admin-Knoten	Wird von externen Grafana-Diensten für den sicheren Zugriff auf den StorageGRID Prometheus-Dienst verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der zertifikatsbasierte Prometheus-Zugriff aktiviert ist.
9092	TCP	Kafka	Speicherknoten mit ADC	Kafka-Cluster	Wird für Plattformdienstnachrichten verwendet, die an einen Kafka-Cluster gesendet werden. Mandanten können die standardmäßige Kafka-Porteinstellung von 9092 beim Erstellen eines Endpunkts überschreiben.
9443	TCP	HTTPS	Browser	Admin-Knoten	Optional. Wird von Webbrowsern und Verwaltungs-API-Clients für den Zugriff auf den Tenant Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen.
18082	TCP	HTTPS	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18083	TCP	HTTPS	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18084	TCP	HTTP	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTP).
18085	TCP	HTTP	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTP).

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
23000-23999	TCP	HTTPS	Alle Knoten im Quellgrid für die Cross-Grid-Replikation	Admin-Knoten und Gateway-Knoten im Ziel-Grid für die Cross-Grid-Replikation	Dieser Portbereich ist für Grid-Föderation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden denselben Port.

Schnellstart für StorageGRID

Befolgen Sie diese allgemeinen Schritte, um ein beliebiges StorageGRID -System zu konfigurieren und zu verwenden.

1 Lernen, planen und Daten sammeln

Arbeiten Sie mit Ihrem NetApp Kundenbetreuer zusammen, um die Optionen zu verstehen und Ihr neues StorageGRID -System zu planen. Stellen Sie sich folgende Fragen:

- Wie viele Objektdaten werden Sie voraussichtlich zunächst und im Laufe der Zeit speichern?
- Wie viele Standorte benötigen Sie?
- Wie viele und welche Arten von Knoten benötigen Sie an jedem Standort?
- Welche StorageGRID Netzwerke werden Sie verwenden?
- Wer wird Ihr Raster zum Speichern von Objekten verwenden? Welche Anwendungen werden sie verwenden?
- Haben Sie besondere Sicherheits- oder Lageranforderungen?
- Müssen Sie gesetzliche oder behördliche Anforderungen erfüllen?

Optional können Sie mit Ihrem NetApp Professional Services-Berater zusammenarbeiten, um auf das NetApp ConfigBuilder-Tool zuzugreifen und eine Konfigurationsarbeitsmappe für die Installation und Bereitstellung Ihres neuen Systems auszufüllen. Sie können dieses Tool auch verwenden, um die Konfiguration beliebiger StorageGRID Geräte zu automatisieren. Sehen "Automatisieren Sie die Installation und Konfiguration von Geräten" .

Rezension"Erfahren Sie mehr über StorageGRID" und die"Netzwerkrichtlinien" .

2 Knoten installieren

Ein StorageGRID -System besteht aus einzelnen hardware- und softwarebasierten Knoten. Sie installieren zunächst die Hardware für jeden Appliance-Knoten und konfigurieren jeden Linux- oder VMware-Host.

Um die Installation abzuschließen, installieren Sie die StorageGRID -Software auf jedem Gerät oder

Softwarehost und verbinden die Knoten zu einem Grid. In diesem Schritt geben Sie Site- und Knotennamen, Subnetzdetails und die IP-Adressen für Ihre NTP- und DNS-Server an.

Erfahren Sie, wie:

- "Installieren der Appliance-Hardware"
- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"

Sign in und Systemintegrität prüfen

Sobald Sie den primären Admin-Knoten installiert haben, können Sie sich beim Grid Manager anmelden. Von dort aus können Sie den allgemeinen Zustand Ihres neuen Systems überprüfen, AutoSupport und Warn-E-Mails aktivieren und S3-Endpunktdomänennamen einrichten.

Erfahren Sie, wie:

- "Sign in"
- "Überwachen Sie den Systemzustand"
- "Konfigurieren Sie AutoSupport"
- "E-Mail-Benachrichtigungen für Warnmeldungen einrichten"
- "Konfigurieren von S3-Endpunktdomänennamen"

Konfigurieren und Verwalten

Die Konfigurationsaufgaben, die Sie für ein neues StorageGRID -System durchführen müssen, hängen davon ab, wie Sie Ihr Grid verwenden werden. Sie richten mindestens den Systemzugriff ein, verwenden die FabricPool und S3-Assistenten und verwalten verschiedene Speicher- und Sicherheitseinstellungen.

Erfahren Sie, wie:

- "Steuern Sie den StorageGRID Zugriff"
- "Verwenden Sie den S3-Setup-Assistenten"
- "Verwenden des FabricPool -Setup-Assistenten"
- "Verwalten der Sicherheit"
- "Systemhärtung"

Einrichten von ILM

Sie steuern die Platzierung und Dauer jedes Objekts in Ihrem StorageGRID -System, indem Sie eine ILM-Richtlinie (Information Lifecycle Management) konfigurieren, die aus einer oder mehreren ILM-Regeln besteht. Die ILM-Regeln weisen StorageGRID an, wie Kopien von Objektdaten erstellt und verteilt und wie diese Kopien im Laufe der Zeit verwaltet werden.

Erfahren Sie, wie:"Objekte mit ILM verwalten"

6 Verwenden Sie StorageGRID

Nachdem die Erstkonfiguration abgeschlossen ist, können StorageGRID Mandantenkonten S3-Clientanwendungen verwenden, um Objekte aufzunehmen, abzurufen und zu löschen.

Erfahren Sie, wie:

- "Verwenden eines Mandantenkontos"
- "Verwenden Sie die S3 REST API"

7 Überwachen und Fehler beheben

Wenn Ihr System betriebsbereit ist, sollten Sie seine Aktivitäten regelmäßig überwachen und alle Fehler beheben und Warnmeldungen beseitigen. Möglicherweise möchten Sie auch einen externen Syslog-Server konfigurieren, SNMP-Überwachung verwenden oder zusätzliche Daten sammeln.

Erfahren Sie, wie:

- "StorageGRID überwachen"
- "Fehlerbehebung bei StorageGRID"

8 Erweitern, pflegen und wiederherstellen

Sie können Knoten oder Sites hinzufügen, um die Kapazität oder Funktionalität Ihres Systems zu erweitern. Sie können auch verschiedene Wartungsverfahren durchführen, um Fehler zu beheben oder Ihr StorageGRID -System auf dem neuesten Stand und effizient zu halten.

Erfahren Sie, wie:

- "Erweitern eines Rasters"
- "Pflegen Sie Ihr Netz"
- "Knoten wiederherstellen"

Installieren, Aktualisieren und Hotfixen von StorageGRID

StorageGRID -Geräte

Gehe zu "StorageGRID Appliance-Dokumentation" um zu erfahren, wie Sie StorageGRID Speicher- und Servicegeräte installieren, konfigurieren und warten.

Installieren Sie StorageGRID unter Red Hat Enterprise Linux

Schnellstart zur Installation von StorageGRID auf Red Hat Enterprise Linux

Befolgen Sie diese allgemeinen Schritte, um einen Red Hat Enterprise Linux (RHEL) Linux StorageGRID Knoten zu installieren.

Vorbereitung

- Erfahren Sie mehr über"StorageGRID -Architektur und Netzwerktopologie" .
- Erfahren Sie mehr über die Besonderheiten von"StorageGRID Netzwerk" .
- Sammeln und vorbereiten Sie die"Benötigte Informationen und Materialien" .
- Bereiten Sie die erforderlichen"CPU und RAM" .
- Sorgen für"Speicher- und Leistungsanforderungen" .
- "Vorbereiten der Linux-Server"das Ihre StorageGRID Knoten hosten wird.

Einsatz

Stellen Sie Grid-Knoten bereit. Wenn Sie Grid-Knoten bereitstellen, werden diese als Teil des StorageGRID -Systems erstellt und mit einem oder mehreren Netzwerken verbunden.

- Um softwarebasierte Grid-Knoten auf den Hosts bereitzustellen, die Sie in Schritt 1 vorbereitet haben, verwenden Sie die Linux-Befehlszeile und"Knotenkonfigurationsdateien" .
- Um StorageGRID Appliance-Knoten bereitzustellen, folgen Sie den "Schnellstart für die Hardwareinstallation" .

Konfiguration

Wenn alle Knoten bereitgestellt wurden, verwenden Sie den Grid Manager, um"Konfigurieren Sie das Grid und schließen Sie die Installation ab" .

Automatisieren Sie die Installation

Um Zeit zu sparen und Konsistenz zu gewährleisten, können Sie die Installation des StorageGRID Hostdienstes und die Konfiguration der Grid-Knoten automatisieren.

- Verwenden Sie ein Standard-Orchestrierungsframework wie Ansible, Puppet oder Chef, um Folgendes zu

automatisieren:

- Installation von RHEL
- Konfiguration von Netzwerk und Speicher
- Installation der Container-Engine und des StorageGRID -Hostdienstes
- Bereitstellung virtueller Grid-Knoten

Sehen "Automatisieren Sie die Installation und Konfiguration des StorageGRID Hostdienstes" .

- Nachdem Sie Grid-Knoten bereitgestellt haben,"Automatisieren Sie die Konfiguration des StorageGRID -Systems" mithilfe des im Installationsarchiv bereitgestellten Python-Konfigurationsskripts.
- "Automatisieren Sie die Installation und Konfiguration von Appliance-Grid-Knoten"
- Wenn Sie ein fortgeschrittener Entwickler von StorageGRID Bereitstellungen sind, automatisieren Sie die Installation von Grid-Knoten mithilfe der"Installation der REST-API" .

Planen und Vorbereiten der Installation auf Red Hat

Benötigte Informationen und Materialien

Bevor Sie StorageGRID installieren, sammeln und bereiten Sie die erforderlichen Informationen und Materialien vor.

Erforderliche Informationen

Netzwerkplan

Welche Netzwerke Sie an jeden StorageGRID Knoten anschließen möchten. StorageGRID unterstützt mehrere Netzwerke zur Verkehrstrennung, Sicherheit und Verwaltungsfreundlichkeit.

Zum StorageGRID"Netzwerkrichtlinien" .

Netzwerkinformationen

Jedem Grid-Knoten zuzuweisende IP-Adressen und die IP-Adressen der DNS- und NTP-Server.

Server für Grid-Knoten

Identifizieren Sie eine Reihe von Servern (physisch, virtuell oder beides), die insgesamt ausreichend Ressourcen bereitstellen, um die Anzahl und Art der StorageGRID Knoten zu unterstützen, die Sie bereitstellen möchten.

> ⓘ Wenn Ihre StorageGRID Installation keine StorageGRID Appliance-(Hardware-)Speicherknoten verwendet, müssen Sie Hardware-RAID-Speicher mit batteriegepuffertem Schreibcache (BBWC) verwenden. StorageGRID unterstützt nicht die Verwendung von virtuellen Storage Area Networks (vSANs), Software-RAID oder keinen RAID-Schutz.

Knotenmigration (falls erforderlich)

Verstehen Sie die"Anforderungen für die Knotenmigration" , wenn Sie geplante Wartungsarbeiten an physischen Hosts ohne Dienstunterbrechung durchführen möchten.

Ähnliche Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Benötigtes Material

NetApp StorageGRID -Lizenz

Sie müssen über eine gültige, digital signierte NetApp -Lizenz verfügen.

> Eine Nicht-Produktionslizenz, die zum Testen und Proof-of-Concept-Grids verwendet werden kann, ist im StorageGRID -Installationsarchiv enthalten.

StorageGRID -Installationsarchiv

"Laden Sie das StorageGRID Installationsarchiv herunter und extrahieren Sie die Dateien" .

Service-Laptop

Die Installation des StorageGRID -Systems erfolgt über einen Service-Laptop.

Der Dienstlaptop muss über Folgendes verfügen:

- Netzwerkanschluss
- SSH-Client (z. B. PuTTY)
- "Unterstützte Webbrowser"

StorageGRID -Dokumentation

- "Versionshinweise"
- "Anleitung zur Administration von StorageGRID"

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Sie müssen das StorageGRID Installationsarchiv herunterladen und die erforderlichen Dateien extrahieren. Optional können Sie die Dateien im Installationspaket manuell überprüfen.

Schritte

1. Gehen Sie zum "NetApp -Downloadseite für StorageGRID" .
2. Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version oder wählen Sie eine andere Version aus dem Dropdown-Menü und wählen Sie **Los**.
3. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Ihr NetApp -Konto an .
4. Wenn eine Warnung/ein unbedingt zu lesender Hinweis erscheint, lesen Sie ihn und aktivieren Sie das Kontrollkästchen.

   > Sie müssen alle erforderlichen Hotfixes anwenden, nachdem Sie die StorageGRID Version installiert haben. Weitere Informationen finden Sie im "Hotfix-Verfahren in den Wiederherstellungs- und Wartungsanweisungen" .

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.
6. Wählen Sie in der Spalte **Install StorageGRID** das .tgz- oder .zip-Installationsarchiv für Red Hat Enterprise Linux aus.

   > Wählen Sie die `.zip` Datei, wenn Sie Windows auf dem Service-Laptop ausführen.

7. Speichern Sie das Installationsarchiv.
8. Wenn Sie das Installationsarchiv überprüfen müssen:
   a. Laden Sie das StorageGRID -Codesignaturüberprüfungspaket herunter. Der Dateiname für dieses Paket verwendet das Format `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , Wo `<version-number>` ist die StorageGRID -Softwareversion.
   b. Folgen Sie den Schritten, um"Überprüfen Sie die Installationsdateien manuell" .
9. Extrahieren Sie die Dateien aus dem Installationsarchiv.
10. Wählen Sie die benötigten Dateien aus.

    Welche Dateien Sie benötigen, hängt von Ihrer geplanten Grid-Topologie und der Art und Weise ab, wie Sie Ihr StorageGRID -System bereitstellen.

    Die in der Tabelle aufgeführten Pfade beziehen sich auf das oberste Verzeichnis, das durch das extrahierte Installationsarchiv installiert wird.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet.
	RPM-Paket zum Installieren der StorageGRID -Knotenimages auf Ihren RHEL-Hosts.
	RPM-Paket zum Installieren des StorageGRID Hostdienstes auf Ihren RHEL-Hosts.
Bereitstellungsskripttool	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.

Pfad und Dateiname	Beschreibung
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Beispiel für eine Ansible-Rolle und ein Playbook zum Konfigurieren von RHEL-Hosts für die Bereitstellung von StorageGRID Containern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

Installationsdateien manuell überprüfen (optional)

Bei Bedarf können Sie die Dateien im StorageGRID Installationsarchiv manuell überprüfen.

Bevor Sie beginnen

Du hast"das Verifizierungspaket heruntergeladen" aus dem "NetApp -Downloadseite für StorageGRID" .

Schritte

1. Extrahieren Sie die Artefakte aus dem Verifizierungspaket:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Stellen Sie sicher, dass diese Artefakte extrahiert wurden:
   - Blattzertifikat: `Leaf-Cert.pem`
   - Zertifikatskette: `CA-Int-Cert.pem`
   - Zeitstempel-Antwortkette: `TS-Cert.pem`
   - Prüfsummendatei: `sha256sum`

- Prüfsummensignatur: `sha256sum.sig`
- Zeitstempel-Antwortdatei: `sha256sum.sig.tsr`

3. Verwenden Sie die Kette, um zu überprüfen, ob das Blattzertifikat gültig ist.

   Beispiel: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

   Erwartete Ausgabe: `Leaf-Cert.pem: OK`

4. Wenn Schritt *2* aufgrund eines abgelaufenen Blattzertifikats fehlgeschlagen ist, verwenden Sie die `tsr` zu überprüfende Datei.

   Beispiel: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

   Die erwartete Ausgabe umfasst: `Verification: OK`

5. Erstellen Sie eine öffentliche Schlüsseldatei aus dem Blattzertifikat.

   Beispiel: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

   Erwartete Ausgabe: *keine*

6. Verwenden Sie den öffentlichen Schlüssel, um die `sha256sum` Datei gegen `sha256sum.sig` .

   Beispiel: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   Erwartete Ausgabe: `Verified OK`

7. Überprüfen Sie die `sha256sum` Dateiinhalte mit neu erstellten Prüfsummen vergleichen.

   Beispiel: `sha256sum -c sha256sum`

   Erwartete Ausgabe: `<filename>: OK`
   <filename> ist der Name der Archivdatei, die Sie heruntergeladen haben.

8. "Führen Sie die restlichen Schritte aus"um die entsprechenden Dateien aus dem Installationsarchiv zu extrahieren und auszuwählen.

Softwareanforderungen für Red Hat Enterprise Linux

Sie können eine virtuelle Maschine verwenden, um jeden StorageGRID Knotentyp zu hosten. Sie benötigen eine virtuelle Maschine für jeden Grid-Knoten.

Um StorageGRID auf Red Hat Enterprise Linux (RHEL) zu installieren, müssen Sie einige Softwarepakete von Drittanbietern installieren. Einige unterstützte Linux-Distributionen enthalten diese Pakete nicht standardmäßig. Zu den Softwarepaketversionen, auf denen StorageGRID Installationen getestet werden, gehören die auf dieser Seite aufgeführten.

Wenn Sie eine Linux-Distribution und eine Container-Runtime-Installationsoption auswählen, die eines dieser Pakete erfordert und diese nicht automatisch von der Linux-Distribution installiert werden, installieren Sie eine der hier aufgeführten Versionen, sofern diese von Ihrem Provider oder dem unterstützenden Anbieter für Ihre

Linux-Distribution verfügbar ist. Verwenden Sie andernfalls die von Ihrem Anbieter verfügbaren Standardpaketversionen.

Alle Installationsoptionen erfordern entweder Podman oder Docker. Installieren Sie nicht beide Pakete. Installieren Sie nur das Paket, das für Ihre Installationsoption erforderlich ist.

Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt.

Getestete Python-Versionen

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Getestete Podman-Versionen

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Getestete Docker-Versionen

Die Docker-Unterstützung ist veraltet und wird in einer zukünftigen Version entfernt.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1

- Docker-CE 24.0.7-1
- 1,5-2

CPU- und RAM-Anforderungen

Überprüfen und konfigurieren Sie vor der Installation der StorageGRID -Software die Hardware, sodass sie das StorageGRID -System unterstützen kann.

Jeder StorageGRID -Knoten benötigt die folgenden Mindestressourcen:

- CPU-Kerne: 8 pro Knoten
- RAM: Abhängig vom insgesamt verfügbaren RAM und der Menge der auf dem System ausgeführten Nicht-StorageGRID -Software
  - Im Allgemeinen mindestens 24 GB pro Knoten und 2 bis 16 GB weniger als der gesamte System-RAM
  - Mindestens 64 GB für jeden Mandanten mit etwa 5.000 Buckets

Softwarebasierte Knotenressourcen, die nur Metadaten enthalten, müssen mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:

- Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
  - 128 GB RAM
  - 8-Kern-CPU
  - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)
- Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).

Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

Stellen Sie sicher, dass die Anzahl der StorageGRID -Knoten, die Sie auf jedem physischen oder virtuellen Host ausführen möchten, die Anzahl der verfügbaren CPU-Kerne oder des physischen RAM nicht überschreitet. Wenn die Hosts nicht ausschließlich für die Ausführung von StorageGRID vorgesehen sind (nicht empfohlen), müssen Sie unbedingt den Ressourcenbedarf der anderen Anwendungen berücksichtigen.

> Überwachen Sie regelmäßig Ihre CPU- und Speichernutzung, um sicherzustellen, dass diese Ressourcen weiterhin Ihrer Arbeitslast gerecht werden. Beispielsweise würde eine Verdoppelung der RAM- und CPU-Zuweisung für virtuelle Speicherknoten ähnliche Ressourcen bereitstellen wie für StorageGRID Appliance-Knoten. Wenn die Menge der Metadaten pro Knoten 500 GB übersteigt, sollten Sie außerdem eine Erhöhung des RAM pro Knoten auf 48 GB oder mehr in Betracht ziehen. Informationen zum Verwalten des Objektmetadatenspeichers, zum Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten und zum Überwachen der CPU- und Speicherauslastung finden Sie in den Anweisungen für"Verabreichung" ,"Überwachung" , Und"Upgrade" StorageGRID.

Wenn Hyperthreading auf den zugrunde liegenden physischen Hosts aktiviert ist, können Sie 8 virtuelle Kerne (4 physische Kerne) pro Knoten bereitstellen. Wenn Hyperthreading auf den zugrunde liegenden physischen Hosts nicht aktiviert ist, müssen Sie 8 physische Kerne pro Knoten bereitstellen.

Wenn Sie virtuelle Maschinen als Hosts verwenden und die Kontrolle über die Größe und Anzahl der VMs haben, sollten Sie für jeden StorageGRID Knoten eine einzelne VM verwenden und die VM entsprechend dimensionieren.

Bei Produktionsbereitstellungen sollten Sie nicht mehrere Speicherknoten auf derselben physischen Speicherhardware oder demselben virtuellen Host ausführen. Jeder Speicherknoten in einer einzelnen StorageGRID Bereitstellung sollte sich in seiner eigenen isolierten Fehlerdomäne befinden. Sie können die Haltbarkeit und Verfügbarkeit von Objektdaten maximieren, wenn Sie sicherstellen, dass ein einzelner Hardwarefehler nur einen einzelnen Speicherknoten beeinträchtigen kann.

Siehe auch "Speicher- und Leistungsanforderungen".

Speicher- und Leistungsanforderungen

Sie müssen die Speicheranforderungen für StorageGRID -Knoten verstehen, damit Sie genügend Speicherplatz für die Erstkonfiguration und zukünftige Speichererweiterungen bereitstellen können.

StorageGRID -Knoten erfordern drei logische Speicherkategorien:

- **Containerpool** – Leistungsstarker Speicher (10K SAS oder SSD) für die Knotencontainer, der dem Speichertreiber der Container-Engine zugewiesen wird, wenn Sie die Container-Engine auf den Hosts installieren und konfigurieren, die Ihre StorageGRID Knoten unterstützen.
- **Systemdaten** – Performance-Tier-Speicher (10K SAS oder SSD) für die dauerhafte Speicherung von Systemdaten und Transaktionsprotokollen pro Knoten, die von den StorageGRID Hostdiensten genutzt und einzelnen Knoten zugeordnet werden.
- **Objektdaten** – Speicher der Leistungsstufe (10K SAS oder SSD) und Massenspeicher der Kapazitätsstufe (NL-SAS/SATA) für die dauerhafte Speicherung von Objektdaten und Objektmetadaten.

Sie müssen für alle Speicherkategorien RAID-gestützte Blockgeräte verwenden. Nicht redundante Festplatten, SSDs oder JBODs werden nicht unterstützt. Sie können für jede Speicherkategorie gemeinsam genutzten oder lokalen RAID-Speicher verwenden. Wenn Sie jedoch die Knotenmigrationsfunktion in StorageGRID verwenden möchten, müssen Sie sowohl Systemdaten als auch Objektdaten auf gemeinsam genutztem Speicher speichern. Weitere Informationen finden Sie unter "Anforderungen für die Migration von Knotencontainern" .

Leistungsanforderungen

Die Leistung der für den Containerpool, die Systemdaten und die Objektmetadaten verwendeten Volumes hat erhebliche Auswirkungen auf die Gesamtleistung des Systems. Sie sollten für diese Volumes Speicher der Leistungsstufe (10K SAS oder SSD) verwenden, um eine angemessene Festplattenleistung hinsichtlich Latenz, Eingabe-/Ausgabevorgängen pro Sekunde (IOPS) und Durchsatz sicherzustellen. Sie können Capacity-Tier-Speicher (NL-SAS/SATA) für die dauerhafte Speicherung von Objektdaten verwenden.

Für die für den Containerpool, die Systemdaten und die Objektdaten verwendeten Volumes muss das Write-Back-Caching aktiviert sein. Der Cache muss sich auf einem geschützten oder dauerhaften Medium befinden.

Anforderungen für Hosts, die NetApp ONTAP -Speicher verwenden

Wenn der StorageGRID Knoten Speicher verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass für das Volume keine FabricPool -Tiering-Richtlinie aktiviert ist. Das Deaktivieren der FabricPool Tiering-Funktion für Volumes, die mit StorageGRID -Knoten verwendet werden, vereinfacht die Fehlerbehebung und Speichervorgänge.

Verwenden Sie FabricPool niemals, um Daten im Zusammenhang mit StorageGRID zurück auf StorageGRID selbst zu verschieben. Das Zurückführen von StorageGRID -Daten in StorageGRID erhöht die Fehlerbehebung und die Betriebskomplexität.

Anzahl der benötigten Hosts

Jeder StorageGRID Standort benötigt mindestens drei Speicherknoten.

Führen Sie bei einer Produktionsbereitstellung nicht mehr als einen Speicherknoten auf einem einzelnen physischen oder virtuellen Host aus. Durch die Verwendung eines dedizierten Hosts für jeden Speicherknoten wird eine isolierte Fehlerdomäne bereitgestellt.

Andere Knotentypen, wie etwa Admin-Knoten oder Gateway-Knoten, können auf denselben Hosts oder je nach Bedarf auf eigenen dedizierten Hosts bereitgestellt werden.

Anzahl der Speichervolumes für jeden Host

Die folgende Tabelle zeigt die Anzahl der für jeden Host erforderlichen Speichervolumes (LUNs) und die für jede LUN erforderliche Mindestgröße, basierend darauf, welche Knoten auf diesem Host bereitgestellt werden.

Die maximal getestete LUN-Größe beträgt 39 TB.

Diese Zahlen gelten für jeden Host, nicht für das gesamte Grid.

LUN-Zweck	Speicherkategorie	Anzahl der LUNs	Mindestgröße/LUN
Container-Engine-Speicherpool	Containerpool	1	Gesamtzahl der Knoten × 100 GB
`/var/local`Volumen	Systemdaten	1 für jeden Knoten auf diesem Host	90 GB
Speicherknoten	Objektdaten	3 für jeden Speicherknoten auf diesem Host **Hinweis:** Ein softwarebasierter Speicherknoten kann 1 bis 48 Speichervolumes haben; mindestens 3 Speichervolumes werden empfohlen.	12 TB (4 TB/LUN) SieheSpeicheranforderungen für Speicherknoten für weitere Informationen.

LUN-Zweck	Speicherkategorie	Anzahl der LUNs	Mindestgröße/LUN
Speicherknoten (nur Metadaten)	Objektmetadaten	1	4 TB SieheSpeicheranforderungen für Speicherknoten für weitere Informationen. **Hinweis**: Für reine Metadaten-Speicherknoten ist nur eine Rangedb erforderlich.
Audit-Protokolle des Admin-Knotens	Systemdaten	1 für jeden Admin-Knoten auf diesem Host	200 GB
Admin-Knotentabellen	Systemdaten	1 für jeden Admin-Knoten auf diesem Host	200 GB

Abhängig von der konfigurierten Prüfebene, der Größe der Benutzereingaben wie dem S3-Objektschlüsselnamen und der Menge der zu bewahrenden Prüfprotokolldaten müssen Sie möglicherweise die Größe der Prüfprotokoll-LUN auf jedem Admin-Knoten erhöhen. Im Allgemeinen generiert ein Grid ungefähr 1 KB Prüfdaten pro S3-Vorgang, was bedeuten würde, dass ein 200 GB großes LUN 70 Millionen Vorgänge pro Tag oder 800 Vorgänge pro Sekunde für zwei bis drei Tage unterstützen würde.

Mindestspeicherplatz für einen Host

Die folgende Tabelle zeigt den für jeden Knotentyp erforderlichen Mindestspeicherplatz. Mithilfe dieser Tabelle können Sie die Mindestspeichermenge ermitteln, die Sie dem Host in jeder Speicherkategorie bereitstellen müssen, basierend darauf, welche Knoten auf diesem Host bereitgestellt werden.

Festplatten-Snapshots können nicht zum Wiederherstellen von Grid-Knoten verwendet werden. Beziehen Sie sich stattdessen auf die"Wiederherstellung von Grid-Knoten" Verfahren für jeden Knotentyp.

Knotentyp	Containerpool	Systemdaten	Objektdaten
Speicherknoten	100 GB	90 GB	4.000 GB
Admin-Knoten	100 GB	490 GB (3 LUNs)	*nicht zutreffend*
Gateway-Knoten	100 GB	90 GB	*nicht zutreffend*

Beispiel: Berechnung des Speicherbedarfs für einen Host

Angenommen, Sie planen, drei Knoten auf demselben Host bereitzustellen: einen Speicherknoten, einen Admin-Knoten und einen Gateway-Knoten. Sie sollten dem Host mindestens neun Speichervolumes zur Verfügung stellen. Sie benötigen mindestens 300 GB Performance-Tier-Speicher für die Knotencontainer, 670 GB Performance-Tier-Speicher für Systemdaten und Transaktionsprotokolle und 12 TB Capacity-Tier-Speicher

für Objektdaten.

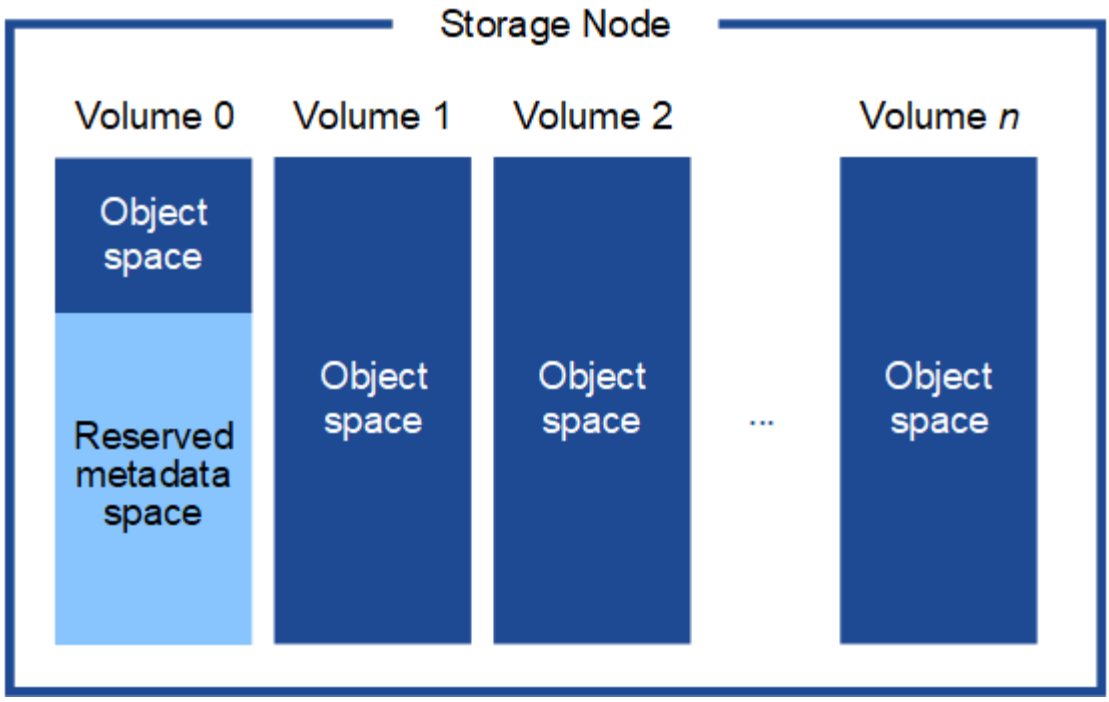
Knotentyp	LUN-Zweck	Anzahl der LUNs	LUN-Größe
Speicherknoten	Container-Engine-Speicherpool	1	300 GB (100 GB/Knoten)
Speicherknoten	`/var/local`Volumen	1	90 GB
Speicherknoten	Objektdaten	3	12 TB (4 TB/LUN)
Admin-Knoten	`/var/local`Volumen	1	90 GB
Admin-Knoten	Audit-Protokolle des Admin-Knotens	1	200 GB
Admin-Knoten	Admin-Knotentabellen	1	200 GB
Gateway-Knoten	`/var/local`Volumen	1	90 GB
Gesamt		**9**	**Containerpool:** 300 GB **Systemdaten:** 670 GB **Objektdaten:** 12.000 GB

Speicheranforderungen für Speicherknoten

Ein softwarebasierter Speicherknoten kann 1 bis 48 Speichervolumes haben; 3 oder mehr Speichervolumes werden empfohlen. Jedes Speichervolumen sollte mindestens 4 TB groß sein.

Ein Appliance-Speicherknoten kann außerdem über bis zu 48 Speichervolumes verfügen.

Wie in der Abbildung gezeigt, reserviert StorageGRID Speicherplatz für Objektmetadaten auf Speichervolume 0 jedes Speicherknotens. Der verbleibende Speicherplatz auf Speichervolume 0 und allen anderen Speichervolumes im Speicherknoten wird ausschließlich für Objektdaten verwendet.



Um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen, speichert StorageGRID an jedem Standort drei Kopien der Metadaten für alle Objekte im System. Die drei Kopien der Objektmetadaten werden gleichmäßig auf alle Speicherknoten an jedem Standort verteilt.

Wenn Sie ein Grid mit reinen Metadaten-Speicherknoten installieren, muss das Grid auch eine Mindestanzahl von Knoten für die Objektspeicherung enthalten. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

- Für ein Single-Site-Grid werden mindestens zwei Storage Nodes für Objekte und Metadaten konfiguriert.
- Für ein Multi-Site-Grid wird mindestens ein Storage Node pro Site für Objekte und Metadaten konfiguriert.

Wenn Sie dem Datenträger 0 eines neuen Speicherknotens Speicherplatz zuweisen, müssen Sie sicherstellen, dass für den Teil aller Objektmetadaten dieses Knotens ausreichend Speicherplatz vorhanden ist.

- Sie müssen dem Volume 0 mindestens 4 TB zuweisen.

  Wenn Sie für einen Speicherknoten nur ein Speichervolume verwenden und dem Volume 4 TB oder weniger zuweisen, wechselt der Speicherknoten beim Start möglicherweise in den schreibgeschützten Speicherzustand und speichert nur Objektmetadaten.

  Wenn Sie Volume 0 (nur für nicht produktive Verwendung) weniger als 500 GB zuweisen, werden 10 % der Kapazität des Speichervolumes für Metadaten reserviert.

- Softwarebasierte Knotenressourcen, die nur Metadaten enthalten, müssen mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:
  - Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
    - 128 GB RAM
    - 8-Kern-CPU
    - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)

    - Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).

      Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

- Wenn Sie ein neues System (StorageGRID 11.6 oder höher) installieren und jeder Speicherknoten über 128 GB oder mehr RAM verfügt, weisen Sie Volume 0 8 TB oder mehr zu. Durch die Verwendung eines größeren Werts für Volume 0 kann der für Metadaten auf jedem Speicherknoten zulässige Speicherplatz erhöht werden.
- Wenn Sie verschiedene Speicherknoten für eine Site konfigurieren, verwenden Sie nach Möglichkeit dieselbe Einstellung für Volume 0. Wenn eine Site Speicherknoten unterschiedlicher Größe enthält, bestimmt der Speicherknoten mit dem kleinsten Volume 0 die Metadatenkapazität dieser Site.

Weitere Informationen finden Sie unter"Verwalten des Objektmetadatenspeichers" .

Anforderungen für die Migration von Knotencontainern

Mit der Knotenmigrationsfunktion können Sie einen Knoten manuell von einem Host auf einen anderen verschieben. Normalerweise befinden sich beide Hosts im selben physischen Rechenzentrum.

Durch die Knotenmigration können Sie die Wartung physischer Hosts durchführen, ohne den Grid-Betrieb zu unterbrechen. Sie verschieben alle StorageGRID -Knoten einzeln auf einen anderen Host, bevor Sie den physischen Host offline nehmen. Die Migration von Knoten erfordert nur eine kurze Ausfallzeit für jeden Knoten und sollte den Betrieb oder die Verfügbarkeit von Grid-Diensten nicht beeinträchtigen.

Wenn Sie die StorageGRID -Knotenmigrationsfunktion verwenden möchten, muss Ihre Bereitstellung zusätzliche Anforderungen erfüllen:

- Einheitliche Netzwerkschnittstellennamen für alle Hosts in einem einzigen physischen Rechenzentrum
- Gemeinsam genutzter Speicher für StorageGRID -Metadaten und Objekt-Repository-Volumes, auf den alle Hosts in einem einzigen physischen Rechenzentrum zugreifen können. Sie könnten beispielsweise Speicher-Arrays der NetApp E-Serie verwenden.

Wenn Sie virtuelle Hosts verwenden und die zugrunde liegende Hypervisor-Schicht die VM-Migration unterstützt, möchten Sie diese Funktion möglicherweise anstelle der Knotenmigrationsfunktion in StorageGRID verwenden. In diesem Fall können Sie diese zusätzlichen Anforderungen ignorieren.

Fahren Sie die Knoten ordnungsgemäß herunter, bevor Sie eine Migration oder Hypervisor-Wartung durchführen. Siehe die Anweisungen für"Herunterfahren eines Netzknotens" .

VMware Live Migration wird nicht unterstützt

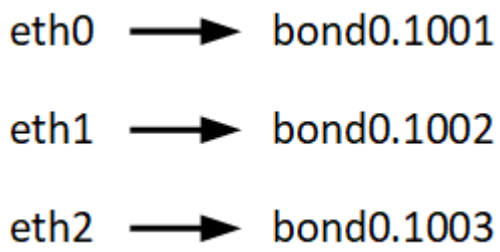
Bei der Durchführung einer Bare-Metal-Installation auf VMware-VMs führen OpenStack Live Migration und VMware Live vMotion dazu, dass die Uhrzeit der virtuellen Maschine springt, und werden für Grid-Knoten jeglicher Art nicht unterstützt. Obwohl es selten vorkommt, können falsche Uhrzeiten zum Verlust von Daten oder Konfigurationsaktualisierungen führen.

Kaltmigration wird unterstützt. Bei der Kaltmigration fahren Sie die StorageGRID -Knoten herunter, bevor Sie sie zwischen Hosts migrieren. Siehe die Anweisungen für"Herunterfahren eines Netzknotens" .

Konsistente Netzwerkschnittstellennamen

Um einen Knoten von einem Host auf einen anderen zu verschieben, muss der StorageGRID Hostdienst ein gewisses Vertrauen darin haben, dass die externe Netzwerkkonnektivität, über die der Knoten an seinem aktuellen Standort verfügt, am neuen Standort dupliziert werden kann. Diese Zuverlässigkeit wird durch die Verwendung konsistenter Netzwerkschnittstellennamen in den Hosts erreicht.

Nehmen wir beispielsweise an, dass StorageGRID NodeA, das auf Host1 ausgeführt wird, mit den folgenden Schnittstellenzuordnungen konfiguriert wurde:



Die linke Seite der Pfeile entspricht den herkömmlichen Schnittstellen, wie sie innerhalb eines StorageGRID Containers angezeigt werden (d. h. jeweils den Schnittstellen Grid, Admin und Client Network). Die rechte Seite der Pfeile entspricht den tatsächlichen Hostschnittstellen, die diese Netzwerke bereitstellen. Dabei handelt es sich um drei VLAN-Schnittstellen, die derselben physischen Schnittstellenverbindung untergeordnet sind.

Nehmen wir nun an, Sie möchten NodeA auf Host2 migrieren. Wenn Host2 auch über Schnittstellen mit den Namen bond0.1001, bond0.1002 und bond0.1003 verfügt, lässt das System die Verschiebung zu, da davon ausgegangen wird, dass die gleichnamigen Schnittstellen auf Host2 dieselbe Konnektivität bieten wie auf Host1. Wenn Host2 keine Schnittstellen mit denselben Namen hat, wird die Verschiebung nicht zugelassen.

Es gibt viele Möglichkeiten, eine konsistente Benennung der Netzwerkschnittstellen über mehrere Hosts hinweg zu erreichen. Siehe"Konfigurieren des Hostnetzwerks" für einige Beispiele.

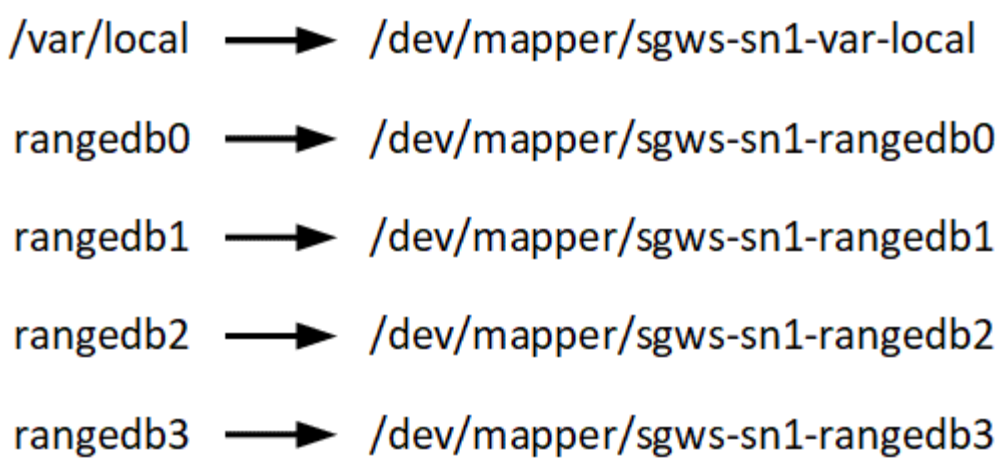
Gemeinsam genutzter Speicher

Um schnelle Knotenmigrationen mit geringem Overhead zu erreichen, verschiebt die StorageGRID Knotenmigrationsfunktion die Knotendaten nicht physisch. Stattdessen wird die Knotenmigration wie folgt als Paar von Export- und Importvorgängen durchgeführt:

1. Während des Vorgangs „Knotenexport“ wird eine kleine Menge persistenter Statusdaten aus dem auf HostA ausgeführten Knotencontainer extrahiert und auf dem Systemdatenvolume dieses Knotens zwischengespeichert. Anschließend wird der Knotencontainer auf HostA deinstanziiert.
2. Während des Vorgangs „Knotenimport“ wird der Knotencontainer auf HostB instanziiert, der dieselbe Netzwerkschnittstelle und dieselben Blockspeicherzuordnungen verwendet, die auf HostA wirksam waren. Anschließend werden die zwischengespeicherten persistenten Statusdaten in die neue Instanz eingefügt.

Bei diesem Betriebsmodus müssen alle Systemdaten und Objektspeichervolumes des Knotens sowohl von HostA als auch von HostB aus zugänglich sein, damit die Migration zulässig ist und funktioniert. Darüber hinaus müssen sie mit Namen in den Knoten abgebildet worden sein, die garantiert auf dieselben LUNs auf HostA und HostB verweisen.

Das folgende Beispiel zeigt eine Lösung für die Blockgerätezuordnung für einen StorageGRID Speicherknoten, bei dem DM-Multipathing auf den Hosts verwendet wird und das Alias-Feld in `/etc/multipath.conf` um konsistente, benutzerfreundliche Blockgerätenamen bereitzustellen, die auf allen Hosts verfügbar sind.



Vorbereiten der Hosts (Red Hat)

So ändern sich hostweite Einstellungen während der Installation

Auf Bare-Metal-Systemen nimmt StorageGRID einige Änderungen an hostweiten `sysctl` Einstellungen.

Folgende Änderungen werden vorgenommen:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
```

```
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
```

```
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Installieren Sie Linux

Sie müssen StorageGRID auf allen Red Hat Enterprise Linux Grid-Hosts installieren. Eine Liste der unterstützten Versionen erhalten Sie mit dem NetApp Interoperability Matrix Tool.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr Betriebssystem die unten aufgeführten Mindestanforderungen an die Kernelversion von StorageGRID erfüllt. Verwenden Sie den Befehl `uname -r` um die Kernelversion Ihres Betriebssystems zu erhalten, oder wenden Sie sich an den Anbieter Ihres Betriebssystems.

Red Hat Enterprise Linux-Version	Mindestkernelversion	Name des Kernelpakets
8.8 (veraltet)	4.18.0-477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8,10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0 (veraltet)	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9.2 (veraltet)	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9,4	5.14.0-427.18.1.el9_4.x86_64	kernel-5.14.0-427.18.1.el9_4.x86_64
9,6	5.14.0-570.18.1.el9_6.x86_64	kernel-5.14.0-570.18.1.el9_6.x86_64

Schritte

1. Installieren Sie Linux auf allen physischen oder virtuellen Grid-Hosts gemäß den Anweisungen des Distributors oder Ihrem Standardverfahren.

   > ⓘ Wenn Sie das Standard-Linux-Installationsprogramm verwenden, wählen Sie die Softwarekonfiguration „Compute Node“ (falls verfügbar) oder die Basisumgebung „Minimalinstallation“. Installieren Sie keine grafischen Desktopumgebungen.

2. Stellen Sie sicher, dass alle Hosts Zugriff auf die Paket-Repositorys haben, einschließlich des Extras-Kanals.

   Möglicherweise benötigen Sie diese zusätzlichen Pakete später in diesem Installationsvorgang.

3. Wenn Swap aktiviert ist:

   a. Führen Sie den folgenden Befehl aus: `$ sudo swapoff --all`

   b. Entfernen Sie alle Swap-Einträge aus `/etc/fstab` um die Einstellungen beizubehalten.

Wenn Sie den Swap-Vorgang nicht vollständig deaktivieren, kann dies zu erheblichen Leistungseinbußen führen.

Konfigurieren des Hostnetzwerks (Red Hat Enterprise Linux)

Nachdem Sie die Linux-Installation auf Ihren Hosts abgeschlossen haben, müssen Sie möglicherweise einige zusätzliche Konfigurationen durchführen, um auf jedem Host eine Reihe von Netzwerkschnittstellen vorzubereiten, die für die Zuordnung zu den StorageGRID -Knoten geeignet sind, die Sie später bereitstellen.

Bevor Sie beginnen

- Sie haben die"StorageGRID Netzwerkrichtlinien" .
- Sie haben die Informationen zu"Anforderungen für die Migration von Knotencontainern" .
- Wenn Sie virtuelle Hosts verwenden, haben Sie dieÜberlegungen und Empfehlungen zum Klonen von MAC-Adressen bevor Sie das Hostnetzwerk konfigurieren.

Wenn Sie VMs als Hosts verwenden, sollten Sie VMXNET 3 als virtuellen Netzwerkadapter auswählen. Der VMware E1000-Netzwerkadapter hat Verbindungsprobleme mit StorageGRID -Containern verursacht, die auf bestimmten Linux-Distributionen bereitgestellt wurden.

Informationen zu diesem Vorgang

Grid-Knoten müssen auf das Grid-Netzwerk und optional auf die Admin- und Client-Netzwerke zugreifen können. Sie stellen diesen Zugriff bereit, indem Sie Zuordnungen erstellen, die die physische Schnittstelle des Hosts mit den virtuellen Schnittstellen für jeden Grid-Knoten verknüpfen. Verwenden Sie beim Erstellen von Hostschnittstellen benutzerfreundliche Namen, um die Bereitstellung auf allen Hosts zu erleichtern und die Migration zu ermöglichen.

Dieselbe Schnittstelle kann zwischen dem Host und einem oder mehreren Knoten gemeinsam genutzt werden. Sie können beispielsweise dieselbe Schnittstelle für den Hostzugriff und den Knotenadministrator-Netzwerkzugriff verwenden, um die Host- und Knotenwartung zu vereinfachen. Obwohl die gleiche Schnittstelle zwischen dem Host und einzelnen Knoten gemeinsam genutzt werden kann, müssen alle unterschiedliche IP-Adressen haben. IP-Adressen können nicht zwischen Knoten oder zwischen dem Host und einem Knoten geteilt werden.

Sie können dieselbe Host-Netzwerkschnittstelle verwenden, um die Grid-Netzwerkschnittstelle für alle StorageGRID -Knoten auf dem Host bereitzustellen. Sie können für jeden Knoten eine andere Host-Netzwerkschnittstelle verwenden oder einen Mittelweg wählen. Normalerweise würden Sie jedoch nicht dieselbe Host-Netzwerkschnittstelle sowohl als Grid- als auch als Admin-Netzwerkschnittstelle für einen einzelnen Knoten oder als Grid-Netzwerkschnittstelle für einen Knoten und als Client-Netzwerkschnittstelle für einen anderen bereitstellen.

Sie können diese Aufgabe auf viele Arten erledigen. Wenn es sich bei Ihren Hosts beispielsweise um virtuelle Maschinen handelt und Sie für jeden Host einen oder zwei StorageGRID Knoten bereitstellen, können Sie die richtige Anzahl von Netzwerkschnittstellen im Hypervisor erstellen und eine 1:1-Zuordnung verwenden. Wenn Sie für den Produktionseinsatz mehrere Knoten auf Bare-Metal-Hosts bereitstellen, können Sie die Unterstützung des Linux-Netzwerk-Stacks für VLAN und LACP zur Fehlertoleranz und Bandbreitenfreigabe nutzen. Die folgenden Abschnitte bieten detaillierte Ansätze für beide Beispiele. Sie müssen keines dieser Beispiele verwenden; Sie können jeden Ansatz verwenden, der Ihren Anforderungen entspricht.

Verwenden Sie Bond- oder Bridge-Geräte nicht direkt als Container-Netzwerkschnittstelle. Dies könnte den Start des Knotens verhindern, der durch ein Kernelproblem bei der Verwendung von MACVLAN mit Bond- und Bridge-Geräten im Container-Namespace verursacht wird. Verwenden Sie stattdessen ein nicht gebundenes Gerät, beispielsweise ein VLAN oder ein virtuelles Ethernet-Paar (veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Knotenkonfigurationsdatei an.

Ähnliche Informationen

"Erstellen von Knotenkonfigurationsdateien"

Überlegungen und Empfehlungen zum Klonen von MAC-Adressen

Durch das Klonen von MAC-Adressen verwendet der Container die MAC-Adresse des Hosts und der Host die MAC-Adresse einer von Ihnen angegebenen oder einer zufällig generierten Adresse. Sie sollten das Klonen von MAC-Adressen verwenden, um die Verwendung von Netzwerkkonfigurationen im Promiscuous-Modus zu vermeiden.

Aktivieren des MAC-Klonens

In bestimmten Umgebungen kann die Sicherheit durch das Klonen von MAC-Adressen verbessert werden, da Sie dadurch eine dedizierte virtuelle Netzwerkkarte für das Admin-Netzwerk, das Grid-Netzwerk und das Client-Netzwerk verwenden können. Wenn der Container die MAC-Adresse der dedizierten Netzwerkkarte auf dem Host verwendet, können Sie die Verwendung von Netzwerkkonfigurationen im Promiscuous-Modus vermeiden.

Das Klonen von MAC-Adressen ist für die Verwendung mit virtuellen Serverinstallationen vorgesehen und funktioniert möglicherweise nicht bei allen physischen Gerätekonfigurationen ordnungsgemäß.

Wenn der Start eines Knotens fehlschlägt, weil eine auf MAC-Klonen ausgerichtete Schnittstelle belegt ist, müssen Sie die Verbindung möglicherweise auf „inaktiv“ setzen, bevor Sie den Knoten starten. Darüber hinaus ist es möglich, dass die virtuelle Umgebung das MAC-Klonen auf einer Netzwerkschnittstelle verhindert, während die Verbindung aktiv ist. Wenn ein Knoten die MAC-Adresse nicht festlegen und nicht starten kann, weil eine Schnittstelle belegt ist, kann das Problem möglicherweise behoben werden, indem die Verbindung vor dem Starten des Knotens auf „inaktiv“ gesetzt wird.

Das Klonen von MAC-Adressen ist standardmäßig deaktiviert und muss über Knotenkonfigurationsschlüssel festgelegt werden. Sie sollten es aktivieren, wenn Sie StorageGRID installieren.

Für jedes Netzwerk gibt es einen Schlüssel:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Wenn Sie den Schlüssel auf „true“ setzen, verwendet der Container die MAC-Adresse der Netzwerkkarte des Hosts. Zusätzlich verwendet der Host dann die MAC-Adresse des angegebenen Containernetzwerks. Standardmäßig ist die Containeradresse eine zufällig generierte Adresse. Wenn Sie jedoch eine Adresse mit dem `_NETWORK_MAC` Knotenkonfigurationsschlüssel, wird stattdessen diese Adresse verwendet. Host und

Container haben immer unterschiedliche MAC-Adressen.

> Wenn Sie das MAC-Klonen auf einem virtuellen Host aktivieren, ohne gleichzeitig den Promiscuous-Modus auf dem Hypervisor zu aktivieren, kann dies dazu führen, dass die Linux-Host-Vernetzung über die Schnittstelle des Hosts nicht mehr funktioniert.

Anwendungsfälle für das MAC-Klonen

Beim MAC-Klonen sind zwei Anwendungsfälle zu berücksichtigen:

- MAC-Klonen nicht aktiviert: Wenn die `_CLONE_MAC` Schlüssel in der Knotenkonfigurationsdatei nicht festgelegt oder auf „false“ gesetzt ist, verwendet der Host die Host-NIC-MAC und der Container verfügt über eine von StorageGRID generierte MAC, sofern in der `_NETWORK_MAC` Schlüssel. Wenn eine Adresse im `_NETWORK_MAC` Schlüssel erhält der Container die Adresse, die im `_NETWORK_MAC` Schlüssel. Diese Tastenkonfiguration erfordert die Verwendung des Promiscuous-Modus.
- MAC-Klonen aktiviert: Wenn die `_CLONE_MAC` Schlüssel in der Knotenkonfigurationsdatei auf „true“ gesetzt ist, verwendet der Container die Host-NIC-MAC und der Host verwendet eine von StorageGRID generierte MAC, sofern in der `_NETWORK_MAC` Schlüssel. Wenn eine Adresse im `_NETWORK_MAC` Schlüssel verwendet der Host die angegebene Adresse anstelle einer generierten. Bei dieser Tastenkonfiguration sollten Sie den Promiscuous-Modus nicht verwenden.

> Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen das Empfangen und Senden von Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen erlauben möchten, stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppe für den Promiscuous-Modus, MAC-Adressänderungen und gefälschte Übertragungen auf **Akzeptieren** eingestellt sind. Die auf dem virtuellen Switch festgelegten Werte können durch die Werte auf Portgruppenebene überschrieben werden. Stellen Sie daher sicher, dass die Einstellungen an beiden Stellen identisch sind.

Informationen zum Aktivieren des MAC-Klonens finden Sie im"Anweisungen zum Erstellen von Knotenkonfigurationsdateien" .

Beispiel für MAC-Klonen

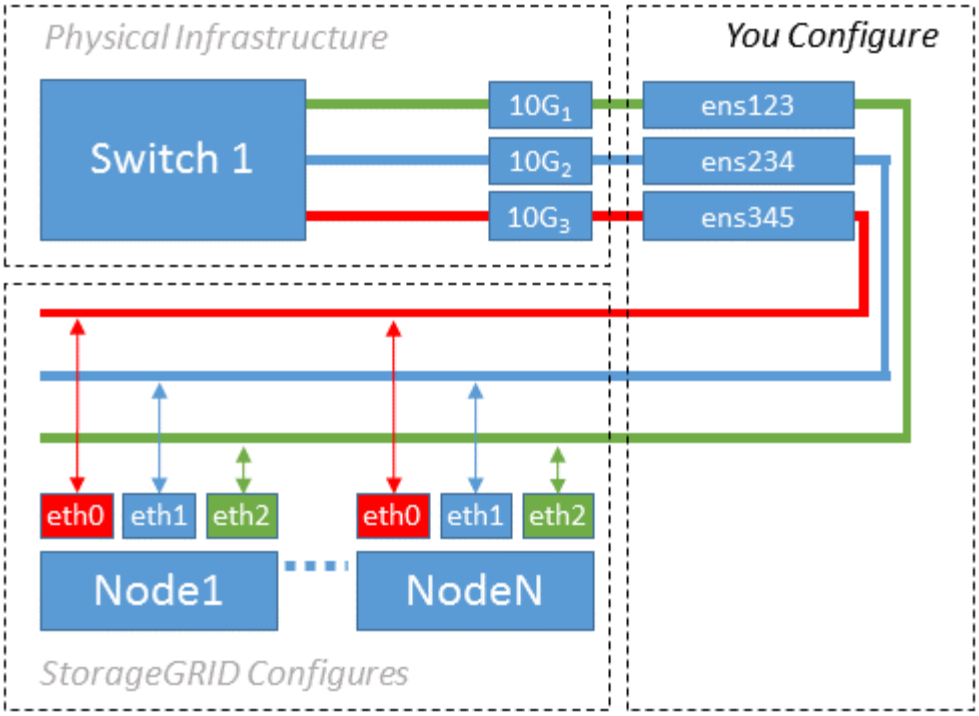
Beispiel für aktiviertes MAC-Klonen mit einem Host mit der MAC-Adresse 11:22:33:44:55:66 für die Schnittstelle ens256 und den folgenden Schlüsseln in der Knotenkonfigurationsdatei:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Ergebnis: Die Host-MAC für ens256 ist b2:9c:02:c2:27:10 und die Admin-Netzwerk-MAC ist 11:22:33:44:55:66

Beispiel 1: 1-zu-1-Zuordnung zu physischen oder virtuellen NICs

Beispiel 1 beschreibt eine einfache physische Schnittstellenzuordnung, die wenig oder keine Konfiguration auf der Hostseite erfordert.



Das Linux-Betriebssystem erstellt die `ensXYZ` Schnittstellen automatisch während der Installation oder beim Booten oder wenn die Schnittstellen im laufenden Betrieb hinzugefügt werden. Es ist keine Konfiguration erforderlich, außer sicherzustellen, dass die Schnittstellen so eingestellt sind, dass sie nach dem Booten automatisch hochgefahren werden. Sie müssen feststellen, welche `ensXYZ` entspricht welchem StorageGRID Netzwerk (Grid, Admin oder Client), sodass Sie später im Konfigurationsprozess die richtigen Zuordnungen angeben können.

Beachten Sie, dass in der Abbildung mehrere StorageGRID -Knoten dargestellt sind. Normalerweise würden Sie diese Konfiguration jedoch für VMs mit einem einzelnen Knoten verwenden.

Wenn Switch 1 ein physischer Switch ist, sollten Sie die mit den Schnittstellen 10G1 bis 10G3 verbundenen Ports für den Zugriffsmodus konfigurieren und sie in den entsprechenden VLANs platzieren.

Beispiel 2: LACP-Bindung mit VLANs

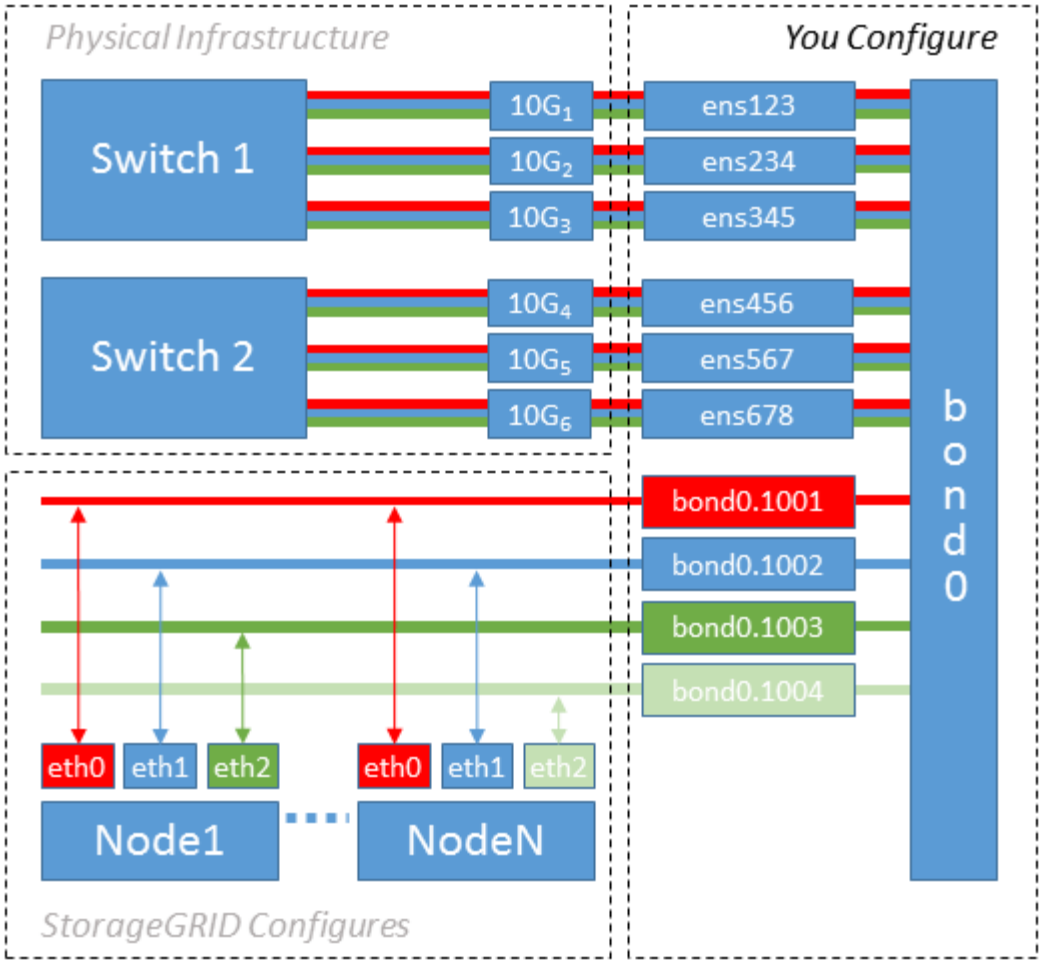
Informationen zu diesem Vorgang

Beispiel 2 setzt voraus, dass Sie mit der Bündelung von Netzwerkschnittstellen und der Erstellung von VLAN-Schnittstellen auf der von Ihnen verwendeten Linux-Distribution vertraut sind.

Beispiel 2 beschreibt ein generisches, flexibles, VLAN-basiertes Schema, das die gemeinsame Nutzung der gesamten verfügbaren Netzwerkbandbreite zwischen allen Knoten auf einem einzelnen Host ermöglicht. Dieses Beispiel ist insbesondere auf Bare-Metal-Hosts anwendbar.

Um dieses Beispiel zu verstehen, nehmen Sie an, dass Sie in jedem Rechenzentrum drei separate Subnetze für die Grid-, Admin- und Client-Netzwerke haben. Die Subnetze befinden sich auf separaten VLANs (1001, 1002 und 1003) und werden dem Host auf einem LACP-gebundenen Trunk-Port (bond0) präsentiert. Sie würden drei VLAN-Schnittstellen auf der Bindung konfigurieren: bond0.1001, bond0.1002 und bond0.1003.

Wenn Sie separate VLANs und Subnetze für Knotennetzwerke auf demselben Host benötigen, können Sie VLAN-Schnittstellen auf der Bindung hinzufügen und sie dem Host zuordnen (in der Abbildung als bond0.1004 angezeigt).



Schritte

1. Fassen Sie alle physischen Netzwerkschnittstellen, die für die StorageGRID -Netzwerkkonnektivität verwendet werden, in einer einzigen LACP-Verbindung zusammen.

   Verwenden Sie für die Bindung auf jedem Host denselben Namen. Beispiel: `bond0` .

2. Erstellen Sie VLAN-Schnittstellen, die diese Verbindung als ihr zugehöriges „physisches Gerät“ verwenden, und verwenden Sie dabei die Standard-Namenskonvention für VLAN-Schnittstellen. `physdev-name.VLAN ID` .

   Beachten Sie, dass für die Schritte 1 und 2 eine entsprechende Konfiguration der Edge-Switches erforderlich ist, die die anderen Enden der Netzwerkverbindungen abschließen. Die Edge-Switch-Ports müssen außerdem in einem LACP-Port-Kanal zusammengefasst, als Trunk konfiguriert und für die Weitergabe aller erforderlichen VLANs zugelassen werden.

   Es werden Beispiel-Schnittstellenkonfigurationsdateien für dieses Netzwerkkonfigurationsschema pro Host bereitgestellt.

Ähnliche Informationen

"Beispiel /etc/sysconfig/network-scripts"

Konfigurieren des Hostspeichers

Sie müssen jedem Host Blockspeichervolumes zuweisen.

Bevor Sie beginnen

Sie haben die folgenden Themen überprüft, die die Informationen enthalten, die Sie zum Ausführen dieser Aufgabe benötigen:

- "Speicher- und Leistungsanforderungen"
- "Anforderungen für die Migration von Knotencontainern"

Informationen zu diesem Vorgang

Verwenden Sie beim Zuweisen von Blockspeichervolumes (LUNs) zu Hosts die Tabellen unter „Speicheranforderungen“, um Folgendes zu bestimmen:

- Anzahl der für jeden Host erforderlichen Volumes (basierend auf der Anzahl und den Typen der Knoten, die auf diesem Host bereitgestellt werden)
- Speicherkategorie für jedes Volume (d. h. Systemdaten oder Objektdaten)
- Größe jedes Volumens

Sie verwenden diese Informationen sowie den von Linux jedem physischen Volume zugewiesenen persistenten Namen, wenn Sie StorageGRID Knoten auf dem Host bereitstellen.

Sie müssen keines dieser Volumes partitionieren, formatieren oder mounten. Sie müssen lediglich sicherstellen, dass sie für die Hosts sichtbar sind.

Für reine Metadaten-Speicherknoten ist nur eine Objektdaten-LUN erforderlich.

Vermeiden Sie die Verwendung von „rohen“ speziellen Gerätedateien(`/dev/sdb` , zum Beispiel), während Sie Ihre Liste mit Datenträgernamen zusammenstellen. Diese Dateien können sich bei Neustarts des Hosts ändern, was sich auf den ordnungsgemäßen Betrieb des Systems auswirkt. Wenn Sie iSCSI-LUNs und Device Mapper Multipathing verwenden, sollten Sie Multipath-Aliase in der `/dev/mapper` Verzeichnis, insbesondere wenn Ihre SAN-Topologie redundante Netzwerkpfade zum gemeinsam genutzten Speicher enthält. Alternativ können Sie die vom System erstellten Softlinks unter `/dev/disk/by-path/` für Ihre persistenten Gerätenamen.

Beispiel:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Die Ergebnisse sind bei jeder Installation unterschiedlich.

Weisen Sie jedem dieser Blockspeichervolumes benutzerfreundliche Namen zu, um die Erstinstallation von StorageGRID und zukünftige Wartungsvorgänge zu vereinfachen. Wenn Sie den Device Mapper Multipath-Treiber für den redundanten Zugriff auf gemeinsam genutzte Speichervolumes verwenden, können Sie den `alias` Feld in Ihrem `/etc/multipath.conf` Datei.

Beispiel:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Wenn Sie das Alias-Feld auf diese Weise verwenden, werden die Aliase als Blockgeräte in der `/dev/mapper` Verzeichnis auf dem Host, sodass Sie einen benutzerfreundlichen, leicht zu validierenden Namen angeben können, wenn für einen Konfigurations- oder Wartungsvorgang die Angabe eines Blockspeicher-Volumes erforderlich ist.

Wenn Sie gemeinsam genutzten Speicher einrichten, um die Migration von StorageGRID -Knoten zu unterstützen und Device Mapper Multipathing verwenden, können Sie einen gemeinsamen `/etc/multipath.conf` auf allen gemeinsam genutzten Hosts. Stellen Sie einfach sicher, dass Sie auf jedem Host ein anderes Container-Engine-Speichervolumen verwenden. Die Verwendung von Aliasnamen und die Einbeziehung des Zielhostnamens in den Alias für jede LUN des Speichervolumens der Container-Engine erleichtert das Merken und wird empfohlen.

Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt.

Ähnliche Informationen

"Konfigurieren des Speichervolumens der Container-Engine"

Konfigurieren des Speichervolumens der Container-Engine

Bevor Sie die Container-Engine (Docker oder Podman) installieren, müssen Sie möglicherweise das Speichervolume formatieren und mounten.

> Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt.

Informationen zu diesem Vorgang

Sie können diese Schritte überspringen, wenn Sie lokalen Speicher für das Docker- oder Podman-Speichervolume verwenden möchten und auf der Hostpartition ausreichend Speicherplatz verfügbar ist, der Folgendes enthält: `/var/lib/docker` für Docker und `/var/lib/containers` für Podman.

> Podman wird nur unter Red Hat Enterprise Linux (RHEL) unterstützt.

Schritte

1. Erstellen Sie ein Dateisystem auf dem Speichervolume der Container-Engine:

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. Hängen Sie das Speichervolume der Container-Engine ein:
   - Für Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

   - Für Podman:

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. Fügen Sie einen Eintrag für Container-Storage-Volume-Device zu /etc/fstab hinzu.

   Dieser Schritt stellt sicher, dass das Speichervolume nach dem Neustart des Hosts automatisch erneut bereitgestellt wird.

Docker installieren

Das StorageGRID -System läuft auf Red Hat Enterprise Linux als Sammlung von Containern. Wenn Sie sich für die Verwendung der Docker-Container-Engine entschieden haben, befolgen Sie diese Schritte, um Docker zu installieren. Ansonsten,Podman installieren .

Schritte

1. Installieren Sie Docker, indem Sie den Anweisungen für Ihre Linux-Distribution folgen.

   Wenn Docker nicht in Ihrer Linux-Distribution enthalten ist, können Sie es von der Docker-Website herunterladen.

2. Stellen Sie sicher, dass Docker aktiviert und gestartet wurde, indem Sie die folgenden beiden Befehle ausführen:

   ```
   sudo systemctl enable docker
   ```

   ```
   sudo systemctl start docker
   ```

3. Bestätigen Sie, dass Sie die erwartete Version von Docker installiert haben, indem Sie Folgendes eingeben:

   ```
   sudo docker version
   ```

   Die Client- und Serverversionen müssen 1.11.0 oder höher sein.

Podman installieren

Das StorageGRID -System läuft auf Red Hat Enterprise Linux als Sammlung von Containern. Wenn Sie sich für die Verwendung der Podman-Container-Engine entschieden haben, befolgen Sie diese Schritte, um Podman zu installieren. Ansonsten,Docker installieren .

Podman wird nur unter Red Hat Enterprise Linux (RHEL) unterstützt.

Schritte

1. Installieren Sie Podman und Podman-Docker, indem Sie den Anweisungen für Ihre Linux-Distribution folgen.

   Sie müssen bei der Installation von Podman auch das Podman-Docker-Paket installieren.

2. Bestätigen Sie, dass Sie die erwartete Version von Podman und Podman-Docker installiert haben, indem Sie Folgendes eingeben:

   ```
   sudo docker version
   ```

   Mit dem Podman-Docker-Paket können Sie Docker-Befehle verwenden.

   Die Client- und Serverversionen müssen 3.2.3 oder höher sein.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

Installieren Sie die StorageGRID Hostdienste

Sie verwenden das StorageGRID RPM-Paket, um die StorageGRID Hostdienste zu installieren.

Informationen zu diesem Vorgang

Diese Anweisungen beschreiben, wie Sie die Hostdienste aus den RPM-Paketen installieren. Alternativ können Sie die im Installationsarchiv enthaltenen DNF-Repository-Metadaten verwenden, um die RPM-Pakete remote zu installieren. Siehe die DNF-Repository-Anweisungen für Ihr Linux-Betriebssystem.

Schritte

1. Kopieren Sie die StorageGRID RPM-Pakete auf jeden Ihrer Hosts oder stellen Sie sie auf einem gemeinsam genutzten Speicher zur Verfügung.

   Platzieren Sie sie beispielsweise in der `/tmp` Verzeichnis, sodass Sie den Beispielbefehl im nächsten Schritt verwenden können.

2. Melden Sie sich bei jedem Host als Root oder mit einem Konto mit Sudo-Berechtigung an und führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
```

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
```

> Sie müssen zuerst das Images-Paket und dann das Service-Paket installieren.

> Wenn Sie die Pakete in einem anderen Verzeichnis als `/tmp` , ändern Sie den Befehl, um den von Ihnen verwendeten Pfad wiederzugeben.

Automatisieren Sie die StorageGRID -Installation auf Red Hat Enterprise Linux

Sie können die Installation des StorageGRID Hostdienstes und die Konfiguration von Grid-Knoten automatisieren.

Die Automatisierung der Bereitstellung kann in den folgenden Fällen nützlich sein:

- Sie verwenden bereits ein Standard-Orchestrierungsframework wie Ansible, Puppet oder Chef, um physische oder virtuelle Hosts bereitzustellen und zu konfigurieren.
- Sie beabsichtigen, mehrere StorageGRID Instanzen bereitzustellen.
- Sie stellen eine große, komplexe StorageGRID Instanz bereit.

Der StorageGRID Hostdienst wird von einem Paket installiert und von Konfigurationsdateien gesteuert. Sie können die Konfigurationsdateien mit einer der folgenden Methoden erstellen:

- "Erstellen Sie die Konfigurationsdateien"interaktiv während einer manuellen Installation.
- Bereiten Sie die Konfigurationsdateien im Voraus (oder programmgesteuert) vor, um eine automatisierte Installation mithilfe von Standard-Orchestrierungsframeworks zu ermöglichen, wie in diesem Artikel beschrieben.

  StorageGRID bietet optionale Python-Skripte zur Automatisierung der Konfiguration von StorageGRID -Geräten und des gesamten StorageGRID Systems (das „Grid“). Sie können diese Skripte direkt verwenden oder sie überprüfen, um zu erfahren, wie Sie die"StorageGRID Installations-REST-API" in Grid-Bereitstellungs- und Konfigurationstools, die Sie selbst entwickeln.

Automatisieren Sie die Installation und Konfiguration des StorageGRID Hostdienstes

Sie können die Installation des StorageGRID Hostdienstes mithilfe von Standard-Orchestrierungsframeworks wie Ansible, Puppet, Chef, Fabric oder SaltStack automatisieren.

Der StorageGRID -Hostdienst ist in einem RPM verpackt und wird durch Konfigurationsdateien gesteuert, die Sie im Voraus (oder programmgesteuert) vorbereiten können, um eine automatische Installation zu ermöglichen. Wenn Sie bereits ein Standard-Orchestrierungsframework zum Installieren und Konfigurieren von RHEL verwenden, sollte das Hinzufügen von StorageGRID zu Ihren Playbooks oder Rezepten unkompliziert sein.

Siehe das Beispiel für eine Ansible-Rolle und ein Playbook im `/extras` Ordner, der mit dem Installationsarchiv geliefert wird. Das Ansible Playbook zeigt, wie die `storagegrid` Die Rolle bereitet den Host vor und installiert StorageGRID auf den Zielservern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.

> Das Beispiel-Playbook enthält nicht die Schritte, die zum Erstellen von Netzwerkgeräten vor dem Starten des StorageGRID Hostdienstes erforderlich sind. Fügen Sie diese Schritte hinzu, bevor Sie das Playbook fertigstellen und verwenden.

Sie können alle Schritte zur Vorbereitung der Hosts und Bereitstellung virtueller Grid-Knoten automatisieren.

Beispiel für eine Ansible-Rolle und ein Playbook

Beispielhafte Ansible-Rolle und Playbook werden mit dem Installationsarchiv im `/extras` Ordner. Das Ansible Playbook zeigt, wie die `storagegrid` Die Rolle bereitet die Hosts vor und installiert StorageGRID auf den Zielservern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.

Die Installationsaufgaben in der bereitgestellten `storagegrid` Rollenbeispiel verwenden Sie die `ansible.builtin.dnf` Modul, um die Installation aus den lokalen RPM-Dateien oder einem Remote-Yum-Repository durchzuführen. Wenn das Modul nicht verfügbar ist oder nicht unterstützt wird, müssen Sie möglicherweise die entsprechenden Ansible-Aufgaben in den folgenden Dateien bearbeiten, um das `yum` oder `ansible.builtin.yum` Modul:

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Automatisieren Sie die Konfiguration von StorageGRID

Nach der Bereitstellung der Grid-Knoten können Sie die Konfiguration des StorageGRID Systems automatisieren.

Bevor Sie beginnen

- Den Speicherort der folgenden Dateien kennen Sie aus dem Installationsarchiv.

Dateiname	Beschreibung
configure-storagegrid.py	Python-Skript zur Automatisierung der Konfiguration
configure-storagegrid.sample.json	Beispielkonfigurationsdatei zur Verwendung mit dem Skript
configure-storagegrid.blank.json	Leere Konfigurationsdatei zur Verwendung mit dem Skript

- Sie haben eine `configure-storagegrid.json` Konfigurationsdatei. Um diese Datei zu erstellen, können Sie die Beispielkonfigurationsdatei ändern(`configure-storagegrid.sample.json`) oder die leere Konfigurationsdatei(`configure-storagegrid.blank.json`).

Informationen zu diesem Vorgang

Sie können die `configure-storagegrid.py` Python-Skript und das `configure-storagegrid.json` Konfigurationsdatei zur Automatisierung der Konfiguration Ihres StorageGRID -Systems.

Sie können das System auch mit dem Grid Manager oder der Installations-API konfigurieren.

Schritte

1. Melden Sie sich bei dem Linux-Computer an, den Sie zum Ausführen des Python-Skripts verwenden.
2. Wechseln Sie in das Verzeichnis, in das Sie das Installationsarchiv extrahiert haben.

   Beispiel:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   Wo `platform` Ist `debs` , `rpms` , oder `vsphere` .

3. Führen Sie das Python-Skript aus und verwenden Sie die von Ihnen erstellte Konfigurationsdatei.

   Beispiel:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Ergebnis

Ein Wiederherstellungspaket `.zip` Die Datei wird während des Konfigurationsprozesses generiert und in das Verzeichnis heruntergeladen, in dem Sie den Installations- und Konfigurationsprozess ausführen. Sie müssen die Wiederherstellungspaketdatei sichern, damit Sie das StorageGRID -System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Kopieren Sie es beispielsweise an einen sicheren, gesicherten Netzwerkspeicherort und an einen sicheren Cloud-Speicherort.

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

Wenn Sie angegeben haben, dass zufällige Passwörter generiert werden sollen, öffnen Sie das `Passwords.txt` und suchen Sie nach den Passwörtern, die für den Zugriff auf Ihr StorageGRID -System erforderlich sind.

```
######################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Ihr StorageGRID -System ist installiert und konfiguriert, wenn eine Bestätigungsmeldung angezeigt wird.

```
StorageGRID has been configured and installed.
```

Ähnliche Informationen

"Installation der REST-API"

Virtuelle Grid-Knoten bereitstellen (Red Hat)

Erstellen Sie Knotenkonfigurationsdateien für Red Hat Enterprise Linux-Bereitstellungen

Knotenkonfigurationsdateien sind kleine Textdateien, die die Informationen bereitstellen, die der StorageGRID Hostdienst benötigt, um einen Knoten zu starten und ihn mit den entsprechenden Netzwerk- und Blockspeicherressourcen zu verbinden. Knotenkonfigurationsdateien werden für virtuelle Knoten verwendet und nicht für Appliance-Knoten.

Speicherort für Knotenkonfigurationsdateien

Platzieren Sie die Konfigurationsdatei für jeden StorageGRID -Knoten im `/etc/storagegrid/nodes` Verzeichnis auf dem Host, auf dem der Knoten ausgeführt wird. Wenn Sie beispielsweise planen, einen Admin-Knoten, einen Gateway-Knoten und einen Storage-Knoten auf HostA auszuführen, müssen Sie drei Knotenkonfigurationsdateien in `/etc/storagegrid/nodes` auf HostA.

Sie können die Konfigurationsdateien mit einem Texteditor wie vim oder nano direkt auf jedem Host erstellen

oder sie an einem anderen Ort erstellen und auf jeden Host verschieben.

Benennung von Knotenkonfigurationsdateien

Die Namen der Konfigurationsdateien sind aussagekräftig. Das Format ist `node-name.conf` , Wo `node-name` ist ein Name, den Sie dem Knoten zuweisen. Dieser Name wird im StorageGRID Installationsprogramm angezeigt und für Knotenwartungsvorgänge wie die Knotenmigration verwendet.

Knotennamen müssen diesen Regeln entsprechen:

- Muss eindeutig sein
- Muss mit einem Buchstaben beginnen
- Kann die Zeichen A bis Z und a bis z enthalten
- Kann die Zahlen 0 bis 9 enthalten
- Kann einen oder mehrere Bindestriche (-) enthalten
- Darf nicht mehr als 32 Zeichen umfassen, ohne die `.conf` Verlängerung

Alle Dateien in `/etc/storagegrid/nodes` die diesen Namenskonventionen nicht folgen, werden vom Hostdienst nicht analysiert.

Wenn Sie für Ihr Grid eine Multi-Site-Topologie planen, könnte ein typisches Knotenbenennungsschema wie folgt aussehen:

```
site-nodetype-nodenumber.conf
```

Sie könnten beispielsweise verwenden `dc1-adm1.conf` für den ersten Admin-Knoten im Rechenzentrum 1 und `dc2-sn3.conf` für den dritten Speicherknoten im Rechenzentrum 2. Sie können jedoch jedes beliebige Schema verwenden, solange alle Knotennamen den Namensregeln entsprechen.

Inhalt einer Knotenkonfigurationsdatei

Eine Konfigurationsdatei enthält Schlüssel-/Wertpaare mit einem Schlüssel und einem Wert pro Zeile. Befolgen Sie für jedes Schlüssel-/Wertpaar die folgenden Regeln:

- Der Schlüssel und der Wert müssen durch ein Gleichheitszeichen getrennt sein(=) und optionalem Leerzeichen.
- Die Schlüssel dürfen keine Leerzeichen enthalten.
- Die Werte können eingebettete Leerzeichen enthalten.
- Vorangehende oder nachfolgende Leerzeichen werden ignoriert.

Die folgende Tabelle definiert die Werte für alle unterstützten Schlüssel. Jeder Schlüssel hat eine der folgenden Bezeichnungen:

- **Erforderlich**: Erforderlich für jeden Knoten oder für die angegebenen Knotentypen
- **Best Practice**: Optional, aber empfohlen
- **Optional**: Optional für alle Knoten

Admin-Netzwerkschlüssel

ADMIN_IP

Wert	Bezeichnung
Grid-Netzwerk-IPv4-Adresse des primären Admin-Knotens für das Grid, zu dem dieser Knoten gehört. Verwenden Sie denselben Wert, den Sie für GRID_NETWORK_IP für den Grid-Knoten mit NODE_TYPE = VM_Admin_Node und ADMIN_ROLE = Primary angegeben haben. Wenn Sie diesen Parameter weglassen, versucht der Knoten, mithilfe von mDNS einen primären Admin-Knoten zu ermitteln. "So erkennen Grid-Knoten den primären Admin-Knoten" **Hinweis**: Dieser Wert wird auf dem primären Admin-Knoten ignoriert und ist möglicherweise verboten.	Bewährte Methode

ADMIN_NETWORK_CONFIG

Wert	Bezeichnung
DHCP, STATISCH oder DEAKTIVIERT	Optional

ADMIN_NETWORK_ESL

Wert	Bezeichnung
Durch Kommas getrennte Liste von Subnetzen in CIDR-Notation, mit denen dieser Knoten über das Admin-Netzwerk-Gateway kommunizieren soll. Beispiel: `172.16.0.0/21,172.17.0.0/21`	Optional

ADMIN_NETWORK_GATEWAY

Wert	Bezeichnung

IPv4-Adresse des lokalen Admin-Netzwerk-Gateways für diesen Knoten. Muss sich im durch ADMIN_NETWORK_IP und ADMIN_NETWORK_MASK definierten Subnetz befinden. Dieser Wert wird für DHCP-konfigurierte Netzwerke ignoriert.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn `ADMIN_NETWORK_ESL` angegeben ist. Andernfalls optional.

ADMIN_NETWORK_IP

Wert	Bezeichnung

IPv4-Adresse dieses Knotens im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC.
	
	Andernfalls optional.

ADMIN_NETWORK_MAC

Wert	Bezeichnung
Die MAC-Adresse für die Admin-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn es weggelassen wird, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Paaren hexadezimaler Ziffern bestehen, die durch Doppelpunkte getrennt sind. Beispiel: `b2:9c:02:c2:27:10`	Optional

ADMIN_NETWORK_MASK

Wert	Bezeichnung

IPv4-Netzmaske für diesen Knoten im Admin-Netzwerk. Geben Sie diesen Schlüssel an, wenn ADMIN_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Erforderlich, wenn ADMIN_NETWORK_IP angegeben ist und ADMIN_NETWORK_CONFIG = STATIC.
	
	Andernfalls optional.

ADMIN_NETWORK_MTU

Wert	Bezeichnung

Die maximale Übertragungseinheit (MTU) für diesen Knoten im Admin-Netzwerk. Nicht angeben, wenn ADMIN_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1500 verwendet.
 	
Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei.
 	
WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Knoten verbunden ist. Andernfalls kann es zu Problemen mit der Netzwerkleistung oder zu Paketverlusten kommen.
 	
Beispiele:
 	
`1500`
 	
`8192`
	Optional

ADMIN_NETWORK_TARGET

Wert	Bezeichnung

Name des Hostgeräts, das Sie für den Admin-Netzwerkzugriff durch den StorageGRID -Knoten verwenden. Es werden nur Netzwerkschnittstellennamen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den, der für GRID_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegeben wurde.
 	
Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) über dem Bond-Gerät oder verwenden Sie ein Bridge- und Virtual-Ethernet-Paar (veth).
 	
Best Practice: Geben Sie einen Wert an, auch wenn dieser Knoten zunächst keine Admin-Netzwerk-IP-Adresse hat. Dann können Sie später eine Admin-Netzwerk-IP-Adresse hinzufügen, ohne den Knoten auf dem Host neu konfigurieren zu müssen.
 	
Beispiele:
 	
`bond0.1002`
 	
`ens256`
	Bewährte Methode

ADMIN_NETWORK_TARGET_TYPE

Wert	Bezeichnung
Schnittstelle (Dies ist der einzige unterstützte Wert.)	Optional

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Wert	Bezeichnung
Wahr oder Falsch Setzen Sie den Schlüssel auf „true“, damit der StorageGRID -Container die MAC-Adresse der Host-Zielschnittstelle im Admin-Netzwerk verwendet. **Best Practice:** Verwenden Sie in Netzwerken, in denen der Promiscuous-Modus erforderlich wäre, stattdessen den Schlüssel ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Weitere Einzelheiten zum MAC-Klonen: • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red Hat Enterprise Linux)" • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"	Bewährte Methode

ADMIN_ROLE

Wert	Bezeichnung
Primär oder nicht primär Dieser Schlüssel ist nur erforderlich, wenn NODE_TYPE = VM_Admin_Node; geben Sie ihn nicht für andere Knotentypen an.	Erforderlich, wenn NODE_TYPE = VM_Admin_Node Andernfalls optional.

Geräteschlüssel sperren

BLOCK_DEVICE_AUDIT_LOGS

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten zur dauerhaften Speicherung von Prüfprotokollen verwendet.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Erforderlich für Knoten mit NODE_TYPE = VM_Admin_Node. Geben Sie es nicht für andere Knotentypen an.

BLOCK_DEVICE_RANGEDB_nnn

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten für die dauerhafte Objektspeicherung verwendet. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Storage_Node erforderlich. Geben Sie ihn nicht für andere Knotentypen an.
 	
Nur BLOCK_DEVICE_RANGEDB_000 ist erforderlich, der Rest ist optional. Das für BLOCK_DEVICE_RANGEDB_000 angegebene Blockgerät muss mindestens 4 TB groß sein, die anderen können kleiner sein.
 	
Lassen Sie keine Lücken. Wenn Sie BLOCK_DEVICE_RANGEDB_005 angeben, müssen Sie auch BLOCK_DEVICE_RANGEDB_004 angeben.
 	
Hinweis: Aus Kompatibilitätsgründen mit vorhandenen Bereitstellungen werden für aktualisierte Knoten zweistellige Schlüssel unterstützt.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Erforderlich:
	
	BLOCK_DEVICE_RANGEDB_000
	
	Optional:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

BLOCK_DEVICE_TABLES

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten zur dauerhaften Speicherung von Datenbanktabellen verwendet. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Admin_Node erforderlich. Geben Sie ihn nicht für andere Knotentypen an.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Erforderlich

BLOCK_DEVICE_VAR_LOCAL

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten für seine `/var/local` dauerhafter Speicher.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Erforderlich

Client-Netzwerkschlüssel

CLIENT_NETWORK_CONFIG

Wert	Bezeichnung
DHCP, STATISCH oder DEAKTIVIERT	Optional

CLIENT_NETWORK_GATEWAY

Wert	Bezeichnung

IPv4-Adresse des lokalen Client-Netzwerk-Gateways für diesen Knoten, das sich im durch CLIENT_NETWORK_IP und CLIENT_NETWORK_MASK definierten Subnetz befinden muss. Dieser Wert wird für DHCP-konfigurierte Netzwerke ignoriert.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Optional

CLIENT_NETWORK_IP

Wert	Bezeichnung

IPv4-Adresse dieses Knotens im Client-Netzwerk.
 	
Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC
	
	Andernfalls optional.

CLIENT_NETWORK_MAC

Wert	Bezeichnung
Die MAC-Adresse für die Client-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn es weggelassen wird, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Paaren hexadezimaler Ziffern bestehen, die durch Doppelpunkte getrennt sind. Beispiel: `b2:9c:02:c2:27:20`	Optional

CLIENT_NETWORK_MASK

Wert	Bezeichnung

IPv4-Netzmaske für diesen Knoten im Client-Netzwerk.
 	
Geben Sie diesen Schlüssel an, wenn CLIENT_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Erforderlich, wenn CLIENT_NETWORK_IP angegeben ist und CLIENT_NETWORK_CONFIG = STATIC
	
	Andernfalls optional.

CLIENT_NETWORK_MTU

Wert	Bezeichnung

Die maximale Übertragungseinheit (MTU) für diesen Knoten im Client-Netzwerk. Nicht angeben, wenn CLIENT_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1500 verwendet.
 	
Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei.
 	
WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Knoten verbunden ist. Andernfalls kann es zu Problemen mit der Netzwerkleistung oder zu Paketverlusten kommen.
 	
Beispiele:
 	
`1500`
 	
`8192`
	Optional

CLIENT_NETWORK_TARGET

Wert	Bezeichnung

Name des Hostgeräts, das Sie für den Client-Netzwerkzugriff durch den StorageGRID -Knoten verwenden. Es werden nur Netzwerkschnittstellennamen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den, der für GRID_NETWORK_TARGET oder ADMIN_NETWORK_TARGET angegeben wurde.
 	
Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) über dem Bond-Gerät oder verwenden Sie ein Bridge- und Virtual-Ethernet-Paar (veth).
 	
Best Practice: Geben Sie einen Wert an, auch wenn dieser Knoten zunächst keine Client-Netzwerk-IP-Adresse hat. Dann können Sie später eine Client-Netzwerk-IP-Adresse hinzufügen, ohne den Knoten auf dem Host neu konfigurieren zu müssen.
 	
Beispiele:
 	
`bond0.1003`
 	
`ens423`
	Bewährte Methode

CLIENT_NETWORK_TARGET_TYPE

Wert	Bezeichnung
Schnittstelle (Dies ist der einzige unterstützte Wert.)	Optional

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Wert	Bezeichnung
Wahr oder Falsch Setzen Sie den Schlüssel auf „true“, damit der StorageGRID Container die MAC-Adresse der Host-Zielschnittstelle im Client-Netzwerk verwendet. **Best Practice:** Verwenden Sie in Netzwerken, in denen der Promiscuous-Modus erforderlich wäre, stattdessen den Schlüssel CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Weitere Einzelheiten zum MAC-Klonen: • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red Hat Enterprise Linux)" • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"	Bewährte Methode

Grid-Netzwerkschlüssel

GRID_NETWORK_CONFIG

Wert	Bezeichnung
STATISCH oder DHCP Der Standardwert ist STATIC, wenn nicht anders angegeben.	Bewährte Methode

GRID_NETWORK_GATEWAY

Wert	Bezeichnung
IPv4-Adresse des lokalen Grid-Netzwerk-Gateways für diesen Knoten, das sich im durch GRID_NETWORK_IP und GRID_NETWORK_MASK definierten Subnetz befinden muss. Dieser Wert wird für DHCP-konfigurierte Netzwerke ignoriert. Wenn das Grid-Netzwerk ein einzelnes Subnetz ohne Gateway ist, verwenden Sie entweder die Standard-Gateway-Adresse für das Subnetz (XYZ1) oder den GRID_NETWORK_IP-Wert dieses Knotens. Beide Werte vereinfachen mögliche zukünftige Erweiterungen des Grid-Netzwerks.	Erforderlich

GRID_NETWORK_IP

Wert	Bezeichnung

IPv4-Adresse dieses Knotens im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn GRID_NETWORK_CONFIG = STATIC
	
	Andernfalls optional.

GRID_NETWORK_MAC

Wert	Bezeichnung
Die MAC-Adresse für die Grid-Netzwerkschnittstelle im Container. Muss aus 6 Paaren hexadezimaler Ziffern bestehen, die durch Doppelpunkte getrennt sind. Beispiel: `b2:9c:02:c2:27:30`	Optional Wenn es weggelassen wird, wird automatisch eine MAC-Adresse generiert.

GRID_NETWORK_MASK

Wert	Bezeichnung

IPv4-Netzmaske für diesen Knoten im Grid-Netzwerk. Geben Sie diesen Schlüssel an, wenn GRID_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Erforderlich, wenn GRID_NETWORK_IP angegeben ist und GRID_NETWORK_CONFIG = STATIC.
	
	Andernfalls optional.

GRID_NETWORK_MTU

Wert	Bezeichnung

Die maximale Übertragungseinheit (MTU) für diesen Knoten im Grid-Netzwerk. Nicht angeben, wenn GRID_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1500 verwendet.
 	
Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei.
 	
WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Knoten verbunden ist. Andernfalls kann es zu Problemen mit der Netzwerkleistung oder zu Paketverlusten kommen.
 	
WICHTIG: Für die beste Netzwerkleistung sollten alle Knoten mit ähnlichen MTU-Werten auf ihren Grid-Netzwerkschnittstellen konfiguriert werden. Die Warnung **MTU-Fehlanpassung des Grid-Netzwerks** wird ausgelöst, wenn es bei den MTU-Einstellungen für das Grid-Netzwerk auf einzelnen Knoten einen signifikanten Unterschied gibt. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.
 	
Beispiele:
 	
`1500`
 	
`8192`
	Optional

GRID_NETWORK_TARGET

Wert	Bezeichnung

Name des Hostgeräts, das Sie für den Grid-Netzwerkzugriff durch den StorageGRID -Knoten verwenden. Es werden nur Netzwerkschnittstellennamen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den, der für ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegeben wurde.
 	
Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) über dem Bond-Gerät oder verwenden Sie ein Bridge- und Virtual-Ethernet-Paar (veth).
 	
Beispiele:
 	
`bond0.1001`
 	
`ens192`
	Erforderlich

GRID_NETWORK_TARGET_TYPE

Wert	Bezeichnung
Schnittstelle (Dies ist der einzige unterstützte Wert.)	Optional

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Wert	Bezeichnung
Wahr oder Falsch Setzen Sie den Wert des Schlüssels auf „true“, damit der StorageGRID Container die MAC-Adresse der Host-Zielschnittstelle im Grid-Netzwerk verwendet. **Best Practice:** Verwenden Sie in Netzwerken, in denen der Promiscuous-Modus erforderlich wäre, stattdessen den Schlüssel GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Weitere Einzelheiten zum MAC-Klonen: • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red Hat Enterprise Linux)" • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"	Bewährte Methode

Installationskennwortschlüssel (temporär)

BENUTZERDEFINIERTER_TEMPORÄRER_PASSWORT_HASH

Wert	Bezeichnung
Legen Sie für den primären Admin-Knoten während der Installation ein temporäres Standardkennwort für die StorageGRID -Installations-API fest. **Hinweis**: Legen Sie nur auf dem primären Admin-Knoten ein Installationskennwort fest. Wenn Sie versuchen, ein Kennwort für einen anderen Knotentyp festzulegen, schlägt die Validierung der Knotenkonfigurationsdatei fehl. Das Festlegen dieses Werts hat nach Abschluss der Installation keine Auswirkungen mehr. Wenn dieser Schlüssel weggelassen wird, wird standardmäßig kein temporäres Passwort festgelegt. Alternativ können Sie mithilfe der StorageGRID Installations-API ein temporäres Passwort festlegen. Muss ein `crypt()` SHA-512-Passwort-Hash mit Format `$6$<salt>$<password hash>` für ein Passwort mit mindestens 8 und höchstens 32 Zeichen. Dieser Hash kann mit CLI-Tools generiert werden, wie zum Beispiel dem `openssl passwd` Befehl im SHA-512-Modus.	Bewährte Methode

Schnittstellenschlüssel

SCHNITTSTELLENZIEL_nnnn

Wert	Bezeichnung
Name und optionale Beschreibung für eine zusätzliche Schnittstelle, die Sie diesem Knoten hinzufügen möchten. Sie können jedem Knoten mehrere zusätzliche Schnittstellen hinzufügen. Geben Sie für *nnnn* eine eindeutige Nummer für jeden INTERFACE_TARGET-Eintrag an, den Sie hinzufügen. Geben Sie als Wert den Namen der physischen Schnittstelle auf dem Bare-Metal-Host an. Fügen Sie dann optional ein Komma hinzu und geben Sie eine Beschreibung der Schnittstelle ein, die auf der Seite „VLAN-Schnittstellen“ und der Seite „HA-Gruppen“ angezeigt wird. Beispiel: `INTERFACE_TARGET_0001=ens256, Trunk` Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt zu einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.	Optional

Maximaler RAM-Schlüssel

MAXIMALER RAM

Wert	Bezeichnung

Die maximale RAM-Menge, die dieser Knoten verbrauchen darf. Wenn dieser Schlüssel weggelassen wird, unterliegt der Knoten keinen Speicherbeschränkungen. Wenn Sie dieses Feld für einen Knoten auf Produktionsebene festlegen, geben Sie einen Wert an, der mindestens 24 GB und 16 bis 32 GB weniger als der gesamte System-RAM beträgt.
 	
Hinweis: Der RAM-Wert wirkt sich auf den tatsächlich für Metadaten reservierten Speicherplatz eines Knotens aus. Siehe die"Beschreibung, was Metadata Reserved Space ist" .
 	
Das Format für dieses Feld ist *`numberunit`* , Wo *`unit`* kann sein `b` , `k` , `m` , oder `g` .
 	
Beispiele:
 	
`24g`
 	
`38654705664b`
 	
Hinweis: Wenn Sie diese Option verwenden möchten, müssen Sie die Kernel-Unterstützung für Speicher-Cgroups aktivieren.
	Optional

Knotentypschlüssel

KNOTENTYP

Wert	Bezeichnung
Knotentyp: • VM_Admin_Node • VM_Speicherknoten • VM_Archive_Node • VM_API_Gateway	Erforderlich

SPEICHERTYP

Wert	Bezeichnung
Definiert den Objekttyp, den ein Speicherknoten enthält. Weitere Informationen finden Sie unter "Arten von Speicherknoten" . Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Storage_Node erforderlich. Geben Sie ihn nicht für andere Knotentypen an. Speichertypen: • kombiniert • Daten • Metadaten **Hinweis**: Wenn STORAGE_TYPE nicht angegeben ist, wird der Speicherknotentyp standardmäßig auf „Kombiniert (Daten und Metadaten)“ eingestellt.	Optional

Port-Neuzuordnungsschlüssel

PORT_REMAP

Wert	Bezeichnung
Ordnet jeden Port neu zu, der von einem Knoten für die interne oder externe Grid-Knotenkommunikation verwendet wird. Eine Neuzuordnung der Ports ist erforderlich, wenn die Netzwerkrichtlinien des Unternehmens einen oder mehrere von StorageGRID verwendete Ports einschränken, wie in beschrieben."Interne Grid-Knoten-Kommunikation" oder"Externe Kommunikation" . **WICHTIG**: Ordnen Sie die Ports, die Sie zum Konfigurieren der Endpunkte des Lastenausgleichs verwenden möchten, nicht neu zu. **Hinweis**: Wenn nur PORT_REMAP festgelegt ist, wird die von Ihnen angegebene Zuordnung sowohl für eingehende als auch für ausgehende Kommunikation verwendet. Wenn auch PORT_REMAP_INBOUND angegeben ist, gilt PORT_REMAP nur für ausgehende Kommunikation. Das verwendete Format ist: *`network type/protocol/default port used by grid node/new port`* , Wo *`network type`* ist Grid, Admin oder Client und *`protocol`* ist TCP oder UDP. Beispiel: `PORT_REMAP = client/tcp/18082/443` Sie können auch mehrere Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen. Beispiel: `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	Optional

PORT_REMAP_INBOUND

Wert	Bezeichnung
Ordnet eingehende Kommunikation dem angegebenen Port neu zu. Wenn Sie PORT_REMAP_INBOUND angeben, aber keinen Wert für PORT_REMAP angeben, bleibt die ausgehende Kommunikation für den Port unverändert. **WICHTIG**: Ordnen Sie die Ports, die Sie zum Konfigurieren der Endpunkte des Lastenausgleichs verwenden möchten, nicht neu zu. Das verwendete Format ist: *`network type/protocol/remapped port/default port used by grid node`* , Wo *`network type`* ist Grid, Admin oder Client und *`protocol`* ist TCP oder UDP. Beispiel: `PORT_REMAP_INBOUND = grid/tcp/3022/22` Sie können auch mehrere eingehende Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen. Beispiel: `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	Optional

So erkennen Grid-Knoten den primären Admin-Knoten

Grid-Knoten kommunizieren zur Konfiguration und Verwaltung mit dem primären Admin-Knoten. Jeder Grid-Knoten muss die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk kennen.

Um sicherzustellen, dass ein Grid-Knoten auf den primären Admin-Knoten zugreifen kann, können Sie beim Bereitstellen des Knotens einen der folgenden Schritte ausführen:

- Sie können den Parameter ADMIN_IP verwenden, um die IP-Adresse des primären Admin-Knotens manuell einzugeben.
- Sie können den Parameter ADMIN_IP weglassen, damit der Grid-Knoten den Wert automatisch erkennt. Die automatische Erkennung ist besonders nützlich, wenn das Grid-Netzwerk DHCP verwendet, um dem primären Admin-Knoten die IP-Adresse zuzuweisen.

Die automatische Erkennung des primären Admin-Knotens erfolgt mithilfe eines Multicast-Domain-Name-Systems (mDNS). Wenn der primäre Admin-Knoten zum ersten Mal gestartet wird, veröffentlicht er seine IP-Adresse mithilfe von mDNS. Andere Knoten im selben Subnetz können dann die IP-Adresse abfragen und automatisch abrufen. Da Multicast-IP-Verkehr jedoch normalerweise nicht über Subnetze hinweg geroutet werden kann, können Knoten in anderen Subnetzen die IP-Adresse des primären Admin-Knotens nicht direkt abrufen.

Wenn Sie die automatische Erkennung verwenden:

- Sie müssen die ADMIN_IP-Einstellung für mindestens einen Grid-Knoten in allen Subnetzen einschließen, an die der primäre Admin-Knoten nicht direkt angeschlossen ist. Dieser Grid-Knoten veröffentlicht dann die IP-Adresse des primären Admin-Knotens, damit andere Knoten im Subnetz sie mit mDNS erkennen können.
- Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur die Weiterleitung von Multicast-IP-Verkehr innerhalb eines Subnetzes unterstützt.

Beispiele für Knotenkonfigurationsdateien

Sie können die Beispielknotenkonfigurationsdateien verwenden, um die Knotenkonfigurationsdateien für Ihr StorageGRID -System einzurichten. Die Beispiele zeigen Knotenkonfigurationsdateien für alle Arten von Grid-Knoten.

Für die meisten Knoten können Sie Administrator- und Client-Netzwerkadressinformationen (IP, Maske, Gateway usw.) hinzufügen, wenn Sie das Grid mit dem Grid Manager oder der Installations-API konfigurieren. Die Ausnahme ist der primäre Admin-Knoten. Wenn Sie zur Admin-Netzwerk-IP des primären Admin-Knotens navigieren möchten, um die Grid-Konfiguration abzuschließen (weil das Grid-Netzwerk beispielsweise nicht geroutet wird), müssen Sie die Admin-Netzwerkverbindung für den primären Admin-Knoten in seiner Knotenkonfigurationsdatei konfigurieren. Dies wird im Beispiel gezeigt.

In den Beispielen wurde das Client-Netzwerkziel als Best Practice konfiguriert, obwohl das Client-Netzwerk standardmäßig deaktiviert ist.

Beispiel für primären Admin-Knoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-adm1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Beispiel für Speicherknoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-sn1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Beispiel für Gateway-Knoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-gw1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Beispiel für einen nicht primären Admin-Knoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-adm2.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validieren der StorageGRID -Konfiguration

Nach dem Erstellen von Konfigurationsdateien in `/etc/storagegrid/nodes` Für jeden Ihrer StorageGRID Knoten müssen Sie den Inhalt dieser Dateien validieren.

Um den Inhalt der Konfigurationsdateien zu validieren, führen Sie auf jedem Host den folgenden Befehl aus:

```
sudo storagegrid node validate all
```

Wenn die Dateien korrekt sind, zeigt die Ausgabe für jede Konfigurationsdatei **PASSED** an, wie im Beispiel gezeigt.

Wenn Sie auf Nur-Metadaten-Knoten nur eine LUN verwenden, erhalten Sie möglicherweise eine Warnmeldung, die ignoriert werden kann.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Bei einer automatisierten Installation können Sie diese Ausgabe unterdrücken, indem Sie den `-q` oder `--quiet` Optionen in der `storagegrid` Befehl (zum Beispiel `storagegrid --quiet…`). Wenn Sie die Ausgabe unterdrücken, hat der Befehl einen Exit-Wert ungleich Null, wenn Konfigurationswarnungen oder -fehler erkannt wurden.

Wenn die Konfigurationsdateien fehlerhaft sind, werden die Probleme wie im Beispiel gezeigt als **WARNUNG** und **FEHLER** angezeigt. Wenn Konfigurationsfehler gefunden werden, müssen Sie diese beheben, bevor Sie mit der Installation fortfahren.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Starten Sie den StorageGRID -Hostdienst

Um Ihre StorageGRID -Knoten zu starten und sicherzustellen, dass sie nach einem Host-Neustart neu gestartet werden, müssen Sie den StorageGRID Hostdienst aktivieren und starten.

Schritte

1. Führen Sie auf jedem Host die folgenden Befehle aus:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Bereitstellung fortgesetzt wird:

```
sudo storagegrid node status node-name
```

3. Wenn ein Knoten den Status „Nicht ausgeführt“ oder „Gestoppt“ zurückgibt, führen Sie den folgenden Befehl aus:

```
sudo storagegrid node start node-name
```

4. Wenn Sie den StorageGRID Hostdienst zuvor aktiviert und gestartet haben (oder wenn Sie nicht sicher sind, ob der Dienst aktiviert und gestartet wurde), führen Sie außerdem den folgenden Befehl aus:

```
sudo systemctl reload-or-restart storagegrid
```

Konfigurieren Sie das Grid und schließen Sie die Installation ab (Red Hat)

Navigieren Sie zum Grid Manager

Mit dem Grid Manager definieren Sie alle erforderlichen Informationen zur Konfiguration Ihres StorageGRID Systems.

Bevor Sie beginnen

Der primäre Admin-Knoten muss bereitgestellt sein und die anfängliche Startsequenz abgeschlossen haben.

Schritte

1. Öffnen Sie Ihren Webbrowser und navigieren Sie zu:

   `https://primary_admin_node_ip`

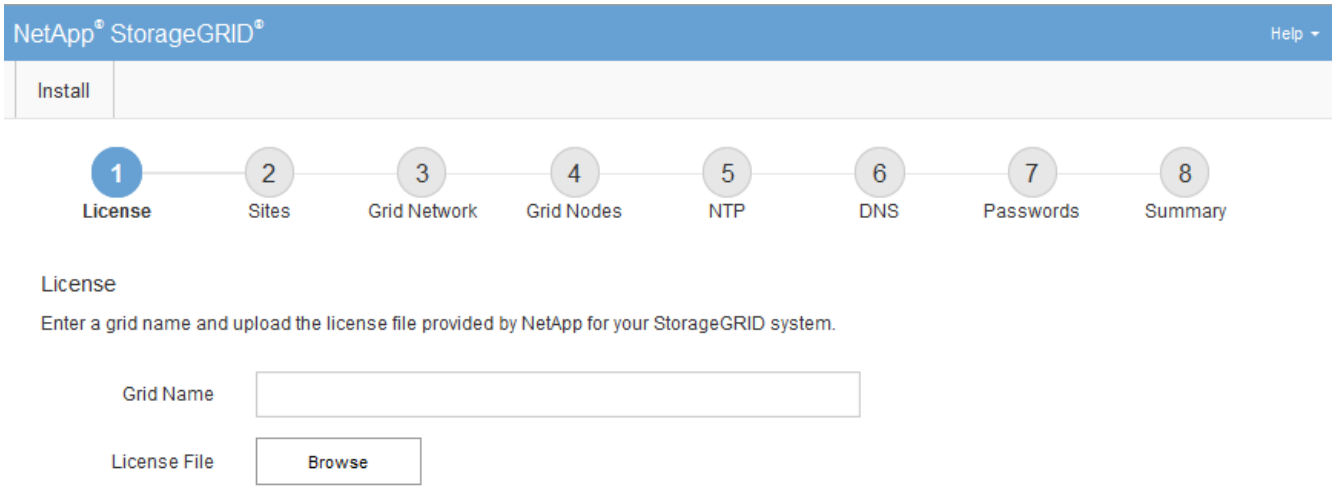
   Alternativ können Sie über Port 8443 auf den Grid Manager zugreifen:

   `https://primary_admin_node_ip:8443`

   Sie können die IP-Adresse für die primäre Admin-Knoten-IP im Grid-Netzwerk oder im Admin-Netzwerk verwenden, je nachdem, was für Ihre Netzwerkkonfiguration angemessen ist.

2. Verwalten Sie bei Bedarf ein temporäres Installateurkennwort:
   - Wenn mit einer dieser Methoden bereits ein Kennwort festgelegt wurde, geben Sie das Kennwort ein, um fortzufahren.
     - Ein Benutzer hat das Kennwort beim Zugriff auf das Installationsprogramm zuvor festgelegt
     - Das Passwort wurde automatisch aus der Knotenkonfigurationsdatei importiert unter `/etc/storagegrid/nodes/<node_name>.conf`
   - Wenn kein Kennwort festgelegt wurde, legen Sie optional ein Kennwort fest, um das StorageGRID Installationsprogramm zu sichern.
3. Wählen Sie **Installieren Sie ein StorageGRID -System**.

Die Seite zum Konfigurieren eines StorageGRID -Systems wird angezeigt.



Geben Sie die StorageGRID -Lizenzinformationen an

Sie müssen den Namen für Ihr StorageGRID -System angeben und die von NetApp bereitgestellte Lizenzdatei hochladen.

Schritte

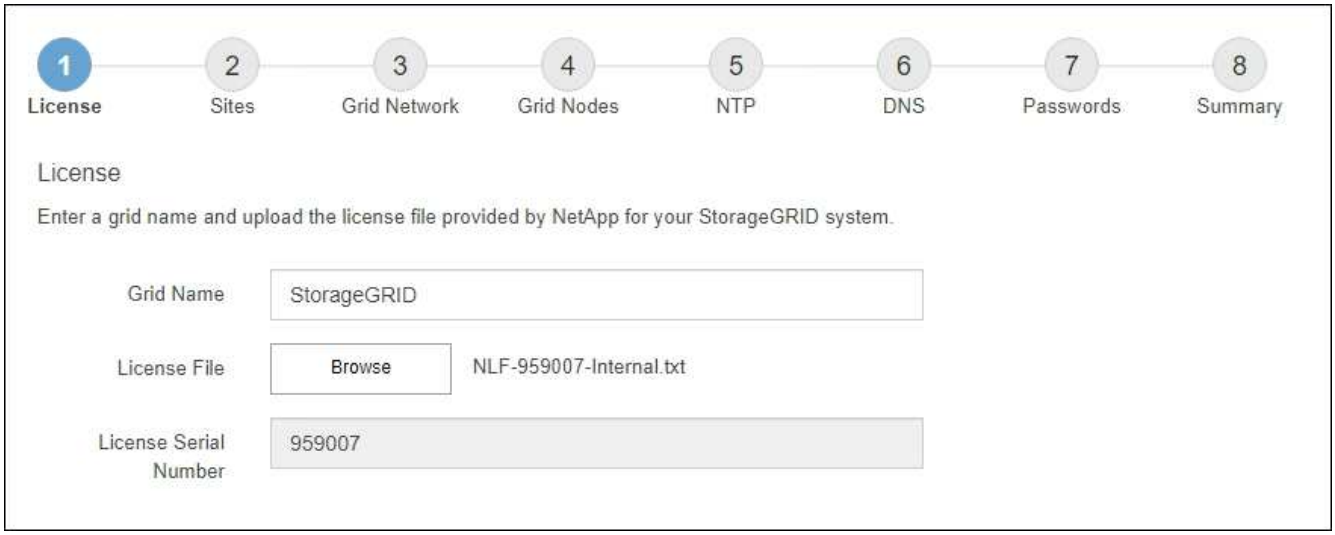
1. Geben Sie auf der Lizenzseite im Feld **Grid-Name** einen aussagekräftigen Namen für Ihr StorageGRID -System ein.

   Nach der Installation wird der Name oben im Knotenmenü angezeigt.

2. Wählen Sie **Durchsuchen**, suchen Sie die NetApp -Lizenzdatei(`NLF-unique-id.txt`) und wählen Sie **Öffnen**.

   Die Lizenzdatei wird validiert und die Seriennummer angezeigt.

> Das StorageGRID -Installationsarchiv enthält eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet. Sie können auf eine Lizenz aktualisieren, die nach der Installation Support bietet.



3. Wählen Sie **Weiter**.

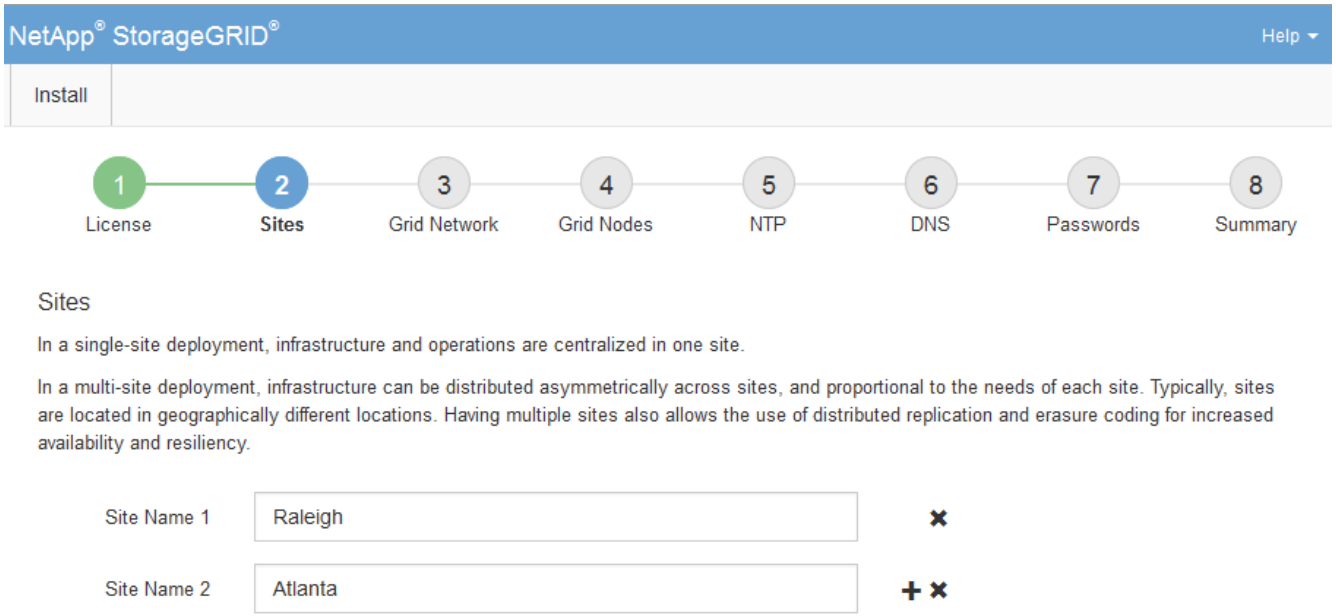
Websites hinzufügen

Sie müssen mindestens eine Site erstellen, wenn Sie StorageGRID installieren. Sie können zusätzliche Sites erstellen, um die Zuverlässigkeit und Speicherkapazität Ihres StorageGRID -Systems zu erhöhen.

Schritte

1. Geben Sie auf der Seite „Sites“ den **Site-Namen** ein.
2. Um weitere Sites hinzuzufügen, klicken Sie auf das Pluszeichen neben dem letzten Site-Eintrag und geben Sie den Namen in das neue Textfeld **Site-Name** ein.

   Fügen Sie so viele zusätzliche Sites hinzu, wie für Ihre Netztopologie erforderlich sind. Sie können bis zu 16 Sites hinzufügen.



3. Klicken Sie auf **Weiter**.

Grid-Netzwerk-Subnetze angeben

Sie müssen die Subnetze angeben, die im Grid-Netzwerk verwendet werden.

Informationen zu diesem Vorgang

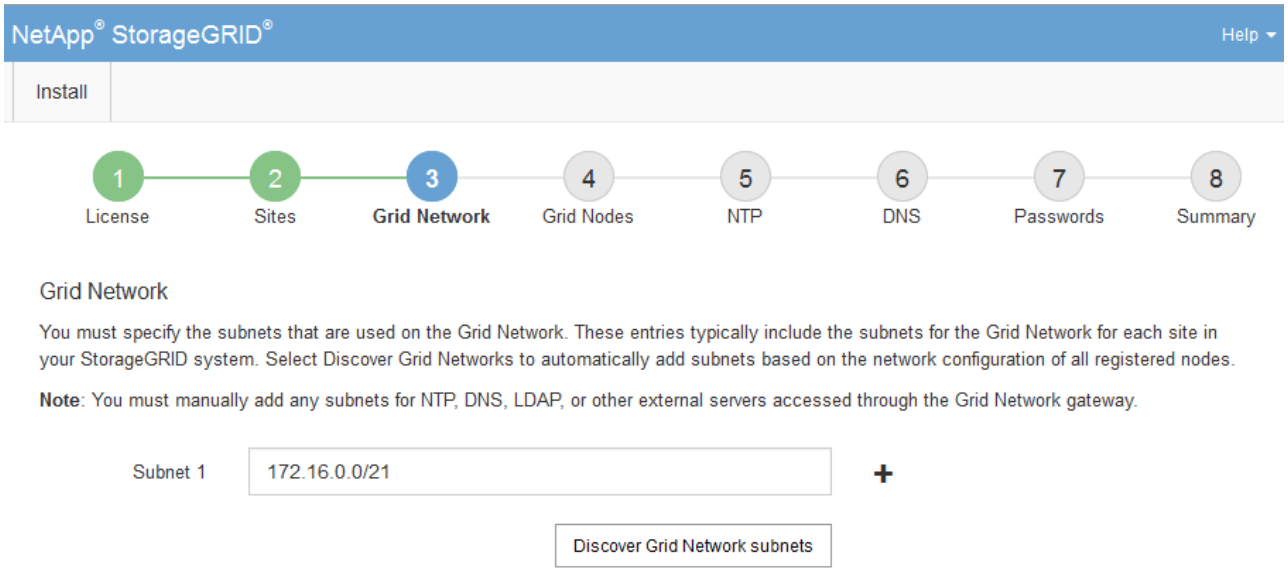
Die Subnetzeinträge umfassen die Subnetze für das Grid-Netzwerk für jeden Standort in Ihrem StorageGRID -System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen.

Wenn Sie über mehrere Grid-Subnetze verfügen, ist das Grid Network-Gateway erforderlich. Alle angegebenen Grid-Subnetze müssen über dieses Gateway erreichbar sein.

Schritte

1. Geben Sie die CIDR-Netzwerkadresse für mindestens ein Grid-Netzwerk im Textfeld **Subnetz 1** an.
2. Klicken Sie auf das Pluszeichen neben dem letzten Eintrag, um einen weiteren Netzwerkeintrag hinzuzufügen. Sie müssen alle Subnetze für alle Sites im Grid-Netzwerk angeben.

- Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf **Grid-Netzwerk-Subnetze ermitteln**, um die Grid-Netzwerk-Subnetzliste automatisch mit den Subnetzen zu füllen, die von Grid-Knoten gemeldet wurden, die beim Grid Manager registriert sind.
- Sie müssen alle Subnetze für NTP, DNS, LDAP oder andere externe Server, auf die über das Grid Network-Gateway zugegriffen wird, manuell hinzufügen.



3. Klicken Sie auf **Weiter**.

Ausstehende Rasterknoten genehmigen

Sie müssen jeden Grid-Knoten genehmigen, bevor er dem StorageGRID -System beitreten kann.

Bevor Sie beginnen

Sie haben alle virtuellen und StorageGRID -Appliance-Grid-Knoten bereitgestellt.

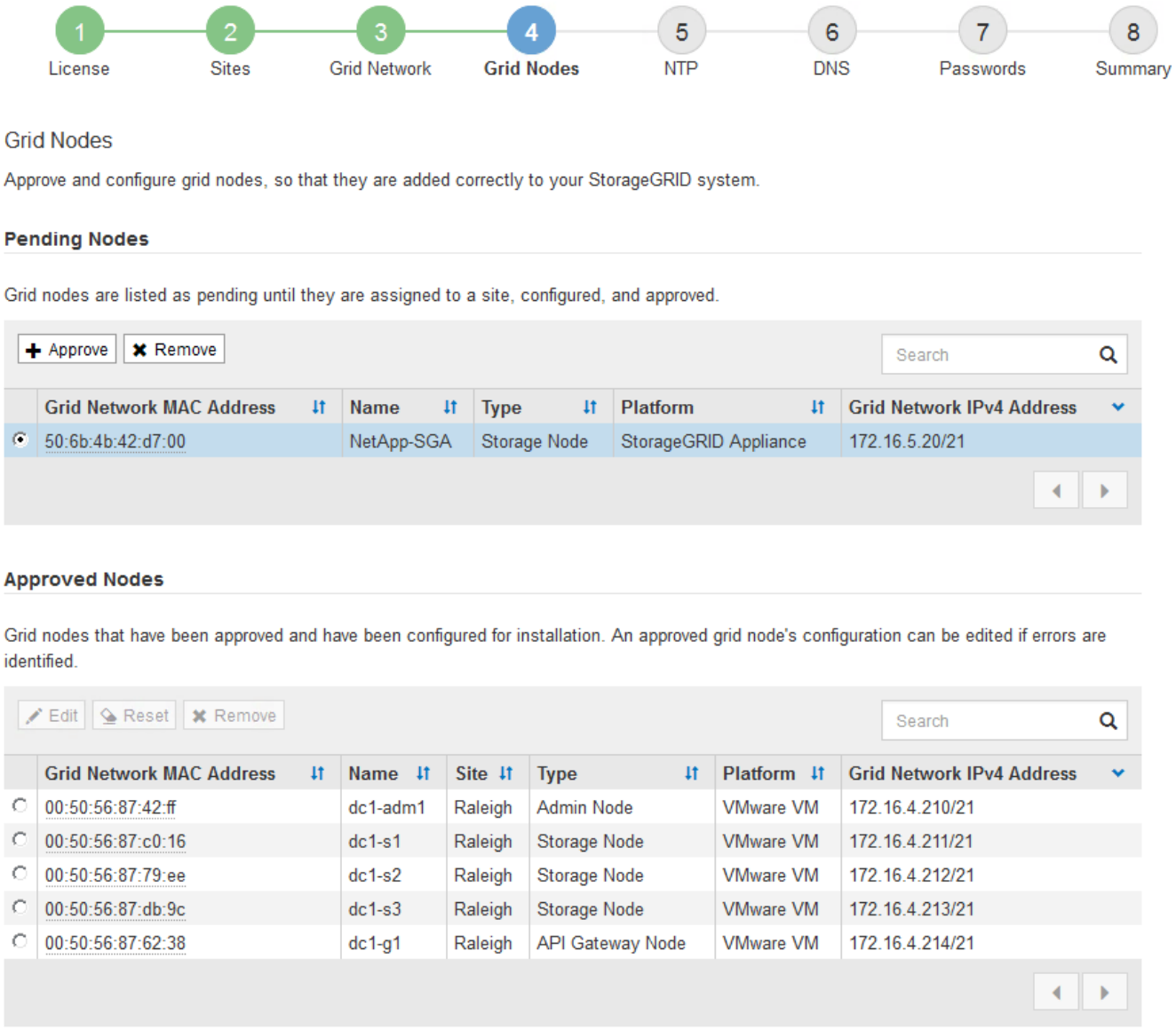
> Es ist effizienter, eine einzige Installation aller Knoten durchzuführen, als einige Knoten jetzt und einige Knoten später zu installieren.

Schritte

1. Überprüfen Sie die Liste der ausstehenden Knoten und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

> Wenn ein Grid-Knoten fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde und die richtige Grid-Netzwerk-IP des primären Admin-Knotens für ADMIN_IP festgelegt ist.

2. Wählen Sie das Optionsfeld neben einem ausstehenden Knoten aus, den Sie genehmigen möchten.



3. Klicken Sie auf **Genehmigen**.
4. Ändern Sie unter „Allgemeine Einstellungen“ nach Bedarf die Einstellungen für die folgenden Eigenschaften:
   - **Site**: Der Systemname der Site für diesen Grid-Knoten.
   - **Name**: Der Systemname für den Knoten. Der Name ist standardmäßig der Name, den Sie bei der Konfiguration des Knotens angegeben haben.

     Systemnamen sind für interne StorageGRID -Vorgänge erforderlich und können nach Abschluss der Installation nicht mehr geändert werden. Während dieses Schritts des Installationsvorgangs können Sie die Systemnamen jedoch nach Bedarf ändern.

     - **NTP-Rolle**: Die Network Time Protocol (NTP)-Rolle des Grid-Knotens. Die Optionen sind **Automatisch**, **Primär** und **Client**. Wenn Sie „**Automatisch**“ auswählen, wird die primäre Rolle den Admin-Knoten, Speicherknoten mit ADC-Diensten, Gateway-Knoten und allen Grid-Knoten mit nicht statischen IP-Adressen zugewiesen. Allen anderen Grid-Knoten wird die Client-Rolle zugewiesen.

Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.

- **Speichertyp** (nur Speicherknoten): Geben Sie an, dass ein neuer Speicherknoten ausschließlich für Daten, nur für Metadaten oder für beides verwendet werden soll. Die Optionen sind **Daten und Metadaten** („kombiniert“), **Nur Daten** und **Nur Metadaten**.

  Sehen"Arten von Speicherknoten" Informationen zu den Anforderungen für diese Knotentypen finden Sie unter.

- **ADC-Dienst** (nur Speicherknoten): Wählen Sie **Automatisch**, damit das System ermittelt, ob der Knoten den Administrative Domain Controller (ADC)-Dienst benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Diensten. Mindestens drei Speicherknoten an jedem Standort müssen den ADC-Dienst enthalten. Sie können den ADC-Dienst nach der Bereitstellung nicht mehr zu einem Knoten hinzufügen.

5. Ändern Sie im Grid-Netzwerk nach Bedarf die Einstellungen für die folgenden Eigenschaften:

   - **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Grid-Netzwerkschnittstelle (eth0 innerhalb des Containers). Beispiel: 192.168.1.234/21
   - **Gateway**: Das Grid-Netzwerk-Gateway. Beispiel: 192.168.0.1

     Das Gateway wird benötigt, wenn mehrere Grid-Subnetze vorhanden sind.

   Wenn Sie DHCP für die Grid-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

6. Wenn Sie das Admin-Netzwerk für den Grid-Knoten konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt „Admin-Netzwerk“ nach Bedarf hinzu oder aktualisieren Sie sie.

   Geben Sie die Zielsubnetze der Routen aus dieser Schnittstelle in das Textfeld **Subnetze (CIDR)** ein. Wenn mehrere Admin-Subnetze vorhanden sind, ist das Admin-Gateway erforderlich.

   Wenn Sie DHCP für die Admin-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

   Geräte: Wenn das Admin-Netzwerk für ein StorageGRID -Gerät während der Erstinstallation mit dem StorageGRID Appliance Installer nicht konfiguriert wurde, kann es in diesem Grid Manager-Dialogfeld nicht konfiguriert werden. Stattdessen müssen Sie die folgenden Schritte ausführen:

   a. Starten Sie das Gerät neu: Wählen Sie im Geräteinstallationsprogramm **Erweitert** > **Neustart**.

      Der Neustart kann mehrere Minuten dauern.

   b. Wählen Sie **Netzwerk konfigurieren** > **Linkkonfiguration** und aktivieren Sie die entsprechenden

Netzwerke.

c. Wählen Sie **Netzwerk konfigurieren** > **IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.

d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

e. Im Grid Manager: Wenn der Knoten in der Tabelle „Genehmigte Knoten“ aufgeführt ist, entfernen Sie den Knoten.

f. Entfernen Sie den Knoten aus der Tabelle „Ausstehende Knoten“.

g. Warten Sie, bis der Knoten wieder in der Liste „Ausstehende Knoten“ angezeigt wird.

h. Bestätigen Sie, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt sein, die Sie auf der IP-Konfigurationsseite des Appliance-Installationsprogramms angegeben haben.

   Weitere Informationen finden Sie in der Installationsanleitung Ihres Gerätemodells.

7. Wenn Sie das Client-Netzwerk für den Grid-Knoten konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt „Client-Netzwerk“ nach Bedarf hinzu oder aktualisieren Sie sie. Wenn das Client-Netzwerk konfiguriert ist, ist das Gateway erforderlich und wird nach der Installation zum Standard-Gateway für den Knoten.

   Wenn Sie DHCP für die Client-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

   Geräte: Wenn das Client-Netzwerk eines StorageGRID Geräts während der Erstinstallation mit dem StorageGRID -Geräteinstallationsprogramm nicht konfiguriert wurde, kann es in diesem Grid Manager-Dialogfeld nicht konfiguriert werden. Stattdessen müssen Sie die folgenden Schritte ausführen:

   a. Starten Sie das Gerät neu: Wählen Sie im Geräteinstallationsprogramm **Erweitert** > **Neustart**.

      Der Neustart kann mehrere Minuten dauern.

   b. Wählen Sie **Netzwerk konfigurieren** > **Linkkonfiguration** und aktivieren Sie die entsprechenden Netzwerke.

   c. Wählen Sie **Netzwerk konfigurieren** > **IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.

   d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

   e. Im Grid Manager: Wenn der Knoten in der Tabelle „Genehmigte Knoten“ aufgeführt ist, entfernen Sie den Knoten.

   f. Entfernen Sie den Knoten aus der Tabelle „Ausstehende Knoten“.

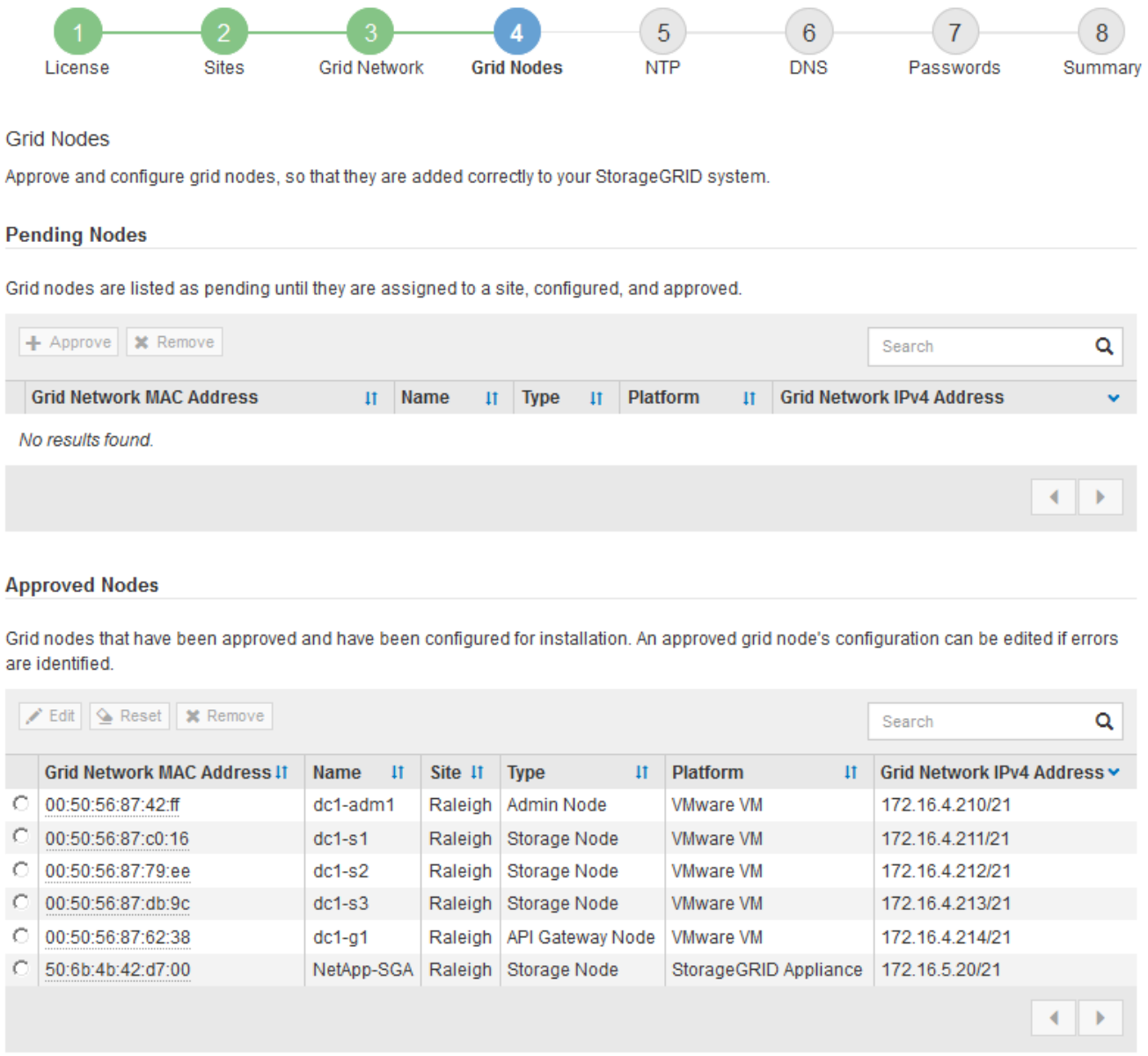
   g. Warten Sie, bis der Knoten wieder in der Liste „Ausstehende Knoten“ angezeigt wird.

   h. Bestätigen Sie, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt sein, die Sie auf der IP-Konfigurationsseite des Appliance-Installationsprogramms angegeben haben.

      Weitere Informationen finden Sie in der Installationsanleitung Ihres Geräts.

8. Klicken Sie auf **Speichern**.

Der Rasterknoteneintrag wird in die Liste „Genehmigte Knoten“ verschoben.



9. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

   Sie müssen alle Knoten genehmigen, die Sie im Raster haben möchten. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Zusammenfassungsseite auf **Installieren** klicken. Sie können die Eigenschaften eines genehmigten Rasterknotens ändern, indem Sie dessen Optionsfeld auswählen und auf **Bearbeiten** klicken.

10. Wenn Sie mit der Genehmigung der Rasterknoten fertig sind, klicken Sie auf **Weiter**.

Geben Sie die Serverinformationen des Network Time Protocol an

Sie müssen die Network Time Protocol (NTP)-Konfigurationsinformationen für das StorageGRID -System angeben, damit die auf separaten Servern ausgeführten Vorgänge synchronisiert bleiben können.

Informationen zu diesem Vorgang

Sie müssen IPv4-Adressen für die NTP-Server angeben.

Sie müssen externe NTP-Server angeben. Die angegebenen NTP-Server müssen das NTP-Protokoll verwenden.

Sie müssen vier NTP-Serverreferenzen von Stratum 3 oder besser angeben, um Probleme mit Zeitabweichungen zu vermeiden.

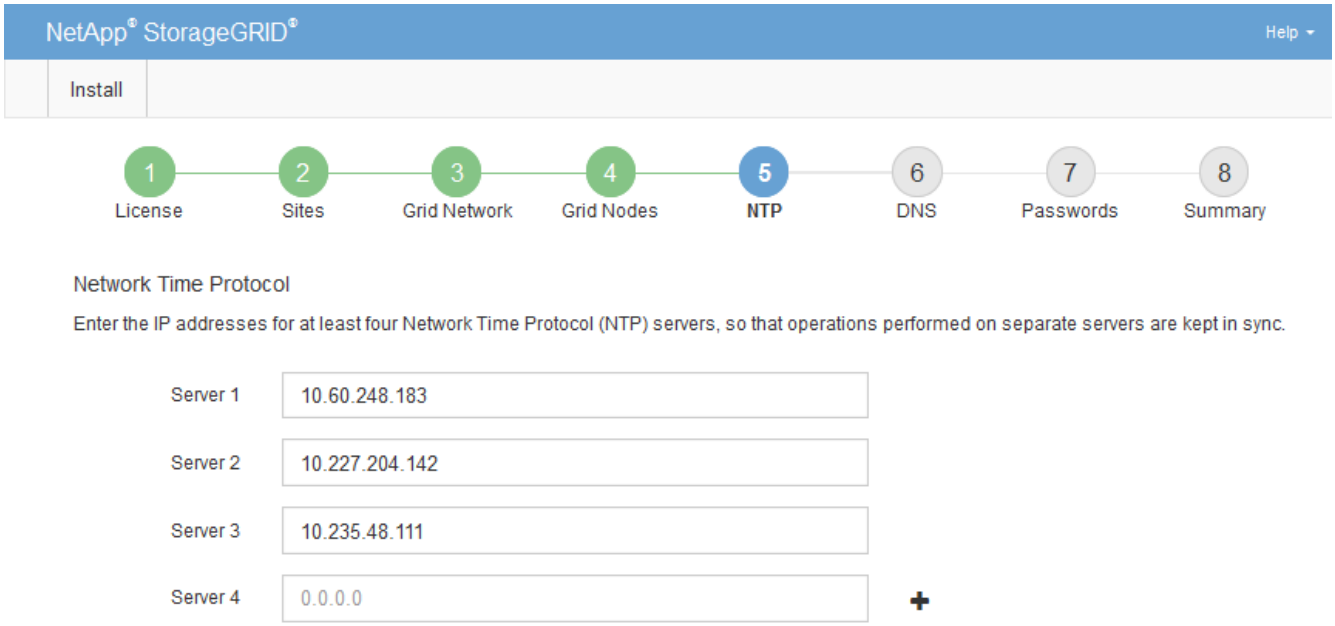
> Wenn Sie die externe NTP-Quelle für eine StorageGRID Installation auf Produktionsebene angeben, verwenden Sie den Windows-Zeitdienst (W32Time) nicht auf einer Windows-Version vor Windows Server 2016. Der Zeitdienst früherer Windows-Versionen ist nicht genau genug und wird von Microsoft für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, nicht unterstützt.
>
> "Supportgrenze zum Konfigurieren des Windows-Zeitdienstes für Umgebungen mit hoher Genauigkeit"

Die externen NTP-Server werden von den Knoten verwendet, denen Sie zuvor primäre NTP-Rollen zugewiesen haben.

> Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.

Schritte

1. Geben Sie die IPv4-Adressen für mindestens vier NTP-Server in den Textfeldern **Server 1** bis **Server 4** an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um weitere Servereinträge hinzuzufügen.



3. Wählen Sie **Weiter**.

DNS-Serverinformationen angeben

Sie müssen DNS-Informationen für Ihr StorageGRID -System angeben, damit Sie auf externe Server über Hostnamen statt über IP-Adressen zugreifen können.

Informationen zu diesem Vorgang

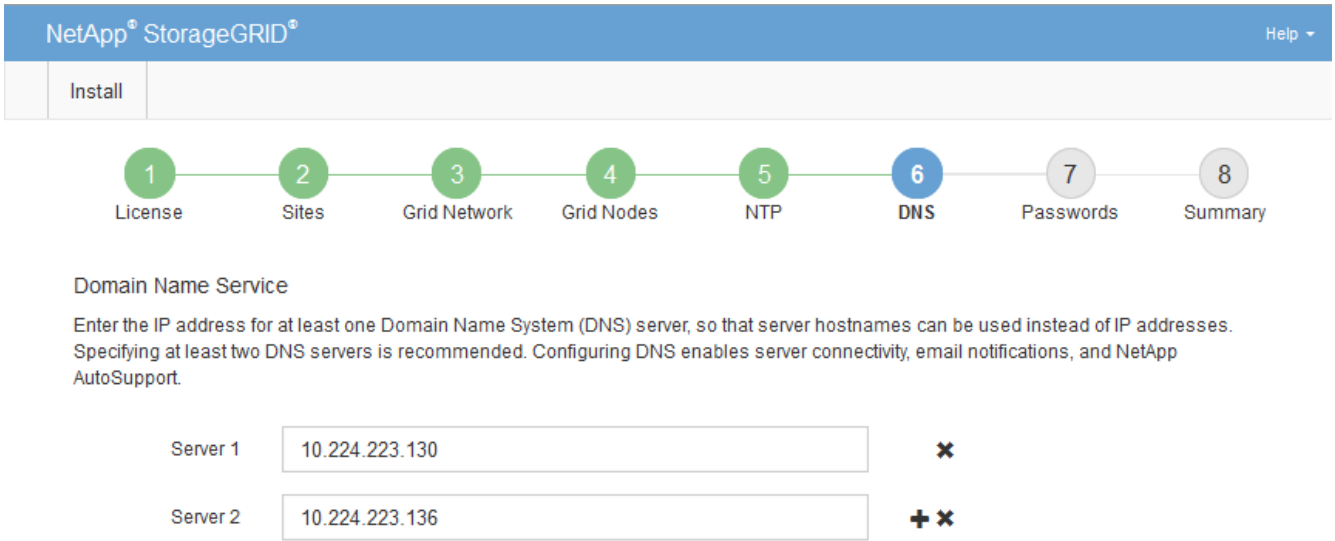
Festlegen "DNS-Serverinformationen" ermöglicht Ihnen die Verwendung von Fully Qualified Domain Name (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport.

Um einen ordnungsgemäßen Betrieb sicherzustellen, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, ist es möglich, dass aufgrund bekannter Betriebssystembeschränkungen auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie"Passen Sie die DNS-Serverliste an" für einzelne Knoten (normalerweise alle Knoten an einem Standort), einen anderen Satz von bis zu drei DNS-Servern zu verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein isolierter Standort die FQDNs für externe Ziele auflösen kann.

Schritte

1. Geben Sie im Textfeld **Server 1** die IPv4-Adresse für mindestens einen DNS-Server an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um weitere Servereinträge hinzuzufügen.



   Die beste Vorgehensweise besteht darin, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Geben Sie die StorageGRID -Systemkennwörter an

Im Rahmen der Installation Ihres StorageGRID -Systems müssen Sie die Passwörter eingeben, mit denen Sie Ihr System sichern und Wartungsaufgaben durchführen können.

Informationen zu diesem Vorgang

Verwenden Sie die Seite „Passwörter installieren“, um die Bereitstellungspassphrase und das Root-Benutzerpasswort für die Grid-Verwaltung anzugeben.

- Die Bereitstellungspassphrase wird als Verschlüsselungsschlüssel verwendet und nicht vom StorageGRID -System gespeichert.
- Sie müssen über die Bereitstellungspassphrase für Installations-, Erweiterungs- und Wartungsvorgänge verfügen, einschließlich des Herunterladens des Wiederherstellungspakets. Daher ist es wichtig, dass Sie die Bereitstellungspassphrase an einem sicheren Ort speichern.
- Sie können die Bereitstellungspassphrase im Grid Manager ändern, wenn Sie die aktuelle haben.
- Das Root-Benutzerkennwort für die Grid-Verwaltung kann mithilfe des Grid-Managers geändert werden.
- Zufällig generierte Befehlszeilenkonsolen- und SSH-Passwörter werden im `Passwords.txt` Datei im Wiederherstellungspaket.

Schritte

1. Geben Sie unter **Bereitstellungspassphrase** die Bereitstellungspassphrase ein, die zum Vornehmen von Änderungen an der Grid-Topologie Ihres StorageGRID Systems erforderlich ist.

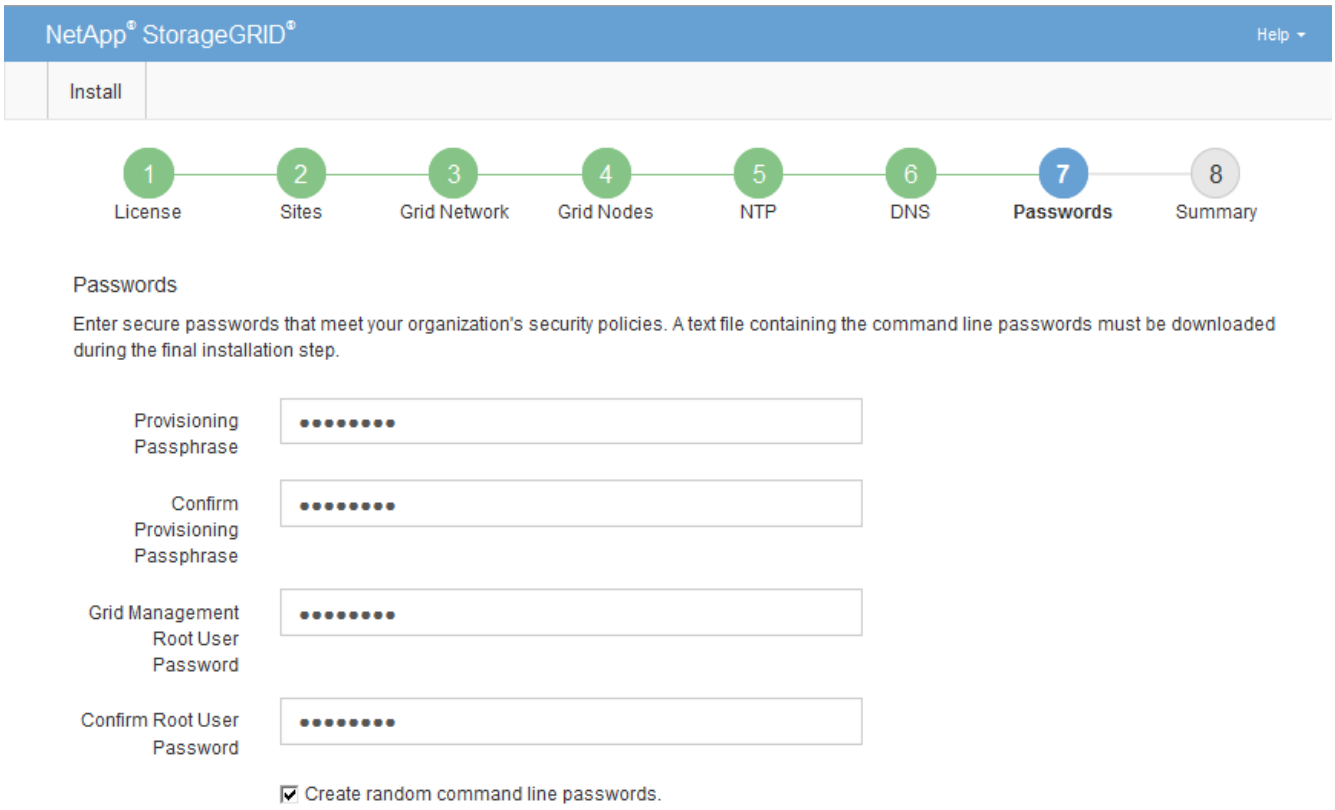
   Bewahren Sie die Bereitstellungspassphrase an einem sicheren Ort auf.

   > Wenn Sie nach Abschluss der Installation die Bereitstellungspassphrase später ändern möchten, können Sie den Grid Manager verwenden. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Grid-Passwörter**.

2. Geben Sie unter **Bereitstellungspassphrase bestätigen** die Bereitstellungspassphrase erneut ein, um sie zu bestätigen.
3. Geben Sie unter **Grid Management Root User Password** das Passwort ein, das Sie für den Zugriff auf den Grid Manager als „Root“-Benutzer verwenden möchten.

   Bewahren Sie das Passwort an einem sicheren Ort auf.

4. Geben Sie unter **Root-Benutzerkennwort bestätigen** das Grid Manager-Kennwort erneut ein, um es zu bestätigen.



5. Wenn Sie ein Grid zu Proof-of-Concept- oder Demozwecken installieren, deaktivieren Sie optional das Kontrollkästchen **Zufällige Befehlszeilenkennwörter erstellen**.

   Bei Produktionsbereitstellungen sollten aus Sicherheitsgründen immer zufällige Passwörter verwendet werden. Deaktivieren Sie **Zufällige Befehlszeilenkennwörter erstellen** nur für Demo-Raster, wenn Sie Standardkennwörter verwenden möchten, um über die Befehlszeile mit dem Konto „root“ oder „admin“ auf Rasterknoten zuzugreifen.

   > Sie werden aufgefordert, die Wiederherstellungspaketdatei herunterzuladen(`sgws-recovery-package-id-revision.zip`), nachdem Sie auf der Seite „Zusammenfassung“ auf **Installieren** geklickt haben. Sie müssen"Laden Sie diese Datei herunter" um die Installation abzuschließen. Die für den Zugriff auf das System erforderlichen Passwörter sind im `Passwords.txt` Datei, die in der Wiederherstellungspaketdatei enthalten ist.

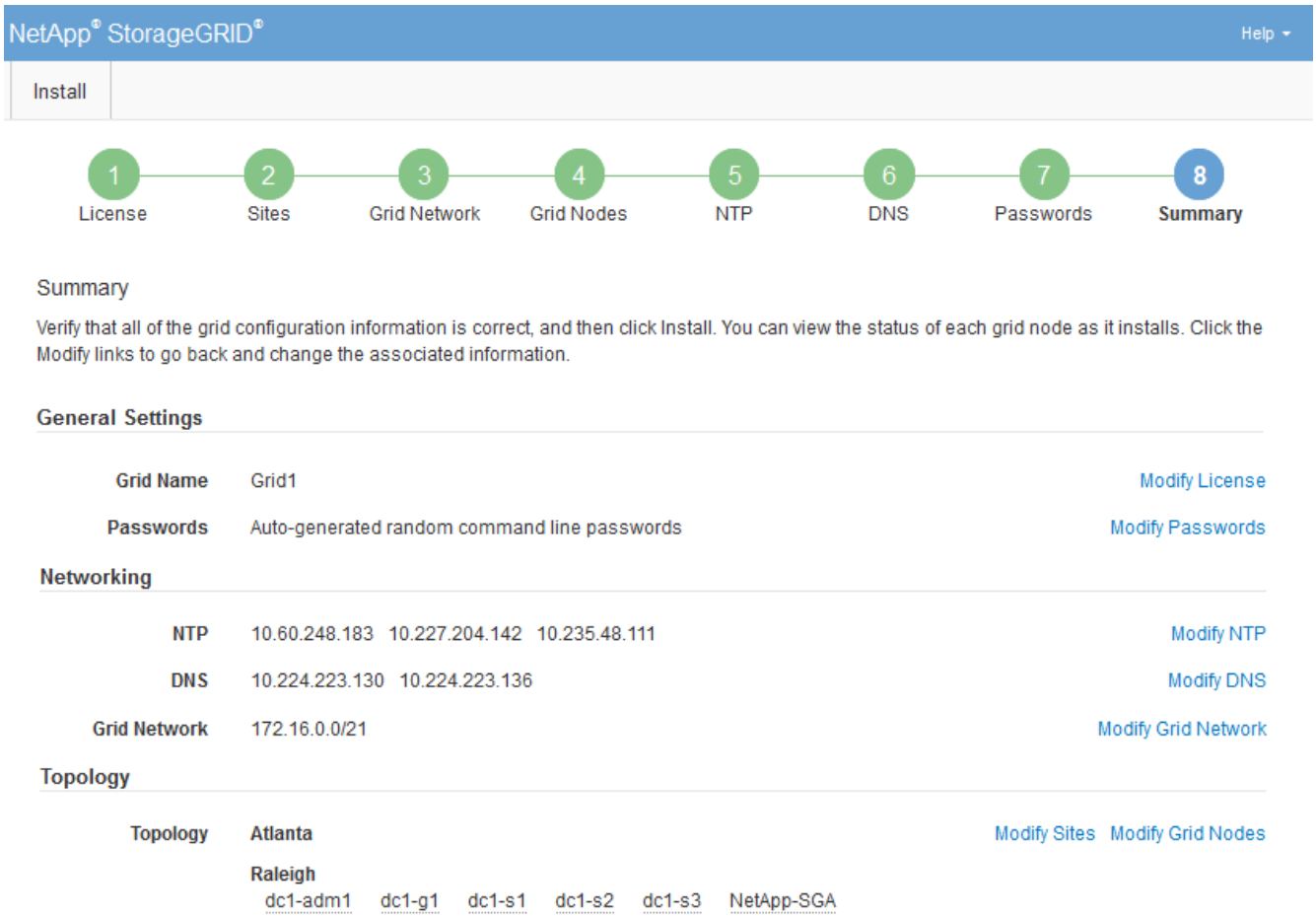
6. Klicken Sie auf **Weiter**.

Überprüfen Sie Ihre Konfiguration und schließen Sie die Installation ab

Sie müssen die eingegebenen Konfigurationsinformationen sorgfältig prüfen, um sicherzustellen, dass die Installation erfolgreich abgeschlossen wird.

Schritte

1. Sehen Sie sich die Seite **Zusammenfassung** an.



2. Überprüfen Sie, ob alle Informationen zur Netzkonfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite „Zusammenfassung“, um zurückzugehen und etwaige Fehler zu korrigieren.
3. Klicken Sie auf **Installieren**.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf **Installieren** klicken. Wenn die Verbindung verloren geht, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Knoten zugreifen. Sehen"Netzwerkrichtlinien" für Details.

4. Klicken Sie auf **Wiederherstellungspaket herunterladen**.

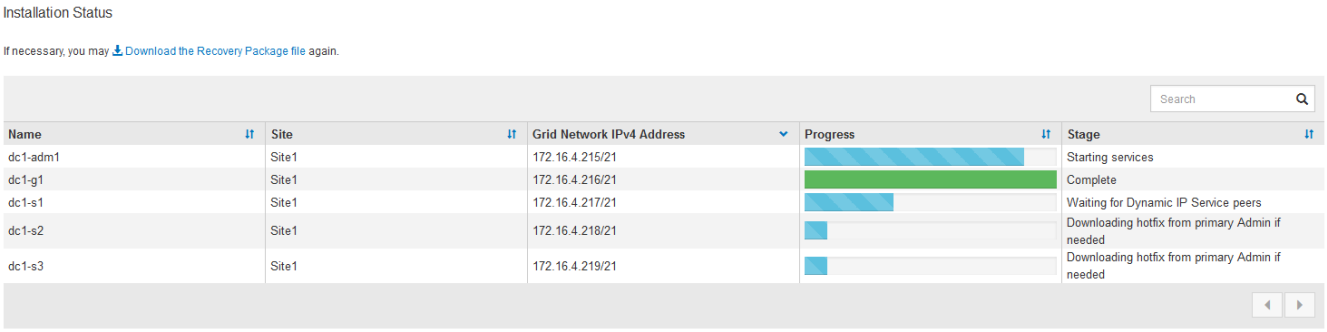
   Wenn die Installation bis zu dem Punkt fortschreitet, an dem die Grid-Topologie definiert ist, werden Sie aufgefordert, die Datei Recovery Package herunterzuladen(`.zip`) und bestätigen Sie, dass Sie erfolgreich auf den Inhalt dieser Datei zugreifen können. Sie müssen die Wiederherstellungspaketdatei herunterladen, damit Sie das StorageGRID -System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Die Installation wird im Hintergrund fortgesetzt, Sie können die Installation jedoch erst abschließen und auf das StorageGRID -System zugreifen, wenn Sie diese Datei heruntergeladen und überprüft haben.

5. Überprüfen Sie, ob Sie den Inhalt der `.zip` Datei und speichern Sie sie dann an zwei sicheren und getrennten Orten.

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

6. Aktivieren Sie das Kontrollkästchen **Ich habe die Wiederherstellungspaketdatei erfolgreich heruntergeladen und überprüft** und klicken Sie auf **Weiter**.

   Wenn die Installation noch läuft, wird die Statusseite angezeigt. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



   Wenn für alle Grid-Knoten die Phase „Abgeschlossen“ erreicht ist, wird die Anmeldeseite für den Grid Manager angezeigt.

7. Sign in beim Grid Manager mit dem Benutzer „root“ und dem Kennwort an, das Sie während der Installation angegeben haben.

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Bereitstellung und Konfiguration des Grid-Knotens diese Richtlinien für DHCP-Adressierung und Netzwerkkonfigurationsänderungen.

- Wenn DHCP zum Zuweisen von IP-Adressen verwendet wurde, konfigurieren Sie eine DHCP-Reservierung für jede IP-Adresse in den verwendeten Netzwerken.

  Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten.

  Knoten werden neu gestartet, wenn die Grid-Netzwerkkonfiguration per DHCP geändert wird. Dies kann zu Ausfällen führen, wenn eine DHCP-Änderung mehrere Knoten gleichzeitig betrifft.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmasken und Standard-Gateways für einen Grid-Knoten ändern möchten. Sehen "Konfigurieren von IP-Adressen" .
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin-Knoten und anderen Grid-Knoten verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Installation der REST-API

StorageGRID bietet die StorageGRID -Installations-API zum Ausführen von

Installationsaufgaben.

Die API verwendet die Open-Source-API-Plattform Swagger, um die API-Dokumentation bereitzustellen. Swagger ermöglicht sowohl Entwicklern als auch Nicht-Entwicklern die Interaktion mit der API in einer Benutzeroberfläche, die veranschaulicht, wie die API auf Parameter und Optionen reagiert. Diese Dokumentation setzt voraus, dass Sie mit Standard-Webtechnologien und dem JSON-Datenformat vertraut sind.

> 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.

Jeder REST-API-Befehl enthält die URL der API, eine HTTP-Aktion, alle erforderlichen oder optionalen URL-Parameter und eine erwartete API-Antwort.

StorageGRID Installations-API

Die StorageGRID Installations-API ist nur verfügbar, wenn Sie Ihr StorageGRID -System zum ersten Mal konfigurieren und eine Wiederherstellung des primären Admin-Knotens durchführen müssen. Auf die Installations-API kann über HTTPS vom Grid Manager aus zugegriffen werden.

Um auf die API-Dokumentation zuzugreifen, gehen Sie zur Installationswebseite auf dem primären Admin-Knoten und wählen Sie in der Menüleiste **Hilfe** > **API-Dokumentation**.

Die StorageGRID -Installations-API umfasst die folgenden Abschnitte:

- **config** – Vorgänge im Zusammenhang mit der Produktversion und den Versionen der API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **grid** – Konfigurationsvorgänge auf Grid-Ebene. Sie können Grid-Einstellungen abrufen und aktualisieren, einschließlich Grid-Details, Grid-Netzwerk-Subnetze, Grid-Passwörter sowie NTP- und DNS-Server-IP-Adressen.
- **Knoten** – Konfigurationsvorgänge auf Knotenebene. Sie können eine Liste von Grid-Knoten abrufen, einen Grid-Knoten löschen, einen Grid-Knoten konfigurieren, einen Grid-Knoten anzeigen und die Konfiguration eines Grid-Knotens zurücksetzen.
- **Bereitstellung** – Bereitstellungsvorgänge. Sie können den Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** – Wiederherstellungsvorgänge für den primären Admin-Knoten. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **recovery-package** – Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **Sites** – Konfigurationsvorgänge auf Site-Ebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.
- **temporäres Passwort** – Vorgänge für das temporäre Passwort, um die Mgmt-API während der Installation zu sichern.

Wohin als nächstes?

Führen Sie nach Abschluss einer Installation die erforderlichen Integrations- und Konfigurationsaufgaben durch. Sie können die optionalen Aufgaben nach Bedarf ausführen.

Erforderliche Aufgaben

- "Erstellen Sie ein Mieterkonto"für das S3-Clientprotokoll, das zum Speichern von Objekten auf Ihrem StorageGRID System verwendet wird.
- "Kontrollsystemzugriff"durch Konfigurieren von Gruppen und Benutzerkonten. Optional können Sie"Konfigurieren einer föderierten Identitätsquelle" (wie Active Directory oder OpenLDAP), sodass Sie Administrationsgruppen und Benutzer importieren können. Oder Sie können"Erstellen Sie lokale Gruppen und Benutzer" .
- Integrieren und testen Sie die"S3 API" Clientanwendungen, die Sie zum Hochladen von Objekten in Ihr StorageGRID System verwenden.
- "Konfigurieren der Regeln und Richtlinien für das Information Lifecycle Management (ILM)"Sie zum Schutz der Objektdaten verwenden möchten.
- Wenn Ihre Installation Appliance-Speicherknoten umfasst, verwenden Sie SANtricity OS, um die folgenden Aufgaben auszuführen:
  - Stellen Sie eine Verbindung zu jedem StorageGRID Gerät her.
  - Überprüfen Sie den Erhalt der AutoSupport -Daten.

    Sehen "Hardware einrichten" .
- Überprüfen und befolgen Sie die"Richtlinien zur Systemhärtung von StorageGRID" um Sicherheitsrisiken auszuschließen.
- "Konfigurieren Sie E-Mail-Benachrichtigungen für Systemwarnungen" .

Optionale Aufgaben

- "Aktualisieren Sie die IP-Adressen der Grid-Knoten"ob sie sich seit der Planung Ihrer Bereitstellung und der Generierung des Wiederherstellungspakets geändert haben.
- "Konfigurieren der Speicherverschlüsselung", falls erforderlich.
- "Konfigurieren der Speicherkomprimierung"um die Größe gespeicherter Objekte bei Bedarf zu reduzieren.
- "Konfigurieren von VLAN-Schnittstellen"um den Netzwerkverkehr bei Bedarf zu isolieren und zu partitionieren.
- "Konfigurieren von Hochverfügbarkeitsgruppen"um bei Bedarf die Verbindungsverfügbarkeit für Grid Manager, Tenant Manager und S3-Clients zu verbessern.
- "Konfigurieren von Load Balancer-Endpunkten"für S3-Client-Konnektivität, falls erforderlich.

Beheben von Installationsproblemen

Wenn bei der Installation Ihres StorageGRID -Systems Probleme auftreten, können Sie auf die Installationsprotokolldateien zugreifen. Der technische Support muss möglicherweise auch die Installationsprotokolldateien verwenden, um Probleme zu lösen.

Die folgenden Installationsprotokolldateien sind aus dem Container verfügbar, in dem jeder Knoten ausgeführt wird:

- `/var/local/log/install.log`(auf allen Grid-Knoten zu finden)
- `/var/local/log/gdu-server.log`(auf dem primären Admin-Knoten zu finden)

Die folgenden Installationsprotokolldateien sind vom Host verfügbar:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Informationen zum Zugriff auf die Protokolldateien finden Sie unter"Erfassen von Protokolldateien und Systemdaten" .

Ähnliche Informationen

"Fehlerbehebung bei einem StorageGRID -System"

Beispiel /etc/sysconfig/network-scripts

Sie können die Beispieldateien verwenden, um vier physische Linux-Schnittstellen in einer einzigen LACP-Verbindung zusammenzufassen und dann drei VLAN-Schnittstellen einzurichten, die die Verbindung zur Verwendung als StorageGRID Grid-, Admin- und Client-Netzwerkschnittstellen unterteilen.

Physikalische Schnittstellen

Beachten Sie, dass die Switches an den anderen Enden der Links die vier Ports ebenfalls als einen einzigen LACP-Trunk oder Port-Kanal behandeln und mindestens die drei referenzierten VLANs mit Tags übergeben müssen.

`/etc/sysconfig/network-scripts/ifcfg-ens160`

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

`/etc/sysconfig/network-scripts/ifcfg-ens192`

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

`/etc/sysconfig/network-scripts/ifcfg-ens224`

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Bond-Schnittstelle

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

VLAN-Schnittstellen

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Installieren Sie StorageGRID unter Ubuntu oder Debian

Schnellstart zur Installation von StorageGRID unter Ubuntu oder Debian

Befolgen Sie diese allgemeinen Schritte, um einen Ubuntu- oder Debian- StorageGRID Knoten zu installieren.

1 **Vorbereitung**

- Erfahren Sie mehr über"StorageGRID -Architektur und Netzwerktopologie" .
- Erfahren Sie mehr über die Besonderheiten von"StorageGRID Netzwerk" .
- Sammeln und vorbereiten Sie die"Benötigte Informationen und Materialien" .
- Bereiten Sie die erforderlichen"CPU und RAM" .
- Sorgen für"Speicher- und Leistungsanforderungen" .
- "Vorbereiten der Linux-Server"das Ihre StorageGRID Knoten hosten wird.

2 **Einsatz**

Stellen Sie Grid-Knoten bereit. Wenn Sie Grid-Knoten bereitstellen, werden diese als Teil des StorageGRID -Systems erstellt und mit einem oder mehreren Netzwerken verbunden.

- Um softwarebasierte Grid-Knoten auf den Hosts bereitzustellen, die Sie in Schritt 1 vorbereitet haben, verwenden Sie die Linux-Befehlszeile und"Knotenkonfigurationsdateien" .
- Um StorageGRID Appliance-Knoten bereitzustellen, folgen Sie den "Schnellstart für die Hardwareinstallation" .

Konfiguration

Wenn alle Knoten bereitgestellt wurden, verwenden Sie den Grid Manager, um"Konfigurieren Sie das Grid und schließen Sie die Installation ab" .

Automatisieren Sie die Installation

Um Zeit zu sparen und Konsistenz zu gewährleisten, können Sie die Installation des StorageGRID Hostdienstes und die Konfiguration der Grid-Knoten automatisieren.

- Verwenden Sie ein Standard-Orchestrierungsframework wie Ansible, Puppet oder Chef, um Folgendes zu automatisieren:
  - Installation von Ubuntu oder Debian
  - Konfiguration von Netzwerk und Speicher
  - Installation der Container-Engine und des StorageGRID -Hostdienstes
  - Bereitstellung virtueller Grid-Knoten

  Sehen "Automatisieren Sie die Installation und Konfiguration des StorageGRID Hostdienstes" .
- Nachdem Sie Grid-Knoten bereitgestellt haben,"Automatisieren Sie die Konfiguration des StorageGRID -Systems" mithilfe des im Installationsarchiv bereitgestellten Python-Konfigurationsskripts.
- "Automatisieren Sie die Installation und Konfiguration von Appliance-Grid-Knoten"
- Wenn Sie ein fortgeschrittener Entwickler von StorageGRID Bereitstellungen sind, automatisieren Sie die Installation von Grid-Knoten mithilfe der"Installation der REST-API" .

Planen und Vorbereiten der Installation auf Ubuntu oder Debian

Benötigte Informationen und Materialien

Bevor Sie StorageGRID installieren, sammeln und bereiten Sie die erforderlichen Informationen und Materialien vor.

Erforderliche Informationen

Netzwerkplan

Welche Netzwerke Sie an jeden StorageGRID Knoten anschließen möchten. StorageGRID unterstützt mehrere Netzwerke zur Verkehrstrennung, Sicherheit und Verwaltungsfreundlichkeit.

Zum StorageGRID"Netzwerkrichtlinien" .

Netzwerkinformationen

Jedem Grid-Knoten zuzuweisende IP-Adressen und die IP-Adressen der DNS- und NTP-Server.

Server für Grid-Knoten

Identifizieren Sie eine Reihe von Servern (physisch, virtuell oder beides), die insgesamt ausreichend Ressourcen bereitstellen, um die Anzahl und Art der StorageGRID Knoten zu unterstützen, die Sie bereitstellen möchten.

> ⓘ Wenn Ihre StorageGRID Installation keine StorageGRID Appliance-(Hardware-)Speicherknoten verwendet, müssen Sie Hardware-RAID-Speicher mit batteriegepuffertem Schreibcache (BBWC) verwenden. StorageGRID unterstützt nicht die Verwendung von virtuellen Storage Area Networks (vSANs), Software-RAID oder keinen RAID-Schutz.

Knotenmigration (falls erforderlich)

Verstehen Sie die"Anforderungen für die Knotenmigration" , wenn Sie geplante Wartungsarbeiten an physischen Hosts ohne Dienstunterbrechung durchführen möchten.

Ähnliche Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Benötigtes Material

NetApp StorageGRID -Lizenz

Sie müssen über eine gültige, digital signierte NetApp -Lizenz verfügen.

> ⓘ Eine Nicht-Produktionslizenz, die zum Testen und Proof-of-Concept-Grids verwendet werden kann, ist im StorageGRID -Installationsarchiv enthalten.

StorageGRID -Installationsarchiv

"Laden Sie das StorageGRID Installationsarchiv herunter und extrahieren Sie die Dateien" .

Service-Laptop

Die Installation des StorageGRID -Systems erfolgt über einen Service-Laptop.

Der Dienstlaptop muss über Folgendes verfügen:

- Netzwerkanschluss
- SSH-Client (z. B. PuTTY)
- "Unterstützte Webbrowser"

StorageGRID -Dokumentation

- "Versionshinweise"
- "Anleitung zur Administration von StorageGRID"

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Sie müssen das StorageGRID Installationsarchiv herunterladen und die erforderlichen Dateien extrahieren. Optional können Sie die Dateien im Installationspaket manuell überprüfen.

Schritte

1. Gehen Sie zum "NetApp -Downloadseite für StorageGRID" .
2. Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version oder wählen Sie eine andere Version aus dem Dropdown-Menü und wählen Sie **Los**.
3. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Ihr NetApp -Konto an .
4. Wenn eine Warnung/ein unbedingt zu lesender Hinweis erscheint, lesen Sie ihn und aktivieren Sie das Kontrollkästchen.

   Sie müssen alle erforderlichen Hotfixes anwenden, nachdem Sie die StorageGRID Version installiert haben. Weitere Informationen finden Sie im"Hotfix-Verfahren in den Wiederherstellungs- und Wartungsanweisungen"

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.
6. Wählen Sie in der Spalte * StorageGRID installieren* das .tgz- oder .zip-Installationsarchiv für Ubuntu oder Debian aus.

   Wählen Sie die `.zip` Datei, wenn Sie Windows auf dem Service-Laptop ausführen.

7. Speichern Sie das Installationsarchiv.
8. Wenn Sie das Installationsarchiv überprüfen müssen:
   a. Laden Sie das StorageGRID -Codesignaturüberprüfungspaket herunter. Der Dateiname für dieses Paket verwendet das Format `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , Wo `<version-number>` ist die StorageGRID -Softwareversion.
   b. Folgen Sie den Schritten, um"Überprüfen Sie die Installationsdateien manuell" .
9. Extrahieren Sie die Dateien aus dem Installationsarchiv.
10. Wählen Sie die benötigten Dateien aus.

    Welche Dateien Sie benötigen, hängt von Ihrer geplanten Grid-Topologie und der Art und Weise ab, wie Sie Ihr StorageGRID -System bereitstellen.

    Die in der Tabelle aufgeführten Pfade beziehen sich auf das oberste Verzeichnis, das durch das extrahierte Installationsarchiv installiert wird.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine nicht für die Produktion NetApp -Lizenzdatei, die Sie für Tests und Proof-of-Concept-Bereitstellungen verwenden können.
	DEB-Paket zum Installieren der StorageGRID -Knotenimages auf Ubuntu- oder Debian-Hosts.

Pfad und Dateiname	Beschreibung
	MD5-Prüfsumme für die Datei `/debs/storagegrid-webscale-images-version-SHA.deb` .
	DEB-Paket zum Installieren des StorageGRID -Hostdienstes auf Ubuntu- oder Debian-Hosts.
Bereitstellungsskripttool	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Beispiel für eine Ansible-Rolle und ein Playbook zum Konfigurieren von Ubuntu- oder Debian-Hosts für die Bereitstellung von StorageGRID Containern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.

Pfad und Dateiname	Beschreibung
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

Installationsdateien manuell überprüfen (optional)

Bei Bedarf können Sie die Dateien im StorageGRID Installationsarchiv manuell überprüfen.

Bevor Sie beginnen

Du hast"das Verifizierungspaket heruntergeladen" aus dem "NetApp -Downloadseite für StorageGRID" .

Schritte

1. Extrahieren Sie die Artefakte aus dem Verifizierungspaket:

   ```
   tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
   ```

2. Stellen Sie sicher, dass diese Artefakte extrahiert wurden:
   - Blattzertifikat: `Leaf-Cert.pem`
   - Zertifikatskette: `CA-Int-Cert.pem`
   - Zeitstempel-Antwortkette: `TS-Cert.pem`
   - Prüfsummendatei: `sha256sum`
   - Prüfsummensignatur: `sha256sum.sig`
   - Zeitstempel-Antwortdatei: `sha256sum.sig.tsr`
3. Verwenden Sie die Kette, um zu überprüfen, ob das Blattzertifikat gültig ist.

   Beispiel: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

   Erwartete Ausgabe: `Leaf-Cert.pem: OK`

4. Wenn Schritt *2* aufgrund eines abgelaufenen Blattzertifikats fehlgeschlagen ist, verwenden Sie die `tsr` zu überprüfende Datei.

   Beispiel: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

   Die erwartete Ausgabe umfasst: `Verification: OK`

5. Erstellen Sie eine öffentliche Schlüsseldatei aus dem Blattzertifikat.

Beispiel: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Erwartete Ausgabe: *keine*

6. Verwenden Sie den öffentlichen Schlüssel, um die `sha256sum` Datei gegen `sha256sum.sig` .

   Beispiel: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   Erwartete Ausgabe: `Verified OK`

7. Überprüfen Sie die `sha256sum` Dateiinhalte mit neu erstellten Prüfsummen vergleichen.

   Beispiel: `sha256sum -c sha256sum`

   Erwartete Ausgabe: *<filename>*`: OK`
   <filename> ist der Name der Archivdatei, die Sie heruntergeladen haben.

8. "Führen Sie die restlichen Schritte aus"um die entsprechenden Installationsdateien zu extrahieren und auszuwählen.

Softwareanforderungen für Ubuntu und Debian

Sie können eine virtuelle Maschine verwenden, um jeden StorageGRID Knotentyp zu hosten. Sie benötigen eine virtuelle Maschine für jeden Grid-Knoten.

Um StorageGRID auf Ubuntu oder Debian zu installieren, müssen Sie einige Softwarepakete von Drittanbietern installieren. Einige unterstützte Linux-Distributionen enthalten diese Pakete nicht standardmäßig. Zu den Softwarepaketversionen, auf denen StorageGRID Installationen getestet werden, gehören die auf dieser Seite aufgeführten.

Wenn Sie eine Linux-Distribution und eine Container-Runtime-Installationsoption auswählen, die eines dieser Pakete erfordert und diese nicht automatisch von der Linux-Distribution installiert werden, installieren Sie eine der hier aufgeführten Versionen, sofern diese von Ihrem Provider oder dem unterstützenden Anbieter für Ihre Linux-Distribution verfügbar ist. Verwenden Sie andernfalls die von Ihrem Anbieter verfügbaren Standardpaketversionen.

Alle Installationsoptionen erfordern entweder Podman oder Docker. Installieren Sie nicht beide Pakete. Installieren Sie nur das Paket, das für Ihre Installationsoption erforderlich ist.

> Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt.

Getestete Python-Versionen

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1

- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Getestete Podman-Versionen

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Getestete Docker-Versionen

Die Docker-Unterstützung ist veraltet und wird in einer zukünftigen Version entfernt.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1
- Docker-CE 24.0.7-1
- 1,5-2

CPU- und RAM-Anforderungen

Überprüfen und konfigurieren Sie vor der Installation der StorageGRID -Software die Hardware, sodass sie das StorageGRID -System unterstützen kann.

Jeder StorageGRID -Knoten benötigt die folgenden Mindestressourcen:

- CPU-Kerne: 8 pro Knoten
- RAM: Abhängig vom insgesamt verfügbaren RAM und der Menge der auf dem System ausgeführten Nicht-StorageGRID -Software
  - Im Allgemeinen mindestens 24 GB pro Knoten und 2 bis 16 GB weniger als der gesamte System-RAM
  - Mindestens 64 GB für jeden Mandanten mit etwa 5.000 Buckets

Softwarebasierte Knotenressourcen, die nur Metadaten enthalten, müssen mit den vorhandenen

Speicherknotenressourcen übereinstimmen. Beispiel:

- Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
  - 128 GB RAM
  - 8-Kern-CPU
  - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)
- Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).

Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

Stellen Sie sicher, dass die Anzahl der StorageGRID -Knoten, die Sie auf jedem physischen oder virtuellen Host ausführen möchten, die Anzahl der verfügbaren CPU-Kerne oder des physischen RAM nicht überschreitet. Wenn die Hosts nicht ausschließlich für die Ausführung von StorageGRID vorgesehen sind (nicht empfohlen), müssen Sie unbedingt den Ressourcenbedarf der anderen Anwendungen berücksichtigen.

> Überwachen Sie regelmäßig Ihre CPU- und Speichernutzung, um sicherzustellen, dass diese Ressourcen weiterhin Ihrer Arbeitslast gerecht werden. Beispielsweise würde eine Verdoppelung der RAM- und CPU-Zuweisung für virtuelle Speicherknoten ähnliche Ressourcen bereitstellen wie für StorageGRID Appliance-Knoten. Wenn die Menge der Metadaten pro Knoten 500 GB übersteigt, sollten Sie außerdem eine Erhöhung des RAM pro Knoten auf 48 GB oder mehr in Betracht ziehen. Informationen zum Verwalten des Objektmetadatenspeichers, zum Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten und zum Überwachen der CPU- und Speicherauslastung finden Sie in den Anweisungen für"Verabreichung" ,"Überwachung" , Und"Upgrade" StorageGRID.

Wenn Hyperthreading auf den zugrunde liegenden physischen Hosts aktiviert ist, können Sie 8 virtuelle Kerne (4 physische Kerne) pro Knoten bereitstellen. Wenn Hyperthreading auf den zugrunde liegenden physischen Hosts nicht aktiviert ist, müssen Sie 8 physische Kerne pro Knoten bereitstellen.

Wenn Sie virtuelle Maschinen als Hosts verwenden und die Kontrolle über die Größe und Anzahl der VMs haben, sollten Sie für jeden StorageGRID Knoten eine einzelne VM verwenden und die VM entsprechend dimensionieren.

Bei Produktionsbereitstellungen sollten Sie nicht mehrere Speicherknoten auf derselben physischen Speicherhardware oder demselben virtuellen Host ausführen. Jeder Speicherknoten in einer einzelnen StorageGRID Bereitstellung sollte sich in seiner eigenen isolierten Fehlerdomäne befinden. Sie können die Haltbarkeit und Verfügbarkeit von Objektdaten maximieren, wenn Sie sicherstellen, dass ein einzelner Hardwarefehler nur einen einzelnen Speicherknoten beeinträchtigen kann.

Siehe auch "Speicher- und Leistungsanforderungen".

Speicher- und Leistungsanforderungen

Sie müssen die Speicheranforderungen für StorageGRID -Knoten verstehen, damit Sie genügend Speicherplatz für die Erstkonfiguration und zukünftige Speichererweiterungen bereitstellen können.

StorageGRID -Knoten erfordern drei logische Speicherkategorien:

- **Containerpool** – Performance-Tier-Speicher (10K SAS oder SSD) für die Knotencontainer, der dem Docker-Speichertreiber zugewiesen wird, wenn Sie Docker auf den Hosts installieren und konfigurieren, die Ihre StorageGRID Knoten unterstützen.
- **Systemdaten** – Performance-Tier-Speicher (10K SAS oder SSD) für die dauerhafte Speicherung von Systemdaten und Transaktionsprotokollen pro Knoten, die von den StorageGRID Hostdiensten genutzt und einzelnen Knoten zugeordnet werden.
- **Objektdaten** – Speicher der Leistungsstufe (10K SAS oder SSD) und Massenspeicher der Kapazitätsstufe (NL-SAS/SATA) für die dauerhafte Speicherung von Objektdaten und Objektmetadaten.

Sie müssen für alle Speicherkategorien RAID-gestützte Blockgeräte verwenden. Nicht redundante Festplatten, SSDs oder JBODs werden nicht unterstützt. Sie können für jede Speicherkategorie gemeinsam genutzten oder lokalen RAID-Speicher verwenden. Wenn Sie jedoch die Knotenmigrationsfunktion in StorageGRID verwenden möchten, müssen Sie sowohl Systemdaten als auch Objektdaten auf gemeinsam genutztem Speicher speichern. Weitere Informationen finden Sie unter "Anforderungen für die Migration von Knotencontainern" .

Leistungsanforderungen

Die Leistung der für den Containerpool, die Systemdaten und die Objektmetadaten verwendeten Volumes hat erhebliche Auswirkungen auf die Gesamtleistung des Systems. Sie sollten für diese Volumes Speicher der Leistungsstufe (10K SAS oder SSD) verwenden, um eine angemessene Festplattenleistung hinsichtlich Latenz, Eingabe-/Ausgabevorgängen pro Sekunde (IOPS) und Durchsatz sicherzustellen. Sie können Capacity-Tier-Speicher (NL-SAS/SATA) für die dauerhafte Speicherung von Objektdaten verwenden.

Für die für den Containerpool, die Systemdaten und die Objektdaten verwendeten Volumes muss das Write-Back-Caching aktiviert sein. Der Cache muss sich auf einem geschützten oder dauerhaften Medium befinden.

Anforderungen für Hosts, die NetApp ONTAP -Speicher verwenden

Wenn der StorageGRID Knoten Speicher verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass für das Volume keine FabricPool -Tiering-Richtlinie aktiviert ist. Das Deaktivieren der FabricPool Tiering-Funktion für Volumes, die mit StorageGRID -Knoten verwendet werden, vereinfacht die Fehlerbehebung und Speichervorgänge.

> Verwenden Sie FabricPool niemals, um Daten im Zusammenhang mit StorageGRID zurück auf StorageGRID selbst zu verschieben. Das Zurückführen von StorageGRID -Daten in StorageGRID erhöht die Fehlerbehebung und die Betriebskomplexität.

Anzahl der benötigten Hosts

Jeder StorageGRID Standort benötigt mindestens drei Speicherknoten.

> Führen Sie bei einer Produktionsbereitstellung nicht mehr als einen Speicherknoten auf einem einzelnen physischen oder virtuellen Host aus. Durch die Verwendung eines dedizierten Hosts für jeden Speicherknoten wird eine isolierte Fehlerdomäne bereitgestellt.

Andere Knotentypen, wie etwa Admin-Knoten oder Gateway-Knoten, können auf denselben Hosts oder je nach Bedarf auf eigenen dedizierten Hosts bereitgestellt werden.

Anzahl der Speichervolumes für jeden Host

Die folgende Tabelle zeigt die Anzahl der für jeden Host erforderlichen Speichervolumes (LUNs) und die für

jede LUN erforderliche Mindestgröße, basierend darauf, welche Knoten auf diesem Host bereitgestellt werden.

Die maximal getestete LUN-Größe beträgt 39 TB.

Diese Zahlen gelten für jeden Host, nicht für das gesamte Grid.

LUN-Zweck	Speicherkategorie	Anzahl der LUNs	Mindestgröße/LUN
Container-Engine-Speicherpool	Containerpool	1	Gesamtzahl der Knoten × 100 GB
`/var/local`Volumen	Systemdaten	1 für jeden Knoten auf diesem Host	90 GB
Speicherknoten	Objektdaten	3 für jeden Speicherknoten auf diesem Host **Hinweis:** Ein softwarebasierter Speicherknoten kann 1 bis 48 Speichervolumes haben; mindestens 3 Speichervolumes werden empfohlen.	12 TB (4 TB/LUN) SieheSpeicheranforderungen für Speicherknoten für weitere Informationen.
Speicherknoten (nur Metadaten)	Objektmetadaten	1	4 TB SieheSpeicheranforderungen für Speicherknoten für weitere Informationen. **Hinweis**: Für reine Metadaten-Speicherknoten ist nur eine Rangedb erforderlich.
Audit-Protokolle des Admin-Knotens	Systemdaten	1 für jeden Admin-Knoten auf diesem Host	200 GB
Admin-Knotentabellen	Systemdaten	1 für jeden Admin-Knoten auf diesem Host	200 GB

Abhängig von der konfigurierten Prüfebene, der Größe der Benutzereingaben wie dem S3-Objektschlüsselnamen und der Menge der zu bewahrenden Prüfprotokolldaten müssen Sie möglicherweise die Größe der Prüfprotokoll-LUN auf jedem Admin-Knoten erhöhen. Im Allgemeinen generiert ein Grid ungefähr 1 KB Prüfdaten pro S3-Vorgang, was bedeuten würde, dass ein 200 GB großes LUN 70 Millionen Vorgänge pro Tag oder 800 Vorgänge pro Sekunde für zwei bis drei Tage unterstützen würde.

Mindestspeicherplatz für einen Host

Die folgende Tabelle zeigt den für jeden Knotentyp erforderlichen Mindestspeicherplatz. Mithilfe dieser Tabelle können Sie die Mindestspeichermenge ermitteln, die Sie dem Host in jeder Speicherkategorie bereitstellen

müssen, basierend darauf, welche Knoten auf diesem Host bereitgestellt werden.

> Festplatten-Snapshots können nicht zum Wiederherstellen von Grid-Knoten verwendet werden. Beziehen Sie sich stattdessen auf die"Wiederherstellung von Grid-Knoten" Verfahren für jeden Knotentyp.

Knotentyp	Containerpool	Systemdaten	Objektdaten
Speicherknoten	100 GB	90 GB	4.000 GB
Admin-Knoten	100 GB	490 GB (3 LUNs)	*nicht zutreffend*
Gateway-Knoten	100 GB	90 GB	*nicht zutreffend*

Beispiel: Berechnung des Speicherbedarfs für einen Host

Angenommen, Sie planen, drei Knoten auf demselben Host bereitzustellen: einen Speicherknoten, einen Admin-Knoten und einen Gateway-Knoten. Sie sollten dem Host mindestens neun Speichervolumes zur Verfügung stellen. Sie benötigen mindestens 300 GB Performance-Tier-Speicher für die Knotencontainer, 670 GB Performance-Tier-Speicher für Systemdaten und Transaktionsprotokolle und 12 TB Capacity-Tier-Speicher für Objektdaten.

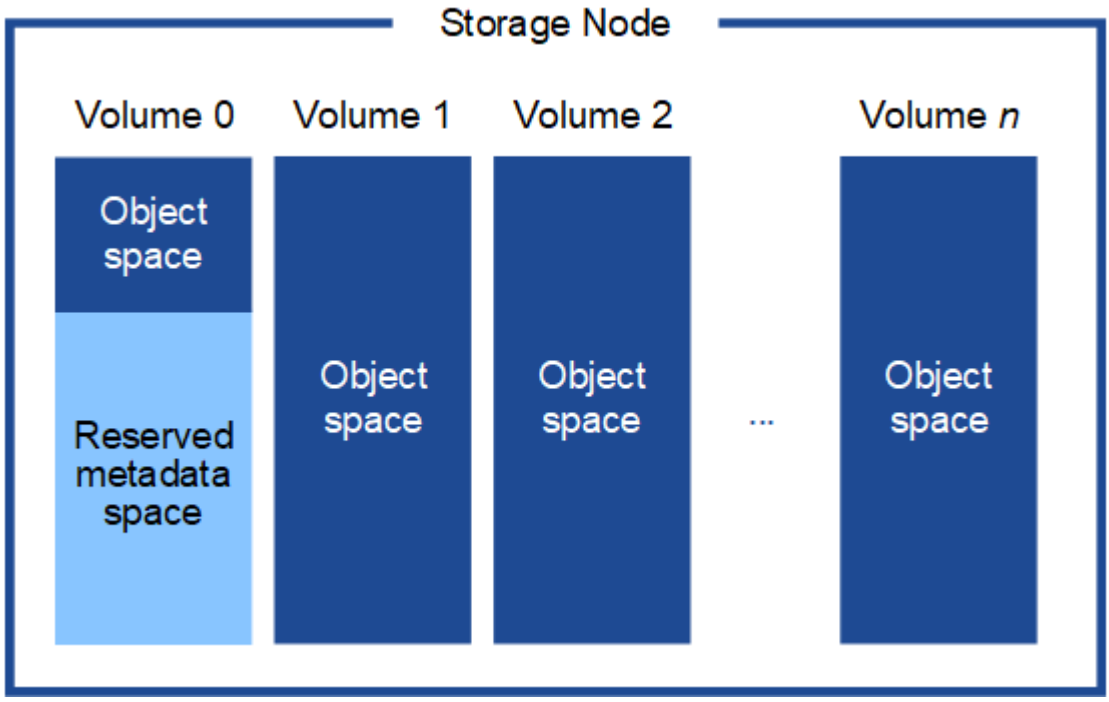
Knotentyp	LUN-Zweck	Anzahl der LUNs	LUN-Größe
Speicherknoten	Docker-Speicherpool	1	300 GB (100 GB/Knoten)
Speicherknoten	`/var/local`Volumen	1	90 GB
Speicherknoten	Objektdaten	3	12 TB (4 TB/LUN)
Admin-Knoten	`/var/local`Volumen	1	90 GB
Admin-Knoten	Audit-Protokolle des Admin-Knotens	1	200 GB
Admin-Knoten	Admin-Knotentabellen	1	200 GB
Gateway-Knoten	`/var/local`Volumen	1	90 GB
Gesamt		**9**	**Containerpool:** 300 GB **Systemdaten:** 670 GB **Objektdaten:** 12.000 GB

Speicheranforderungen für Speicherknoten

Ein softwarebasierter Speicherknoten kann 1 bis 48 Speichervolumes haben; 3 oder mehr Speichervolumes werden empfohlen. Jedes Speichervolumen sollte mindestens 4 TB groß sein.

Ein Appliance-Speicherknoten kann außerdem über bis zu 48 Speichervolumes verfügen.

Wie in der Abbildung gezeigt, reserviert StorageGRID Speicherplatz für Objektmetadaten auf Speichervolume 0 jedes Speicherknotens. Der verbleibende Speicherplatz auf Speichervolume 0 und allen anderen Speichervolumes im Speicherknoten wird ausschließlich für Objektdaten verwendet.



Um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen, speichert StorageGRID an jedem Standort drei Kopien der Metadaten für alle Objekte im System. Die drei Kopien der Objektmetadaten werden gleichmäßig auf alle Speicherknoten an jedem Standort verteilt.

Wenn Sie ein Grid mit reinen Metadaten-Speicherknoten installieren, muss das Grid auch eine Mindestanzahl von Knoten für die Objektspeicherung enthalten. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

- Für ein Single-Site-Grid werden mindestens zwei Storage Nodes für Objekte und Metadaten konfiguriert.
- Für ein Multi-Site-Grid wird mindestens ein Storage Node pro Site für Objekte und Metadaten konfiguriert.

Wenn Sie dem Datenträger 0 eines neuen Speicherknotens Speicherplatz zuweisen, müssen Sie sicherstellen, dass für den Teil aller Objektmetadaten dieses Knotens ausreichend Speicherplatz vorhanden ist.

- Sie müssen dem Volume 0 mindestens 4 TB zuweisen.

  Wenn Sie für einen Speicherknoten nur ein Speichervolume verwenden und dem Volume 4 TB oder weniger zuweisen, wechselt der Speicherknoten beim Start möglicherweise in den schreibgeschützten Speicherzustand und speichert nur Objektmetadaten.

  Wenn Sie Volume 0 (nur für nicht produktive Verwendung) weniger als 500 GB zuweisen, werden 10 % der Kapazität des Speichervolumes für Metadaten reserviert.

- Softwarebasierte Knotenressourcen, die nur Metadaten enthalten, müssen mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:

    - Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
        - 128 GB RAM
        - 8-Kern-CPU
        - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)
    - Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).

      Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

- Wenn Sie ein neues System (StorageGRID 11.6 oder höher) installieren und jeder Speicherknoten über 128 GB oder mehr RAM verfügt, weisen Sie Volume 0 8 TB oder mehr zu. Durch die Verwendung eines größeren Werts für Volume 0 kann der für Metadaten auf jedem Speicherknoten zulässige Speicherplatz erhöht werden.
- Wenn Sie verschiedene Speicherknoten für eine Site konfigurieren, verwenden Sie nach Möglichkeit dieselbe Einstellung für Volume 0. Wenn eine Site Speicherknoten unterschiedlicher Größe enthält, bestimmt der Speicherknoten mit dem kleinsten Volume 0 die Metadatenkapazität dieser Site.

Weitere Informationen finden Sie unter"Verwalten des Objektmetadatenspeichers" .

Anforderungen für die Migration von Knotencontainern

Mit der Knotenmigrationsfunktion können Sie einen Knoten manuell von einem Host auf einen anderen verschieben. Normalerweise befinden sich beide Hosts im selben physischen Rechenzentrum.

Durch die Knotenmigration können Sie die Wartung physischer Hosts durchführen, ohne den Grid-Betrieb zu unterbrechen. Sie verschieben alle StorageGRID -Knoten einzeln auf einen anderen Host, bevor Sie den physischen Host offline nehmen. Die Migration von Knoten erfordert nur eine kurze Ausfallzeit für jeden Knoten und sollte den Betrieb oder die Verfügbarkeit von Grid-Diensten nicht beeinträchtigen.

Wenn Sie die StorageGRID -Knotenmigrationsfunktion verwenden möchten, muss Ihre Bereitstellung zusätzliche Anforderungen erfüllen:

- Einheitliche Netzwerkschnittstellennamen für alle Hosts in einem einzigen physischen Rechenzentrum
- Gemeinsam genutzter Speicher für StorageGRID -Metadaten und Objekt-Repository-Volumes, auf den alle Hosts in einem einzigen physischen Rechenzentrum zugreifen können. Sie könnten beispielsweise Speicher-Arrays der NetApp E-Serie verwenden.

Wenn Sie virtuelle Hosts verwenden und die zugrunde liegende Hypervisor-Schicht die VM-Migration unterstützt, möchten Sie diese Funktion möglicherweise anstelle der Knotenmigrationsfunktion in StorageGRID verwenden. In diesem Fall können Sie diese zusätzlichen Anforderungen ignorieren.

Fahren Sie die Knoten ordnungsgemäß herunter, bevor Sie eine Migration oder Hypervisor-Wartung durchführen. Siehe die Anweisungen für"Herunterfahren eines Netzknotens" .

VMware Live Migration wird nicht unterstützt

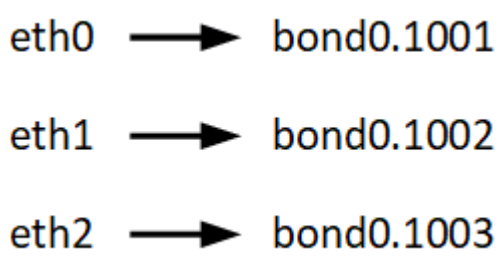
Bei der Durchführung einer Bare-Metal-Installation auf VMware-VMs führen OpenStack Live Migration und VMware Live vMotion dazu, dass die Uhrzeit der virtuellen Maschine springt, und werden für Grid-Knoten jeglicher Art nicht unterstützt. Obwohl es selten vorkommt, können falsche Uhrzeiten zum Verlust von Daten oder Konfigurationsaktualisierungen führen.

Kaltmigration wird unterstützt. Bei der Kaltmigration fahren Sie die StorageGRID -Knoten herunter, bevor Sie sie zwischen Hosts migrieren. Siehe die Anweisungen für"Herunterfahren eines Netzknotens" .

Konsistente Netzwerkschnittstellennamen

Um einen Knoten von einem Host auf einen anderen zu verschieben, muss der StorageGRID Hostdienst ein gewisses Vertrauen darin haben, dass die externe Netzwerkkonnektivität, über die der Knoten an seinem aktuellen Standort verfügt, am neuen Standort dupliziert werden kann. Diese Zuverlässigkeit wird durch die Verwendung konsistenter Netzwerkschnittstellennamen in den Hosts erreicht.

Nehmen wir beispielsweise an, dass StorageGRID NodeA, das auf Host1 ausgeführt wird, mit den folgenden Schnittstellenzuordnungen konfiguriert wurde:



Die linke Seite der Pfeile entspricht den herkömmlichen Schnittstellen, wie sie innerhalb eines StorageGRID Containers angezeigt werden (d. h. jeweils den Schnittstellen Grid, Admin und Client Network). Die rechte Seite der Pfeile entspricht den tatsächlichen Hostschnittstellen, die diese Netzwerke bereitstellen. Dabei handelt es sich um drei VLAN-Schnittstellen, die derselben physischen Schnittstellenverbindung untergeordnet sind.

Nehmen wir nun an, Sie möchten NodeA auf Host2 migrieren. Wenn Host2 auch über Schnittstellen mit den Namen bond0.1001, bond0.1002 und bond0.1003 verfügt, lässt das System die Verschiebung zu, da davon ausgegangen wird, dass die gleichnamigen Schnittstellen auf Host2 dieselbe Konnektivität bieten wie auf Host1. Wenn Host2 keine Schnittstellen mit denselben Namen hat, wird die Verschiebung nicht zugelassen.

Es gibt viele Möglichkeiten, eine konsistente Benennung der Netzwerkschnittstellen über mehrere Hosts hinweg zu erreichen. Siehe"Konfigurieren des Hostnetzwerks" für einige Beispiele.

Gemeinsam genutzter Speicher

Um schnelle Knotenmigrationen mit geringem Overhead zu erreichen, verschiebt die StorageGRID Knotenmigrationsfunktion die Knotendaten nicht physisch. Stattdessen wird die Knotenmigration wie folgt als Paar von Export- und Importvorgängen durchgeführt:

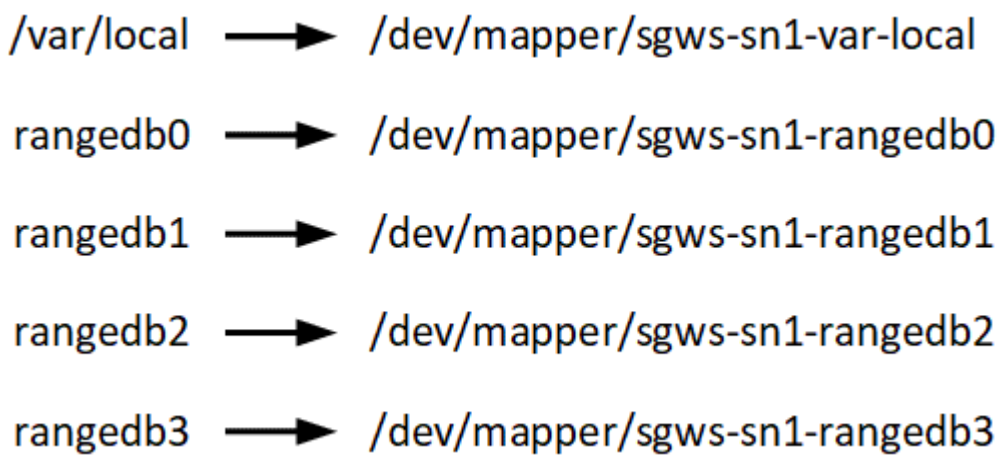
Schritte

1. Während des Vorgangs „Knotenexport“ wird eine kleine Menge persistenter Statusdaten aus dem auf HostA ausgeführten Knotencontainer extrahiert und auf dem Systemdatenvolume dieses Knotens zwischengespeichert. Anschließend wird der Knotencontainer auf HostA deinstanziiert.
2. Während des Vorgangs „Knotenimport“ wird der Knotencontainer auf HostB instanziiert, der dieselbe

Netzwerkschnittstelle und dieselben Blockspeicherzuordnungen verwendet, die auf HostA wirksam waren. Anschließend werden die zwischengespeicherten persistenten Statusdaten in die neue Instanz eingefügt.

Bei diesem Betriebsmodus müssen alle Systemdaten und Objektspeichervolumes des Knotens sowohl von HostA als auch von HostB aus zugänglich sein, damit die Migration zulässig ist und funktioniert. Darüber hinaus müssen sie mit Namen in den Knoten abgebildet worden sein, die garantiert auf dieselben LUNs auf HostA und HostB verweisen.

Das folgende Beispiel zeigt eine Lösung für die Blockgerätezuordnung für einen StorageGRID Speicherknoten, bei dem DM-Multipathing auf den Hosts verwendet wird und das Alias-Feld in `/etc/multipath.conf` um konsistente, benutzerfreundliche Blockgerätenamen bereitzustellen, die auf allen Hosts verfügbar sind.



Bereiten Sie die Hosts vor (Ubuntu oder Debian)

So ändern sich hostweite Einstellungen während der Installation

Auf Bare-Metal-Systemen nimmt StorageGRID einige Änderungen an hostweiten `sysctl` Einstellungen.

Folgende Änderungen werden vorgenommen:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
```

```
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
```

```
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Installieren Sie Linux

Sie müssen StorageGRID auf allen Ubuntu- oder Debian-Grid-Hosts installieren. Eine Liste der unterstützten Versionen erhalten Sie mit dem NetApp Interoperability Matrix Tool.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr Betriebssystem die unten aufgeführten Mindestanforderungen an die Kernelversion von StorageGRID erfüllt. Verwenden Sie den Befehl `uname -r` um die Kernelversion Ihres Betriebssystems zu erhalten, oder wenden Sie sich an den Anbieter Ihres Betriebssystems.

Hinweis: Die Unterstützung für die Ubuntu-Versionen 18.04 und 20.04 ist veraltet und wird in einer zukünftigen Version entfernt.

Ubuntu-Version	Mindestkernelversion	Name des Kernelpakets
18.04.6 (veraltet)	5.4.0-150-generisch	linux-image-5.4.0-150-generic/bionic-updates,bionic-security,now 5.4.0-150.167~18.04.1
20.04.5 (veraltet)	5.4.0-131-generisch	linux-image-5.4.0-131-generic/focal-updates,jetzt 5.4.0-131.147
22.04.1	5.15.0-47-generisch	linux-image-5.15.0-47-generic/jammy-updates,jammy-security,now 5.15.0-47.51
24,04	6.8.0-31-generisch	linux-image-6.8.0-31-generic/noble,jetzt 6.8.0-31.31

Hinweis: Die Unterstützung für Debian Version 11 ist veraltet und wird in einer zukünftigen Version entfernt.

Debian-Version	Mindestkernelversion	Name des Kernelpakets
11 (veraltet)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable,now 5.10.150-1

Debian-Version	Mindestkernelversion	Name des Kernelpakets
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable,now 6.1.27-1

Schritte

1. Installieren Sie Linux auf allen physischen oder virtuellen Grid-Hosts gemäß den Anweisungen des Distributors oder Ihrem Standardverfahren.

   > Installieren Sie keine grafischen Desktopumgebungen. Bei der Installation von Ubuntu müssen Sie **Standardsystemdienstprogramme** auswählen. Es wird empfohlen, **OpenSSH-Server** auszuwählen, um den SSH-Zugriff auf Ihre Ubuntu-Hosts zu ermöglichen. Alle anderen Optionen können deaktiviert bleiben.

2. Stellen Sie sicher, dass alle Hosts Zugriff auf Ubuntu- oder Debian-Paket-Repositories haben.
3. Wenn Swap aktiviert ist:
   a. Führen Sie den folgenden Befehl aus: `$ sudo swapoff --all`
   b. Entfernen Sie alle Swap-Einträge aus `/etc/fstab` um die Einstellungen beizubehalten.

   > Wenn Sie den Swap-Vorgang nicht vollständig deaktivieren, kann dies zu erheblichen Leistungseinbußen führen.

Verstehen Sie die Installation des AppArmor-Profils

Wenn Sie in einer selbst bereitgestellten Ubuntu-Umgebung arbeiten und das obligatorische Zugriffskontrollsystem AppArmor verwenden, werden die AppArmor-Profile, die mit den Paketen verknüpft sind, die Sie auf dem Basissystem installieren, möglicherweise durch die entsprechenden Pakete blockiert, die mit StorageGRID installiert wurden.

Standardmäßig werden AppArmor-Profile für Pakete installiert, die Sie auf dem Basisbetriebssystem installieren. Wenn Sie diese Pakete aus dem StorageGRID -Systemcontainer ausführen, werden die AppArmor-Profile blockiert. Die DHCP-, MySQL-, NTP- und tcdump-Basispakete stehen im Konflikt mit AppArmor, und auch bei anderen Basispaketen kann es zu Konflikten kommen.

Sie haben zwei Möglichkeiten, AppArmor-Profile zu handhaben:

- Deaktivieren Sie einzelne Profile für die auf dem Basissystem installierten Pakete, die sich mit den Paketen im StorageGRID -Systemcontainer überschneiden. Wenn Sie einzelne Profile deaktivieren, wird in den StorageGRID -Protokolldateien ein Eintrag angezeigt, der angibt, dass AppArmor aktiviert ist.

  Verwenden Sie die folgenden Befehle:

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

  Beispiel:

```
sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/bin.ping
```

- Deaktivieren Sie AppArmor vollständig. Befolgen Sie für Ubuntu 9.10 oder höher die Anweisungen in der Ubuntu-Online-Community: "AppArmor deaktivieren" . Das vollständige Deaktivieren von AppArmor ist bei neueren Ubuntu-Versionen möglicherweise nicht möglich.

  Nachdem Sie AppArmor deaktiviert haben, werden in den StorageGRID Protokolldateien keine Einträge angezeigt, die darauf hinweisen, dass AppArmor aktiviert ist.

Konfigurieren Sie das Hostnetzwerk (Ubuntu oder Debian).

Nachdem Sie die Linux-Installation auf Ihren Hosts abgeschlossen haben, müssen Sie möglicherweise einige zusätzliche Konfigurationen durchführen, um auf jedem Host eine Reihe von Netzwerkschnittstellen vorzubereiten, die für die Zuordnung zu den StorageGRID -Knoten geeignet sind, die Sie später bereitstellen.

Bevor Sie beginnen

- Sie haben die"StorageGRID Netzwerkrichtlinien" .
- Sie haben die Informationen zu"Anforderungen für die Migration von Knotencontainern" .
- Wenn Sie virtuelle Hosts verwenden, haben Sie dieÜberlegungen und Empfehlungen zum Klonen von MAC-Adressen bevor Sie das Hostnetzwerk konfigurieren.

> ⓘ Wenn Sie VMs als Hosts verwenden, sollten Sie VMXNET 3 als virtuellen Netzwerkadapter auswählen. Der VMware E1000-Netzwerkadapter hat Verbindungsprobleme mit StorageGRID -Containern verursacht, die auf bestimmten Linux-Distributionen bereitgestellt wurden.

Informationen zu diesem Vorgang

Grid-Knoten müssen auf das Grid-Netzwerk und optional auf die Admin- und Client-Netzwerke zugreifen können. Sie stellen diesen Zugriff bereit, indem Sie Zuordnungen erstellen, die die physische Schnittstelle des Hosts mit den virtuellen Schnittstellen für jeden Grid-Knoten verknüpfen. Verwenden Sie beim Erstellen von Hostschnittstellen benutzerfreundliche Namen, um die Bereitstellung auf allen Hosts zu erleichtern und die Migration zu ermöglichen.

Dieselbe Schnittstelle kann zwischen dem Host und einem oder mehreren Knoten gemeinsam genutzt werden. Sie können beispielsweise dieselbe Schnittstelle für den Hostzugriff und den Knotenadministrator-Netzwerkzugriff verwenden, um die Host- und Knotenwartung zu vereinfachen. Obwohl die gleiche Schnittstelle zwischen dem Host und einzelnen Knoten gemeinsam genutzt werden kann, müssen alle unterschiedliche IP-Adressen haben. IP-Adressen können nicht zwischen Knoten oder zwischen dem Host und einem Knoten geteilt werden.

Sie können dieselbe Host-Netzwerkschnittstelle verwenden, um die Grid-Netzwerkschnittstelle für alle StorageGRID -Knoten auf dem Host bereitzustellen. Sie können für jeden Knoten eine andere Host-Netzwerkschnittstelle verwenden oder einen Mittelweg wählen. Normalerweise würden Sie jedoch nicht dieselbe Host-Netzwerkschnittstelle sowohl als Grid- als auch als Admin-Netzwerkschnittstelle für einen einzelnen Knoten oder als Grid-Netzwerkschnittstelle für einen Knoten und als Client-Netzwerkschnittstelle für einen anderen bereitstellen.

Sie können diese Aufgabe auf viele Arten erledigen. Wenn es sich bei Ihren Hosts beispielsweise um virtuelle

Maschinen handelt und Sie für jeden Host einen oder zwei StorageGRID Knoten bereitstellen, können Sie die richtige Anzahl von Netzwerkschnittstellen im Hypervisor erstellen und eine 1:1-Zuordnung verwenden. Wenn Sie für den Produktionseinsatz mehrere Knoten auf Bare-Metal-Hosts bereitstellen, können Sie die Unterstützung des Linux-Netzwerk-Stacks für VLAN und LACP zur Fehlertoleranz und Bandbreitenfreigabe nutzen. Die folgenden Abschnitte bieten detaillierte Ansätze für beide Beispiele. Sie müssen keines dieser Beispiele verwenden; Sie können jeden Ansatz verwenden, der Ihren Anforderungen entspricht.

> Verwenden Sie Bond- oder Bridge-Geräte nicht direkt als Container-Netzwerkschnittstelle. Dies könnte den Start des Knotens verhindern, der durch ein Kernelproblem bei der Verwendung von MACVLAN mit Bond- und Bridge-Geräten im Container-Namespace verursacht wird. Verwenden Sie stattdessen ein nicht gebundenes Gerät, beispielsweise ein VLAN oder ein virtuelles Ethernet-Paar (veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Knotenkonfigurationsdatei an.

Überlegungen und Empfehlungen zum Klonen von MAC-Adressen

Durch das Klonen von MAC-Adressen verwendet der Container die MAC-Adresse des Hosts und der Host die MAC-Adresse einer von Ihnen angegebenen oder einer zufällig generierten Adresse. Sie sollten das Klonen von MAC-Adressen verwenden, um die Verwendung von Netzwerkkonfigurationen im Promiscuous-Modus zu vermeiden.

Aktivieren des MAC-Klonens

In bestimmten Umgebungen kann die Sicherheit durch das Klonen von MAC-Adressen verbessert werden, da Sie dadurch eine dedizierte virtuelle Netzwerkkarte für das Admin-Netzwerk, das Grid-Netzwerk und das Client-Netzwerk verwenden können. Wenn der Container die MAC-Adresse der dedizierten Netzwerkkarte auf dem Host verwendet, können Sie die Verwendung von Netzwerkkonfigurationen im Promiscuous-Modus vermeiden.

> Das Klonen von MAC-Adressen ist für die Verwendung mit virtuellen Serverinstallationen vorgesehen und funktioniert möglicherweise nicht bei allen physischen Gerätekonfigurationen ordnungsgemäß.

> Wenn der Start eines Knotens fehlschlägt, weil eine auf MAC-Klonen ausgerichtete Schnittstelle belegt ist, müssen Sie die Verbindung möglicherweise auf „inaktiv“ setzen, bevor Sie den Knoten starten. Darüber hinaus ist es möglich, dass die virtuelle Umgebung das MAC-Klonen auf einer Netzwerkschnittstelle verhindert, während die Verbindung aktiv ist. Wenn ein Knoten die MAC-Adresse nicht festlegen und nicht starten kann, weil eine Schnittstelle belegt ist, kann das Problem möglicherweise behoben werden, indem die Verbindung vor dem Starten des Knotens auf „inaktiv“ gesetzt wird.

Das Klonen von MAC-Adressen ist standardmäßig deaktiviert und muss über Knotenkonfigurationsschlüssel festgelegt werden. Sie sollten es aktivieren, wenn Sie StorageGRID installieren.

Für jedes Netzwerk gibt es einen Schlüssel:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Wenn Sie den Schlüssel auf „true“ setzen, verwendet der Container die MAC-Adresse der Netzwerkkarte des Hosts. Zusätzlich verwendet der Host dann die MAC-Adresse des angegebenen Containernetzwerks. Standardmäßig ist die Containeradresse eine zufällig generierte Adresse. Wenn Sie jedoch eine Adresse mit dem `_NETWORK_MAC` Knotenkonfigurationsschlüssel, wird stattdessen diese Adresse verwendet. Host und Container haben immer unterschiedliche MAC-Adressen.

> Wenn Sie das MAC-Klonen auf einem virtuellen Host aktivieren, ohne gleichzeitig den Promiscuous-Modus auf dem Hypervisor zu aktivieren, kann dies dazu führen, dass die Linux-Host-Vernetzung über die Schnittstelle des Hosts nicht mehr funktioniert.

Anwendungsfälle für das MAC-Klonen

Beim MAC-Klonen sind zwei Anwendungsfälle zu berücksichtigen:

- MAC-Klonen nicht aktiviert: Wenn die `_CLONE_MAC` Schlüssel in der Knotenkonfigurationsdatei nicht festgelegt oder auf „false“ gesetzt ist, verwendet der Host die Host-NIC-MAC und der Container verfügt über eine von StorageGRID generierte MAC, sofern in der `_NETWORK_MAC` Schlüssel. Wenn eine Adresse im `_NETWORK_MAC` Schlüssel erhält der Container die Adresse, die im `_NETWORK_MAC` Schlüssel. Diese Tastenkonfiguration erfordert die Verwendung des Promiscuous-Modus.
- MAC-Klonen aktiviert: Wenn die `_CLONE_MAC` Schlüssel in der Knotenkonfigurationsdatei auf „true“ gesetzt ist, verwendet der Container die Host-NIC-MAC und der Host verwendet eine von StorageGRID generierte MAC, sofern in der `_NETWORK_MAC` Schlüssel. Wenn eine Adresse im `_NETWORK_MAC` Schlüssel verwendet der Host die angegebene Adresse anstelle einer generierten. Bei dieser Tastenkonfiguration sollten Sie den Promiscuous-Modus nicht verwenden.

> Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen das Empfangen und Senden von Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen erlauben möchten, stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppe für den Promiscuous-Modus, MAC-Adressänderungen und gefälschte Übertragungen auf **Akzeptieren** eingestellt sind. Die auf dem virtuellen Switch festgelegten Werte können durch die Werte auf Portgruppenebene überschrieben werden. Stellen Sie daher sicher, dass die Einstellungen an beiden Stellen identisch sind.

Informationen zum Aktivieren des MAC-Klonens finden Sie im"Anweisungen zum Erstellen von Knotenkonfigurationsdateien" .

Beispiel für MAC-Klonen

Beispiel für aktiviertes MAC-Klonen mit einem Host mit der MAC-Adresse 11:22:33:44:55:66 für die Schnittstelle ens256 und den folgenden Schlüsseln in der Knotenkonfigurationsdatei:

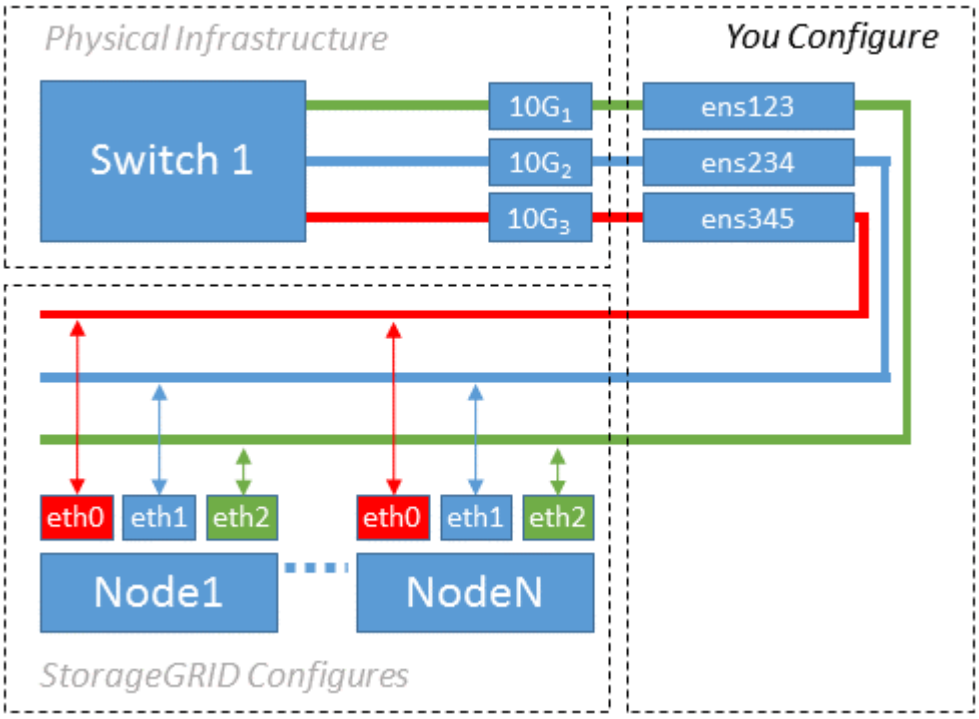
- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Ergebnis: Die Host-MAC für ens256 ist b2:9c:02:c2:27:10 und die Admin-Netzwerk-MAC ist 11:22:33:44:55:66

Beispiel 1: 1-zu-1-Zuordnung zu physischen oder virtuellen NICs

Beispiel 1 beschreibt eine einfache physische Schnittstellenzuordnung, die wenig oder keine Konfiguration auf

der Hostseite erfordert.



Das Linux-Betriebssystem erstellt die ensXYZ-Schnittstellen automatisch während der Installation oder beim Booten oder wenn die Schnittstellen im laufenden Betrieb hinzugefügt werden. Es ist keine Konfiguration erforderlich, außer sicherzustellen, dass die Schnittstellen so eingestellt sind, dass sie nach dem Booten automatisch hochgefahren werden. Sie müssen feststellen, welches ensXYZ welchem StorageGRID Netzwerk (Grid, Admin oder Client) entspricht, damit Sie später im Konfigurationsprozess die richtigen Zuordnungen bereitstellen können.

Beachten Sie, dass in der Abbildung mehrere StorageGRID -Knoten dargestellt sind. Normalerweise würden Sie diese Konfiguration jedoch für VMs mit einem einzelnen Knoten verwenden.

Wenn Switch 1 ein physischer Switch ist, sollten Sie die mit den Schnittstellen $10G_1$ bis $10G_3$ verbundenen Ports für den Zugriffsmodus konfigurieren und sie in den entsprechenden VLANs platzieren.

Beispiel 2: LACP-Bindung mit VLANs

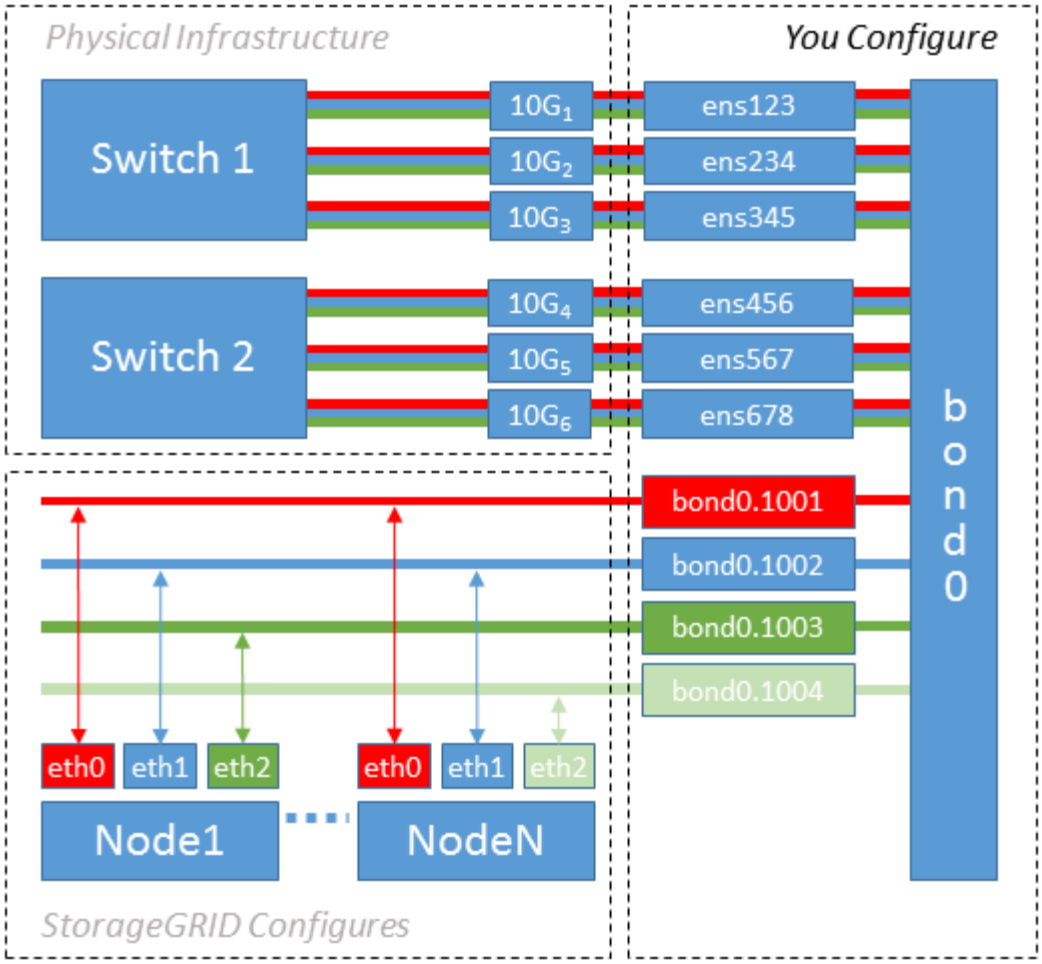
Beispiel 2 setzt voraus, dass Sie mit der Bündelung von Netzwerkschnittstellen und der Erstellung von VLAN-Schnittstellen auf der von Ihnen verwendeten Linux-Distribution vertraut sind.

Informationen zu diesem Vorgang

Beispiel 2 beschreibt ein generisches, flexibles, VLAN-basiertes Schema, das die gemeinsame Nutzung der gesamten verfügbaren Netzwerkbandbreite zwischen allen Knoten auf einem einzelnen Host ermöglicht. Dieses Beispiel ist insbesondere auf Bare-Metal-Hosts anwendbar.

Um dieses Beispiel zu verstehen, nehmen Sie an, dass Sie in jedem Rechenzentrum drei separate Subnetze für die Grid-, Admin- und Client-Netzwerke haben. Die Subnetze befinden sich auf separaten VLANs (1001, 1002 und 1003) und werden dem Host auf einem LACP-gebundenen Trunk-Port (bond0) präsentiert. Sie würden drei VLAN-Schnittstellen auf der Bindung konfigurieren: bond0.1001, bond0.1002 und bond0.1003.

Wenn Sie separate VLANs und Subnetze für Knotennetzwerke auf demselben Host benötigen, können Sie VLAN-Schnittstellen auf der Bindung hinzufügen und sie dem Host zuordnen (in der Abbildung als bond0.1004 angezeigt).



Schritte

1. Fassen Sie alle physischen Netzwerkschnittstellen, die für die StorageGRID -Netzwerkkonnektivität verwendet werden, in einer einzigen LACP-Verbindung zusammen.

   Verwenden Sie für die Bindung auf jedem Host denselben Namen, beispielsweise bond0.

2. Erstellen Sie VLAN-Schnittstellen, die diese Verbindung als ihr zugehöriges „physisches Gerät“ verwenden, und verwenden Sie dabei die Standard-Namenskonvention für VLAN-Schnittstellen. `physdev-name.VLAN ID`.

   Beachten Sie, dass für die Schritte 1 und 2 eine entsprechende Konfiguration der Edge-Switches erforderlich ist, die die anderen Enden der Netzwerkverbindungen abschließen. Die Edge-Switch-Ports müssen außerdem in einem LACP-Port-Kanal zusammengefasst, als Trunk konfiguriert und für die Weitergabe aller erforderlichen VLANs zugelassen werden.

   Es werden Beispiel-Schnittstellenkonfigurationsdateien für dieses Netzwerkkonfigurationsschema pro Host bereitgestellt.

Ähnliche Informationen

"Beispiel /etc/network/interfaces"

Konfigurieren des Hostspeichers

Sie müssen jedem Host Blockspeichervolumes zuweisen.

Bevor Sie beginnen

Sie haben die folgenden Themen überprüft, die die Informationen enthalten, die Sie zum Ausführen dieser Aufgabe benötigen:

- "Speicher- und Leistungsanforderungen"
- "Anforderungen für die Migration von Knotencontainern"

Informationen zu diesem Vorgang

Verwenden Sie beim Zuweisen von Blockspeichervolumes (LUNs) zu Hosts die Tabellen unter „Speicheranforderungen“, um Folgendes zu bestimmen:

- Anzahl der für jeden Host erforderlichen Volumes (basierend auf der Anzahl und den Typen der Knoten, die auf diesem Host bereitgestellt werden)
- Speicherkategorie für jedes Volume (d. h. Systemdaten oder Objektdaten)
- Größe jedes Volumens

Sie verwenden diese Informationen sowie den von Linux jedem physischen Volume zugewiesenen persistenten Namen, wenn Sie StorageGRID Knoten auf dem Host bereitstellen.

Sie müssen keines dieser Volumes partitionieren, formatieren oder mounten. Sie müssen lediglich sicherstellen, dass sie für die Hosts sichtbar sind.

Für reine Metadaten-Speicherknoten ist nur eine Objektdaten-LUN erforderlich.

Vermeiden Sie die Verwendung von „rohen“ speziellen Gerätedateien(`/dev/sdb` , zum Beispiel), während Sie Ihre Liste mit Datenträgernamen zusammenstellen. Diese Dateien können sich bei Neustarts des Hosts ändern, was sich auf den ordnungsgemäßen Betrieb des Systems auswirkt. Wenn Sie iSCSI-LUNs und Device Mapper Multipathing verwenden, sollten Sie Multipath-Aliase in der `/dev/mapper` Verzeichnis, insbesondere wenn Ihre SAN-Topologie redundante Netzwerkpfade zum gemeinsam genutzten Speicher enthält. Alternativ können Sie die vom System erstellten Softlinks unter `/dev/disk/by-path/` für Ihre persistenten Gerätenamen.

Beispiel:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Die Ergebnisse sind bei jeder Installation unterschiedlich.

Weisen Sie jedem dieser Blockspeichervolumes benutzerfreundliche Namen zu, um die Erstinstallation von StorageGRID und zukünftige Wartungsvorgänge zu vereinfachen. Wenn Sie den Device Mapper Multipath-Treiber für den redundanten Zugriff auf gemeinsam genutzte Speichervolumes verwenden, können Sie den `alias` Feld in Ihrem `/etc/multipath.conf` Datei.

Beispiel:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Wenn Sie das Alias-Feld auf diese Weise verwenden, werden die Aliase als Blockgeräte in der `/dev/mapper` Verzeichnis auf dem Host, sodass Sie einen benutzerfreundlichen, leicht zu validierenden Namen angeben können, wenn für einen Konfigurations- oder Wartungsvorgang die Angabe eines Blockspeicher-Volumes erforderlich ist.

Wenn Sie gemeinsam genutzten Speicher einrichten, um die Migration von StorageGRID -Knoten zu unterstützen und Device Mapper Multipathing verwenden, können Sie einen gemeinsamen `/etc/multipath.conf` auf allen gemeinsam genutzten Hosts. Stellen Sie einfach sicher, dass Sie auf jedem Host ein anderes Docker-Speichervolume verwenden. Die Verwendung von Aliasnamen und die Einbeziehung des Zielhostnamens in den Alias für jede Docker-Speichervolume-LUN erleichtert das Merken und wird empfohlen.

> Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt.

Ähnliche Informationen

- "Speicher- und Leistungsanforderungen"
- "Anforderungen für die Migration von Knotencontainern"

Konfigurieren des Speichervolumens der Container-Engine

Bevor Sie die Container-Engine (Docker oder Podman) installieren, müssen Sie möglicherweise das Speichervolume formatieren und mounten.

> Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt.

Informationen zu diesem Vorgang

Sie können diese Schritte überspringen, wenn Sie lokalen Speicher für das Docker-Speichervolume verwenden möchten und auf der Hostpartition ausreichend Speicherplatz verfügbar ist, der Folgendes enthält: `/var/lib` .

Schritte

1. Erstellen Sie ein Dateisystem auf dem Docker-Speichervolume:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Mounten Sie das Docker-Speichervolume:

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Fügen Sie einen Eintrag für Docker-Storage-Volume-Device zu /etc/fstab hinzu.

   Dieser Schritt stellt sicher, dass das Speichervolume nach dem Neustart des Hosts automatisch erneut bereitgestellt wird.

Docker installieren

Das StorageGRID -System läuft unter Linux als Sammlung von Docker-Containern. Bevor Sie StorageGRID installieren können, müssen Sie Docker installieren.

> Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt.

Schritte

1. Installieren Sie Docker, indem Sie den Anweisungen für Ihre Linux-Distribution folgen.

   > Wenn Docker nicht in Ihrer Linux-Distribution enthalten ist, können Sie es von der Docker-Website herunterladen.

2. Stellen Sie sicher, dass Docker aktiviert und gestartet wurde, indem Sie die folgenden beiden Befehle ausführen:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Bestätigen Sie, dass Sie die erwartete Version von Docker installiert haben, indem Sie Folgendes eingeben:

```
sudo docker version
```

Die Client- und Serverversionen müssen 1.11.0 oder höher sein.

Ähnliche Informationen

"Konfigurieren des Hostspeichers"

Installieren Sie die StorageGRID Hostdienste

Sie verwenden das StorageGRID DEB-Paket, um die StorageGRID Hostdienste zu installieren.

Informationen zu diesem Vorgang

Diese Anweisungen beschreiben, wie Sie die Hostdienste aus den DEB-Paketen installieren. Alternativ können Sie die im Installationsarchiv enthaltenen Metadaten des APT-Repositorys verwenden, um die DEB-Pakete remote zu installieren. Weitere Informationen finden Sie in den APT-Repository-Anweisungen für Ihr Linux-Betriebssystem.

Schritte

1. Kopieren Sie die StorageGRID DEB-Pakete auf jeden Ihrer Hosts oder stellen Sie sie auf einem gemeinsam genutzten Speicher zur Verfügung.

   Platzieren Sie sie beispielsweise in der `/tmp` Verzeichnis, sodass Sie den Beispielbefehl im nächsten Schritt verwenden können.

2. Melden Sie sich bei jedem Host als Root oder mit einem Konto mit Sudo-Berechtigung an und führen Sie die folgenden Befehle aus.

   Sie müssen die `images` Paket zuerst, und die `service` Paket Sekunde. Wenn Sie die Pakete in einem anderen Verzeichnis als `/tmp` , ändern Sie den Befehl, um den von Ihnen verwendeten Pfad wiederzugeben.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

Python 2,7 muss bereits installiert sein, bevor die StorageGRID -Pakete installiert werden können. Der `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` Der Befehl schlägt fehl, bis Sie dies getan haben.

Automatisieren Sie die Installation (Ubuntu oder Debian)

Sie können die Installation des StorageGRID Hostdienstes und die Konfiguration von Grid-Knoten automatisieren.

Informationen zu diesem Vorgang

Die Automatisierung der Bereitstellung kann in den folgenden Fällen nützlich sein:

- Sie verwenden bereits ein Standard-Orchestrierungsframework wie Ansible, Puppet oder Chef, um physische oder virtuelle Hosts bereitzustellen und zu konfigurieren.
- Sie beabsichtigen, mehrere StorageGRID Instanzen bereitzustellen.
- Sie stellen eine große, komplexe StorageGRID Instanz bereit.

Der StorageGRID -Hostdienst wird über ein Paket installiert und durch Konfigurationsdateien gesteuert, die während einer manuellen Installation interaktiv erstellt oder im Voraus (oder programmgesteuert) vorbereitet werden können, um eine automatisierte Installation mithilfe von Standard-Orchestrierungsframeworks zu ermöglichen. StorageGRID bietet optionale Python-Skripte zur Automatisierung der Konfiguration von StorageGRID -Geräten und des gesamten StorageGRID Systems (das „Grid“). Sie können diese Skripte direkt verwenden oder sie überprüfen, um zu erfahren, wie Sie die StorageGRID -Installations-REST-API in Grid-Bereitstellungs- und Konfigurationstools verwenden, die Sie selbst entwickeln.

Automatisieren Sie die Installation und Konfiguration des StorageGRID Hostdienstes

Sie können die Installation des StorageGRID Hostdienstes mithilfe von Standard-Orchestrierungsframeworks wie Ansible, Puppet, Chef, Fabric oder SaltStack automatisieren.

Der StorageGRID -Hostdienst ist in einem DEB verpackt und wird durch Konfigurationsdateien gesteuert, die im Voraus (oder programmgesteuert) vorbereitet werden können, um eine automatisierte Installation zu ermöglichen. Wenn Sie bereits ein Standard-Orchestrierungsframework zum Installieren und Konfigurieren von Ubuntu oder Debian verwenden, sollte das Hinzufügen von StorageGRID zu Ihren Playbooks oder Rezepten unkompliziert sein.

Sie können diese Aufgaben automatisieren:

1. Linux installieren
2. Linux konfigurieren
3. Konfigurieren von Host-Netzwerkschnittstellen zur Erfüllung der StorageGRID -Anforderungen
4. Konfigurieren des Hostspeichers zur Erfüllung der StorageGRID Anforderungen
5. Docker installieren
6. Installieren des StorageGRID Hostdienstes
7. Erstellen von StorageGRID -Knotenkonfigurationsdateien in `/etc/storagegrid/nodes`
8. Validieren von StorageGRID -Knotenkonfigurationsdateien
9. Starten des StorageGRID Hostdienstes

Beispiel für eine Ansible-Rolle und ein Playbook

Beispielhafte Ansible-Rolle und Playbook werden mit dem Installationsarchiv im `/extras` Ordner. Das Ansible Playbook zeigt, wie die `storagegrid` Die Rolle bereitet die Hosts vor und installiert StorageGRID auf den Zielservern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.

Automatisieren Sie die Konfiguration von StorageGRID

Nach der Bereitstellung der Grid-Knoten können Sie die Konfiguration des StorageGRID Systems automatisieren.

Bevor Sie beginnen

- Den Speicherort der folgenden Dateien kennen Sie aus dem Installationsarchiv.

Dateiname	Beschreibung
configure-storagegrid.py	Python-Skript zur Automatisierung der Konfiguration
configure-storagegrid.sample.json	Beispielkonfigurationsdatei zur Verwendung mit dem Skript
configure-storagegrid.blank.json	Leere Konfigurationsdatei zur Verwendung mit dem Skript

- Sie haben eine `configure-storagegrid.json` Konfigurationsdatei. Um diese Datei zu erstellen, können Sie die Beispielkonfigurationsdatei ändern(`configure-storagegrid.sample.json`) oder die leere Konfigurationsdatei(`configure-storagegrid.blank.json`).

Informationen zu diesem Vorgang

Sie können die `configure-storagegrid.py` Python-Skript und das `configure-storagegrid.json` Konfigurationsdatei zur Automatisierung der Konfiguration Ihres StorageGRID -Systems.

Sie können das System auch mit dem Grid Manager oder der Installations-API konfigurieren.

Schritte

1. Melden Sie sich bei dem Linux-Computer an, den Sie zum Ausführen des Python-Skripts verwenden.
2. Wechseln Sie in das Verzeichnis, in das Sie das Installationsarchiv extrahiert haben.

   Beispiel:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   Wo `platform` Ist `debs` , `rpms` , oder `vsphere` .

3. Führen Sie das Python-Skript aus und verwenden Sie die von Ihnen erstellte Konfigurationsdatei.

   Beispiel:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Ergebnis

Ein Wiederherstellungspaket `.zip` Die Datei wird während des Konfigurationsprozesses generiert und in das Verzeichnis heruntergeladen, in dem Sie den Installations- und Konfigurationsprozess ausführen. Sie müssen die Wiederherstellungspaketdatei sichern, damit Sie das StorageGRID -System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Kopieren Sie es beispielsweise an einen sicheren, gesicherten Netzwerkspeicherort und an einen sicheren Cloud-Speicherort.

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

Wenn Sie angegeben haben, dass zufällige Passwörter generiert werden sollen, öffnen Sie das `Passwords.txt` und suchen Sie nach den Passwörtern, die für den Zugriff auf Ihr StorageGRID -System erforderlich sind.

```
######################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Ihr StorageGRID -System ist installiert und konfiguriert, wenn eine Bestätigungsmeldung angezeigt wird.

```
StorageGRID has been configured and installed.
```

Ähnliche Informationen

"Installation der REST-API"

Bereitstellen virtueller Grid-Knoten (Ubuntu oder Debian)

Erstellen Sie Knotenkonfigurationsdateien für Ubuntu- oder Debian-Bereitstellungen

Knotenkonfigurationsdateien sind kleine Textdateien, die die Informationen bereitstellen, die der StorageGRID Hostdienst benötigt, um einen Knoten zu starten und ihn mit den entsprechenden Netzwerk- und Blockspeicherressourcen zu verbinden. Knotenkonfigurationsdateien werden für virtuelle Knoten verwendet und nicht für Appliance-Knoten.

Speicherort für Knotenkonfigurationsdateien

Platzieren Sie die Konfigurationsdatei für jeden StorageGRID -Knoten im `/etc/storagegrid/nodes` Verzeichnis auf dem Host, auf dem der Knoten ausgeführt wird. Wenn Sie beispielsweise planen, einen Admin-

Knoten, einen Gateway-Knoten und einen Storage-Knoten auf HostA auszuführen, müssen Sie drei Knotenkonfigurationsdateien in `/etc/storagegrid/nodes` auf HostA.

Sie können die Konfigurationsdateien mit einem Texteditor wie vim oder nano direkt auf jedem Host erstellen oder sie an einem anderen Ort erstellen und auf jeden Host verschieben.

Benennung von Knotenkonfigurationsdateien

Die Namen der Konfigurationsdateien sind aussagekräftig. Das Format ist `node-name.conf` , Wo `node-name` ist ein Name, den Sie dem Knoten zuweisen. Dieser Name wird im StorageGRID Installationsprogramm angezeigt und für Knotenwartungsvorgänge wie die Knotenmigration verwendet.

Knotennamen müssen diesen Regeln entsprechen:

- Muss eindeutig sein
- Muss mit einem Buchstaben beginnen
- Kann die Zeichen A bis Z und a bis z enthalten
- Kann die Zahlen 0 bis 9 enthalten
- Kann einen oder mehrere Bindestriche (-) enthalten
- Darf nicht mehr als 32 Zeichen umfassen, ohne die `.conf` Verlängerung

Alle Dateien in `/etc/storagegrid/nodes` die diesen Namenskonventionen nicht folgen, werden vom Hostdienst nicht analysiert.

Wenn Sie für Ihr Grid eine Multi-Site-Topologie planen, könnte ein typisches Knotenbenennungsschema wie folgt aussehen:

```
site-nodetype-nodenumber.conf
```

Sie könnten beispielsweise verwenden `dc1-adm1.conf` für den ersten Admin-Knoten im Rechenzentrum 1 und `dc2-sn3.conf` für den dritten Speicherknoten im Rechenzentrum 2. Sie können jedoch jedes beliebige Schema verwenden, solange alle Knotennamen den Namensregeln entsprechen.

Inhalt einer Knotenkonfigurationsdatei

Eine Konfigurationsdatei enthält Schlüssel-/Wertpaare mit einem Schlüssel und einem Wert pro Zeile. Befolgen Sie für jedes Schlüssel-/Wertpaar die folgenden Regeln:

- Der Schlüssel und der Wert müssen durch ein Gleichheitszeichen getrennt sein(=) und optionalem Leerzeichen.
- Die Schlüssel dürfen keine Leerzeichen enthalten.
- Die Werte können eingebettete Leerzeichen enthalten.
- Vorangehende oder nachfolgende Leerzeichen werden ignoriert.

Die folgende Tabelle definiert die Werte für alle unterstützten Schlüssel. Jeder Schlüssel hat eine der folgenden Bezeichnungen:

- **Erforderlich**: Erforderlich für jeden Knoten oder für die angegebenen Knotentypen
- **Best Practice**: Optional, aber empfohlen
- **Optional**: Optional für alle Knoten

Admin-Netzwerkschlüssel

ADMIN_IP

Wert	Bezeichnung
Grid-Netzwerk-IPv4-Adresse des primären Admin-Knotens für das Grid, zu dem dieser Knoten gehört. Verwenden Sie denselben Wert, den Sie für GRID_NETWORK_IP für den Grid-Knoten mit NODE_TYPE = VM_Admin_Node und ADMIN_ROLE = Primary angegeben haben. Wenn Sie diesen Parameter weglassen, versucht der Knoten, mithilfe von mDNS einen primären Admin-Knoten zu ermitteln. "So erkennen Grid-Knoten den primären Admin-Knoten" **Hinweis**: Dieser Wert wird auf dem primären Admin-Knoten ignoriert und ist möglicherweise verboten.	Bewährte Methode

ADMIN_NETWORK_CONFIG

Wert	Bezeichnung
DHCP, STATISCH oder DEAKTIVIERT	Optional

ADMIN_NETWORK_ESL

Wert	Bezeichnung
Durch Kommas getrennte Liste von Subnetzen in CIDR-Notation, mit denen dieser Knoten über das Admin-Netzwerk-Gateway kommunizieren soll. Beispiel: `172.16.0.0/21,172.17.0.0/21`	Optional

ADMIN_NETWORK_GATEWAY

Wert	Bezeichnung

IPv4-Adresse des lokalen Admin-Netzwerk-Gateways für diesen Knoten. Muss sich im durch ADMIN_NETWORK_IP und ADMIN_NETWORK_MASK definierten Subnetz befinden. Dieser Wert wird für DHCP-konfigurierte Netzwerke ignoriert.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn `ADMIN_NETWORK_ESL` angegeben ist. Andernfalls optional.

ADMIN_NETWORK_IP

Wert	Bezeichnung

IPv4-Adresse dieses Knotens im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC.
	
	Andernfalls optional.

ADMIN_NETWORK_MAC

Wert	Bezeichnung
Die MAC-Adresse für die Admin-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn es weggelassen wird, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Paaren hexadezimaler Ziffern bestehen, die durch Doppelpunkte getrennt sind. Beispiel: `b2:9c:02:c2:27:10`	Optional

ADMIN_NETWORK_MASK

Wert	Bezeichnung

IPv4-Netzmaske für diesen Knoten im Admin-Netzwerk. Geben Sie diesen Schlüssel an, wenn ADMIN_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Erforderlich, wenn ADMIN_NETWORK_IP angegeben ist und ADMIN_NETWORK_CONFIG = STATIC.
	
	Andernfalls optional.

ADMIN_NETWORK_MTU

Wert	Bezeichnung

Die maximale Übertragungseinheit (MTU) für diesen Knoten im Admin-Netzwerk. Nicht angeben, wenn ADMIN_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1500 verwendet.
 	
Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei.
 	
WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Knoten verbunden ist. Andernfalls kann es zu Problemen mit der Netzwerkleistung oder zu Paketverlusten kommen.
 	
Beispiele:
 	
`1500`
 	
`8192`
	Optional

ADMIN_NETWORK_TARGET

Wert	Bezeichnung

Name des Hostgeräts, das Sie für den Admin-Netzwerkzugriff durch den StorageGRID -Knoten verwenden. Es werden nur Netzwerkschnittstellennamen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den, der für GRID_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegeben wurde.
 	
Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) über dem Bond-Gerät oder verwenden Sie ein Bridge- und Virtual-Ethernet-Paar (veth).
 	
Best Practice: Geben Sie einen Wert an, auch wenn dieser Knoten zunächst keine Admin-Netzwerk-IP-Adresse hat. Dann können Sie später eine Admin-Netzwerk-IP-Adresse hinzufügen, ohne den Knoten auf dem Host neu konfigurieren zu müssen.
 	
Beispiele:
 	
`bond0.1002`
 	
`ens256`
	Bewährte Methode

ADMIN_NETWORK_TARGET_TYPE

Wert	Bezeichnung
Schnittstelle (Dies ist der einzige unterstützte Wert.)	Optional

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Wert	Bezeichnung
Wahr oder Falsch Setzen Sie den Schlüssel auf „true“, damit der StorageGRID -Container die MAC-Adresse der Host-Zielschnittstelle im Admin-Netzwerk verwendet. **Best Practice:** Verwenden Sie in Netzwerken, in denen der Promiscuous-Modus erforderlich wäre, stattdessen den Schlüssel ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Weitere Einzelheiten zum MAC-Klonen: • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red Hat Enterprise Linux)" • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"	Bewährte Methode

ADMIN_ROLE

Wert	Bezeichnung
Primär oder nicht primär Dieser Schlüssel ist nur erforderlich, wenn NODE_TYPE = VM_Admin_Node; geben Sie ihn nicht für andere Knotentypen an.	Erforderlich, wenn NODE_TYPE = VM_Admin_Node Andernfalls optional.

Geräteschlüssel sperren

BLOCK_DEVICE_AUDIT_LOGS

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten zur dauerhaften Speicherung von Prüfprotokollen verwendet.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Erforderlich für Knoten mit NODE_TYPE = VM_Admin_Node. Geben Sie es nicht für andere Knotentypen an.

BLOCK_DEVICE_RANGEDB_nnn

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten für die dauerhafte Objektspeicherung verwendet. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Storage_Node erforderlich. Geben Sie ihn nicht für andere Knotentypen an.
 	
Nur BLOCK_DEVICE_RANGEDB_000 ist erforderlich, der Rest ist optional. Das für BLOCK_DEVICE_RANGEDB_000 angegebene Blockgerät muss mindestens 4 TB groß sein, die anderen können kleiner sein.
 	
Lassen Sie keine Lücken. Wenn Sie BLOCK_DEVICE_RANGEDB_005 angeben, müssen Sie auch BLOCK_DEVICE_RANGEDB_004 angeben.
 	
Hinweis: Aus Kompatibilitätsgründen mit vorhandenen Bereitstellungen werden für aktualisierte Knoten zweistellige Schlüssel unterstützt.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Erforderlich:
	
	BLOCK_DEVICE_RANGEDB_000
	
	Optional:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

BLOCK_DEVICE_TABLES

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten zur dauerhaften Speicherung von Datenbanktabellen verwendet. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Admin_Node erforderlich. Geben Sie ihn nicht für andere Knotentypen an.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Erforderlich

BLOCK_DEVICE_VAR_LOCAL

Wert	Bezeichnung

Pfad und Name der speziellen Blockgerätedatei, die dieser Knoten für seine `/var/local` dauerhafter Speicher.
 	
Beispiele:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Erforderlich

Client-Netzwerkschlüssel

CLIENT_NETWORK_CONFIG

Wert	Bezeichnung
DHCP, STATISCH oder DEAKTIVIERT	Optional

CLIENT_NETWORK_GATEWAY

Wert	Bezeichnung

IPv4-Adresse des lokalen Client-Netzwerk-Gateways für diesen Knoten, das sich im durch CLIENT_NETWORK_IP und CLIENT_NETWORK_MASK definierten Subnetz befinden muss. Dieser Wert wird für DHCP-konfigurierte Netzwerke ignoriert.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Optional

CLIENT_NETWORK_IP

Wert	Bezeichnung

IPv4-Adresse dieses Knotens im Client-Netzwerk.
 	
Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC
	
	Andernfalls optional.

CLIENT_NETWORK_MAC

Wert	Bezeichnung
Die MAC-Adresse für die Client-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn es weggelassen wird, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Paaren hexadezimaler Ziffern bestehen, die durch Doppelpunkte getrennt sind. Beispiel: `b2:9c:02:c2:27:20`	Optional

CLIENT_NETWORK_MASK

Wert	Bezeichnung

IPv4-Netzmaske für diesen Knoten im Client-Netzwerk.
 	
Geben Sie diesen Schlüssel an, wenn CLIENT_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Erforderlich, wenn CLIENT_NETWORK_IP angegeben ist und CLIENT_NETWORK_CONFIG = STATIC
	
	Andernfalls optional.

CLIENT_NETWORK_MTU

Wert	Bezeichnung

Die maximale Übertragungseinheit (MTU) für diesen Knoten im Client-Netzwerk. Nicht angeben, wenn CLIENT_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1500 verwendet.
 	
Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei.
 	
WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Knoten verbunden ist. Andernfalls kann es zu Problemen mit der Netzwerkleistung oder zu Paketverlusten kommen.
 	
Beispiele:
 	
`1500`
 	
`8192`
	Optional

CLIENT_NETWORK_TARGET

Wert	Bezeichnung

Name des Hostgeräts, das Sie für den Client-Netzwerkzugriff durch den StorageGRID -Knoten verwenden. Es werden nur Netzwerkschnittstellennamen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den, der für GRID_NETWORK_TARGET oder ADMIN_NETWORK_TARGET angegeben wurde.
 	
Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) über dem Bond-Gerät oder verwenden Sie ein Bridge- und Virtual-Ethernet-Paar (veth).
 	
Best Practice: Geben Sie einen Wert an, auch wenn dieser Knoten zunächst keine Client-Netzwerk-IP-Adresse hat. Dann können Sie später eine Client-Netzwerk-IP-Adresse hinzufügen, ohne den Knoten auf dem Host neu konfigurieren zu müssen.
 	
Beispiele:
 	
`bond0.1003`
 	
`ens423`
	Bewährte Methode

CLIENT_NETWORK_TARGET_TYPE

Wert	Bezeichnung
Schnittstelle (Dies ist der einzige unterstützte Wert.)	Optional

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Wert	Bezeichnung
Wahr oder Falsch Setzen Sie den Schlüssel auf „true“, damit der StorageGRID Container die MAC-Adresse der Host-Zielschnittstelle im Client-Netzwerk verwendet. **Best Practice:** Verwenden Sie in Netzwerken, in denen der Promiscuous-Modus erforderlich wäre, stattdessen den Schlüssel CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Weitere Einzelheiten zum MAC-Klonen: • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red Hat Enterprise Linux)" • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"	Bewährte Methode

Grid-Netzwerkschlüssel

GRID_NETWORK_CONFIG

Wert	Bezeichnung
STATISCH oder DHCP Der Standardwert ist STATIC, wenn nicht anders angegeben.	Bewährte Methode

GRID_NETWORK_GATEWAY

Wert	Bezeichnung
IPv4-Adresse des lokalen Grid-Netzwerk-Gateways für diesen Knoten, das sich im durch GRID_NETWORK_IP und GRID_NETWORK_MASK definierten Subnetz befinden muss. Dieser Wert wird für DHCP-konfigurierte Netzwerke ignoriert. Wenn das Grid-Netzwerk ein einzelnes Subnetz ohne Gateway ist, verwenden Sie entweder die Standard-Gateway-Adresse für das Subnetz (XYZ1) oder den GRID_NETWORK_IP-Wert dieses Knotens. Beide Werte vereinfachen mögliche zukünftige Erweiterungen des Grid-Netzwerks.	Erforderlich

GRID_NETWORK_IP

Wert	Bezeichnung

IPv4-Adresse dieses Knotens im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Erforderlich, wenn GRID_NETWORK_CONFIG = STATIC
	
	Andernfalls optional.

GRID_NETWORK_MAC

Wert	Bezeichnung
Die MAC-Adresse für die Grid-Netzwerkschnittstelle im Container. Muss aus 6 Paaren hexadezimaler Ziffern bestehen, die durch Doppelpunkte getrennt sind. Beispiel: `b2:9c:02:c2:27:30`	Optional Wenn es weggelassen wird, wird automatisch eine MAC-Adresse generiert.

GRID_NETWORK_MASK

Wert	Bezeichnung

IPv4-Netzmaske für diesen Knoten im Grid-Netzwerk. Geben Sie diesen Schlüssel an, wenn GRID_NETWORK_CONFIG = STATIC ist. Geben Sie ihn nicht für andere Werte an.
 	
Beispiele:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Erforderlich, wenn GRID_NETWORK_IP angegeben ist und GRID_NETWORK_CONFIG = STATIC.
	
	Andernfalls optional.

GRID_NETWORK_MTU

Wert	Bezeichnung

Die maximale Übertragungseinheit (MTU) für diesen Knoten im Grid-Netzwerk. Nicht angeben, wenn GRID_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1500 verwendet.
 	
Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei.
 	
WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Knoten verbunden ist. Andernfalls kann es zu Problemen mit der Netzwerkleistung oder zu Paketverlusten kommen.
 	
WICHTIG: Für die beste Netzwerkleistung sollten alle Knoten mit ähnlichen MTU-Werten auf ihren Grid-Netzwerkschnittstellen konfiguriert werden. Die Warnung **MTU-Fehlanpassung des Grid-Netzwerks** wird ausgelöst, wenn es bei den MTU-Einstellungen für das Grid-Netzwerk auf einzelnen Knoten einen signifikanten Unterschied gibt. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.
 	
Beispiele:
 	
`1500`
 	
`8192`
	Optional

GRID_NETWORK_TARGET

Wert	Bezeichnung

Name des Hostgeräts, das Sie für den Grid-Netzwerkzugriff durch den StorageGRID -Knoten verwenden. Es werden nur Netzwerkschnittstellennamen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den, der für ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegeben wurde.
 	
Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) über dem Bond-Gerät oder verwenden Sie ein Bridge- und Virtual-Ethernet-Paar (veth).
 	
Beispiele:
 	
`bond0.1001`
 	
`ens192`
	Erforderlich

GRID_NETWORK_TARGET_TYPE

Wert	Bezeichnung
Schnittstelle (Dies ist der einzige unterstützte Wert.)	Optional

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Wert	Bezeichnung
Wahr oder Falsch Setzen Sie den Wert des Schlüssels auf „true“, damit der StorageGRID Container die MAC-Adresse der Host-Zielschnittstelle im Grid-Netzwerk verwendet. **Best Practice:** Verwenden Sie in Netzwerken, in denen der Promiscuous-Modus erforderlich wäre, stattdessen den Schlüssel GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Weitere Einzelheiten zum MAC-Klonen: • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red Hat Enterprise Linux)" • "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"	Bewährte Methode

Installationskennwortschlüssel (temporär)

BENUTZERDEFINIERTER_TEMPORÄRER_PASSWORT_HASH

Wert	Bezeichnung
Legen Sie für den primären Admin-Knoten während der Installation ein temporäres Standardkennwort für die StorageGRID -Installations-API fest. **Hinweis**: Legen Sie nur auf dem primären Admin-Knoten ein Installationskennwort fest. Wenn Sie versuchen, ein Kennwort für einen anderen Knotentyp festzulegen, schlägt die Validierung der Knotenkonfigurationsdatei fehl. Das Festlegen dieses Werts hat nach Abschluss der Installation keine Auswirkungen mehr. Wenn dieser Schlüssel weggelassen wird, wird standardmäßig kein temporäres Passwort festgelegt. Alternativ können Sie mithilfe der StorageGRID Installations-API ein temporäres Passwort festlegen. Muss ein `crypt()` SHA-512-Passwort-Hash mit Format `$6$<salt>$<password hash>` für ein Passwort mit mindestens 8 und höchstens 32 Zeichen. Dieser Hash kann mit CLI-Tools generiert werden, wie zum Beispiel dem `openssl passwd` Befehl im SHA-512-Modus.	Bewährte Methode

Schnittstellenschlüssel

SCHNITTSTELLENZIEL_nnnn

Wert	Bezeichnung
Name und optionale Beschreibung für eine zusätzliche Schnittstelle, die Sie diesem Knoten hinzufügen möchten. Sie können jedem Knoten mehrere zusätzliche Schnittstellen hinzufügen. Geben Sie für *nnnn* eine eindeutige Nummer für jeden INTERFACE_TARGET-Eintrag an, den Sie hinzufügen. Geben Sie als Wert den Namen der physischen Schnittstelle auf dem Bare-Metal-Host an. Fügen Sie dann optional ein Komma hinzu und geben Sie eine Beschreibung der Schnittstelle ein, die auf der Seite „VLAN-Schnittstellen“ und der Seite „HA-Gruppen“ angezeigt wird. Beispiel: `INTERFACE_TARGET_0001=ens256, Trunk` Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt zu einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.	Optional

Maximaler RAM-Schlüssel

MAXIMALER RAM

Wert	Bezeichnung

Die maximale RAM-Menge, die dieser Knoten verbrauchen darf. Wenn dieser Schlüssel weggelassen wird, unterliegt der Knoten keinen Speicherbeschränkungen. Wenn Sie dieses Feld für einen Knoten auf Produktionsebene festlegen, geben Sie einen Wert an, der mindestens 24 GB und 16 bis 32 GB weniger als der gesamte System-RAM beträgt.
 	
Hinweis: Der RAM-Wert wirkt sich auf den tatsächlich für Metadaten reservierten Speicherplatz eines Knotens aus. Siehe die"Beschreibung, was Metadata Reserved Space ist" .
 	
Das Format für dieses Feld ist *`numberunit`* , Wo *`unit`* kann sein `b` , `k` , `m` , oder `g` .
 	
Beispiele:
 	
`24g`
 	
`38654705664b`
 	
Hinweis: Wenn Sie diese Option verwenden möchten, müssen Sie die Kernel-Unterstützung für Speicher-Cgroups aktivieren.
	Optional

Knotentypschlüssel

KNOTENTYP

Wert	Bezeichnung
Knotentyp: • VM_Admin_Node • VM_Speicherknoten • VM_Archive_Node • VM_API_Gateway	Erforderlich

SPEICHERTYP

Wert	Bezeichnung
Definiert den Objekttyp, den ein Speicherknoten enthält. Weitere Informationen finden Sie unter "Arten von Speicherknoten" . Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Storage_Node erforderlich. Geben Sie ihn nicht für andere Knotentypen an. Speichertypen: • kombiniert • Daten • Metadaten **Hinweis**: Wenn STORAGE_TYPE nicht angegeben ist, wird der Speicherknotentyp standardmäßig auf „Kombiniert (Daten und Metadaten)“ eingestellt.	Optional

Port-Neuzuordnungsschlüssel

PORT_REMAP

Wert	Bezeichnung
Ordnet jeden Port neu zu, der von einem Knoten für die interne oder externe Grid-Knotenkommunikation verwendet wird. Eine Neuzuordnung der Ports ist erforderlich, wenn die Netzwerkrichtlinien des Unternehmens einen oder mehrere von StorageGRID verwendete Ports einschränken, wie in beschrieben."Interne Grid-Knoten-Kommunikation" oder"Externe Kommunikation" . **WICHTIG**: Ordnen Sie die Ports, die Sie zum Konfigurieren der Endpunkte des Lastenausgleichs verwenden möchten, nicht neu zu. **Hinweis**: Wenn nur PORT_REMAP festgelegt ist, wird die von Ihnen angegebene Zuordnung sowohl für eingehende als auch für ausgehende Kommunikation verwendet. Wenn auch PORT_REMAP_INBOUND angegeben ist, gilt PORT_REMAP nur für ausgehende Kommunikation. Das verwendete Format ist: *`network type/protocol/default port used by grid node/new port`* , Wo *`network type`* ist Grid, Admin oder Client und *`protocol`* ist TCP oder UDP. Beispiel: `PORT_REMAP = client/tcp/18082/443` Sie können auch mehrere Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen. Beispiel: `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	Optional

PORT_REMAP_INBOUND

Wert	Bezeichnung
Ordnet eingehende Kommunikation dem angegebenen Port neu zu. Wenn Sie PORT_REMAP_INBOUND angeben, aber keinen Wert für PORT_REMAP angeben, bleibt die ausgehende Kommunikation für den Port unverändert. **WICHTIG**: Ordnen Sie die Ports, die Sie zum Konfigurieren der Endpunkte des Lastenausgleichs verwenden möchten, nicht neu zu. Das verwendete Format ist: *`network type/protocol/remapped port/default port used by grid node`* , Wo *`network type`* ist Grid, Admin oder Client und *`protocol`* ist TCP oder UDP. Beispiel: `PORT_REMAP_INBOUND = grid/tcp/3022/22` Sie können auch mehrere eingehende Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen. Beispiel: `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	Optional

So erkennen Grid-Knoten den primären Admin-Knoten

Grid-Knoten kommunizieren zur Konfiguration und Verwaltung mit dem primären Admin-Knoten. Jeder Grid-Knoten muss die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk kennen.

Um sicherzustellen, dass ein Grid-Knoten auf den primären Admin-Knoten zugreifen kann, können Sie beim Bereitstellen des Knotens einen der folgenden Schritte ausführen:

- Sie können den Parameter ADMIN_IP verwenden, um die IP-Adresse des primären Admin-Knotens manuell einzugeben.
- Sie können den Parameter ADMIN_IP weglassen, damit der Grid-Knoten den Wert automatisch erkennt. Die automatische Erkennung ist besonders nützlich, wenn das Grid-Netzwerk DHCP verwendet, um dem primären Admin-Knoten die IP-Adresse zuzuweisen.

Die automatische Erkennung des primären Admin-Knotens erfolgt mithilfe eines Multicast-Domain-Name-Systems (mDNS). Wenn der primäre Admin-Knoten zum ersten Mal gestartet wird, veröffentlicht er seine IP-Adresse mithilfe von mDNS. Andere Knoten im selben Subnetz können dann die IP-Adresse abfragen und automatisch abrufen. Da Multicast-IP-Verkehr jedoch normalerweise nicht über Subnetze hinweg geroutet werden kann, können Knoten in anderen Subnetzen die IP-Adresse des primären Admin-Knotens nicht direkt abrufen.

Wenn Sie die automatische Erkennung verwenden:

- Sie müssen die ADMIN_IP-Einstellung für mindestens einen Grid-Knoten in allen Subnetzen einschließen, an die der primäre Admin-Knoten nicht direkt angeschlossen ist. Dieser Grid-Knoten veröffentlicht dann die IP-Adresse des primären Admin-Knotens, damit andere Knoten im Subnetz sie mit mDNS erkennen können.
- Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur die Weiterleitung von Multicast-IP-Verkehr innerhalb eines Subnetzes unterstützt.

Beispiele für Knotenkonfigurationsdateien

Sie können die Beispielknotenkonfigurationsdateien verwenden, um die Knotenkonfigurationsdateien für Ihr StorageGRID -System einzurichten. Die Beispiele zeigen Knotenkonfigurationsdateien für alle Arten von Grid-Knoten.

Für die meisten Knoten können Sie Administrator- und Client-Netzwerkadressinformationen (IP, Maske, Gateway usw.) hinzufügen, wenn Sie das Grid mit dem Grid Manager oder der Installations-API konfigurieren. Die Ausnahme ist der primäre Admin-Knoten. Wenn Sie zur Admin-Netzwerk-IP des primären Admin-Knotens navigieren möchten, um die Grid-Konfiguration abzuschließen (weil das Grid-Netzwerk beispielsweise nicht geroutet wird), müssen Sie die Admin-Netzwerkverbindung für den primären Admin-Knoten in seiner Knotenkonfigurationsdatei konfigurieren. Dies wird im Beispiel gezeigt.

In den Beispielen wurde das Client-Netzwerkziel als Best Practice konfiguriert, obwohl das Client-Netzwerk standardmäßig deaktiviert ist.

Beispiel für primären Admin-Knoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-adm1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Beispiel für Speicherknoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-sn1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Beispiel für Gateway-Knoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-gw1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Beispiel für einen nicht primären Admin-Knoten

Beispieldateiname: `/etc/storagegrid/nodes/dc1-adm2.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validieren der StorageGRID -Konfiguration

Nach dem Erstellen von Konfigurationsdateien in `/etc/storagegrid/nodes` Für jeden Ihrer StorageGRID Knoten müssen Sie den Inhalt dieser Dateien validieren.

Um den Inhalt der Konfigurationsdateien zu validieren, führen Sie auf jedem Host den folgenden Befehl aus:

```
sudo storagegrid node validate all
```

Wenn die Dateien korrekt sind, zeigt die Ausgabe für jede Konfigurationsdatei **PASSED** an, wie im Beispiel gezeigt.

Wenn Sie auf Nur-Metadaten-Knoten nur eine LUN verwenden, erhalten Sie möglicherweise eine Warnmeldung, die ignoriert werden kann.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Bei einer automatisierten Installation können Sie diese Ausgabe unterdrücken, indem Sie den `-q` oder `--quiet` Optionen in der `storagegrid` Befehl (zum Beispiel `storagegrid --quiet…`). Wenn Sie die Ausgabe unterdrücken, hat der Befehl einen Exit-Wert ungleich Null, wenn Konfigurationswarnungen oder -fehler erkannt wurden.

Wenn die Konfigurationsdateien fehlerhaft sind, werden die Probleme wie im Beispiel gezeigt als **WARNUNG** und **FEHLER** angezeigt. Wenn Konfigurationsfehler gefunden werden, müssen Sie diese beheben, bevor Sie mit der Installation fortfahren.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Starten Sie den StorageGRID -Hostdienst

Um Ihre StorageGRID -Knoten zu starten und sicherzustellen, dass sie nach einem Host-Neustart neu gestartet werden, müssen Sie den StorageGRID Hostdienst aktivieren und starten.

Schritte

1. Führen Sie auf jedem Host die folgenden Befehle aus:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Bereitstellung fortgesetzt wird:

```
sudo storagegrid node status node-name
```

3. Wenn ein Knoten den Status „Nicht ausgeführt“ oder „Gestoppt“ zurückgibt, führen Sie den folgenden Befehl aus:

```
sudo storagegrid node start node-name
```

4. Wenn Sie den StorageGRID Hostdienst zuvor aktiviert und gestartet haben (oder wenn Sie nicht sicher sind, ob der Dienst aktiviert und gestartet wurde), führen Sie außerdem den folgenden Befehl aus:

```
sudo systemctl reload-or-restart storagegrid
```

Grid konfigurieren und Installation abschließen (Ubuntu oder Debian)

Navigieren Sie zum Grid Manager

Mit dem Grid Manager definieren Sie alle erforderlichen Informationen zur Konfiguration Ihres StorageGRID Systems.

Bevor Sie beginnen

Der primäre Admin-Knoten muss bereitgestellt sein und die anfängliche Startsequenz abgeschlossen haben.

Schritte

1. Öffnen Sie Ihren Webbrowser und navigieren Sie zu:

   `https://primary_admin_node_ip`

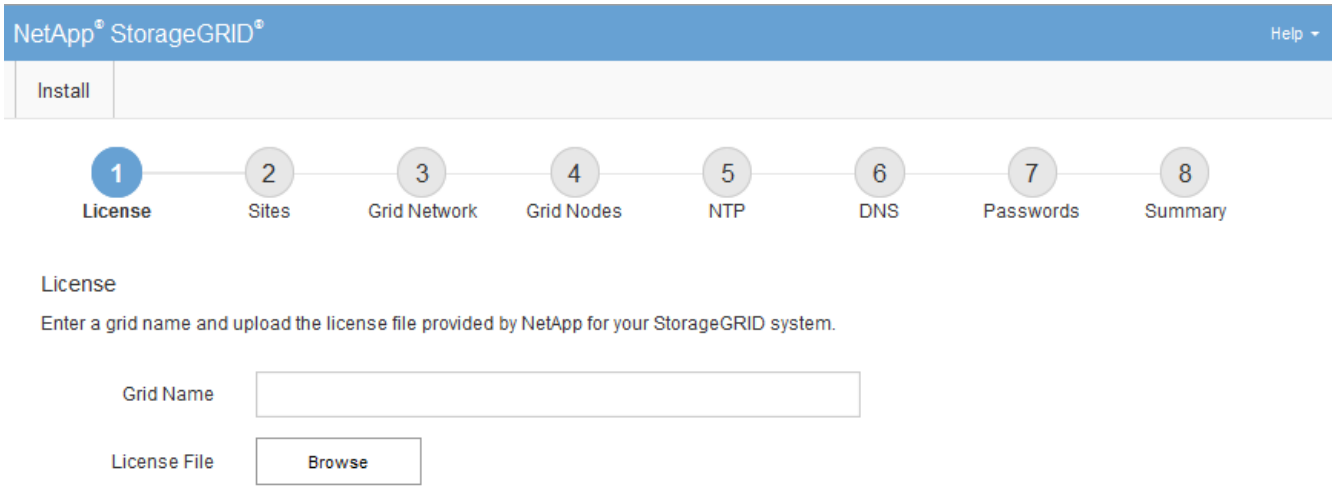
   Alternativ können Sie über Port 8443 auf den Grid Manager zugreifen:

   `https://primary_admin_node_ip:8443`

   Sie können die IP-Adresse für die primäre Admin-Knoten-IP im Grid-Netzwerk oder im Admin-Netzwerk verwenden, je nachdem, was für Ihre Netzwerkkonfiguration angemessen ist.

2. Verwalten Sie bei Bedarf ein temporäres Installateurkennwort:
   - Wenn mit einer dieser Methoden bereits ein Kennwort festgelegt wurde, geben Sie das Kennwort ein, um fortzufahren.
     - Ein Benutzer hat das Kennwort beim Zugriff auf das Installationsprogramm zuvor festgelegt
     - Das Passwort wurde automatisch aus der Knotenkonfigurationsdatei importiert unter `/etc/storagegrid/nodes/<node_name>.conf`
   - Wenn kein Kennwort festgelegt wurde, legen Sie optional ein Kennwort fest, um das StorageGRID Installationsprogramm zu sichern.
3. Wählen Sie **Installieren Sie ein StorageGRID -System**.

Die Seite zum Konfigurieren eines StorageGRID -Systems wird angezeigt.



Geben Sie die StorageGRID -Lizenzinformationen an

Sie müssen den Namen für Ihr StorageGRID -System angeben und die von NetApp bereitgestellte Lizenzdatei hochladen.

Schritte

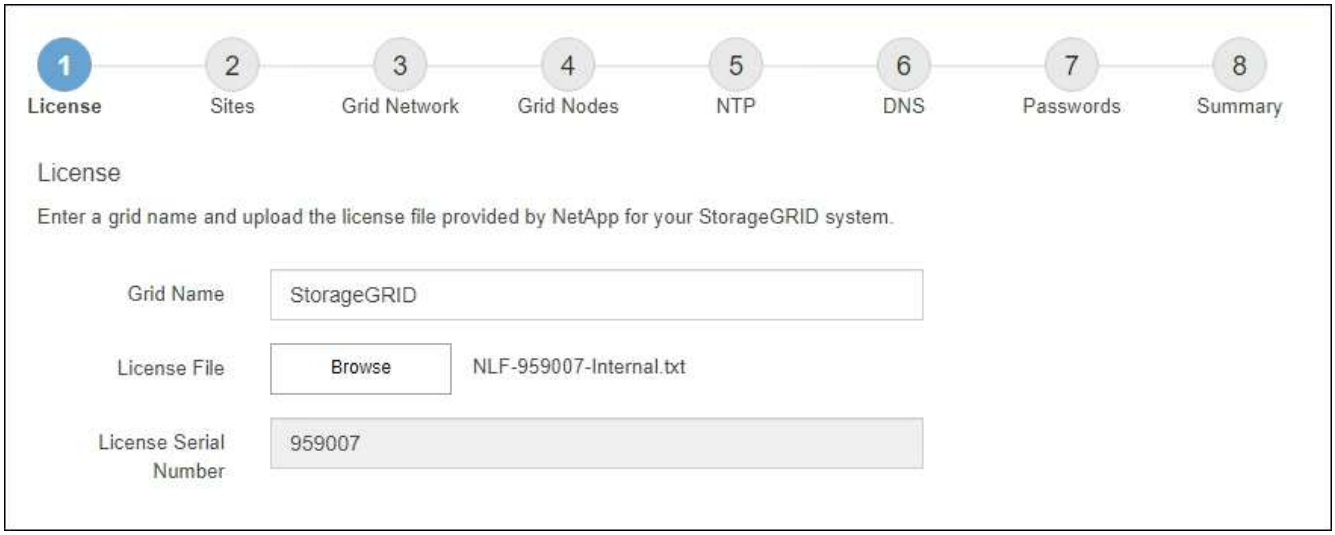
1. Geben Sie auf der Lizenzseite im Feld **Grid-Name** einen aussagekräftigen Namen für Ihr StorageGRID -System ein.

   Nach der Installation wird der Name oben im Knotenmenü angezeigt.

2. Wählen Sie **Durchsuchen**, suchen Sie die NetApp -Lizenzdatei(`NLF-unique-id.txt`) und wählen Sie **Öffnen**.

   Die Lizenzdatei wird validiert und die Seriennummer angezeigt.

> Das StorageGRID -Installationsarchiv enthält eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet. Sie können auf eine Lizenz aktualisieren, die nach der Installation Support bietet.



3. Wählen Sie **Weiter**.

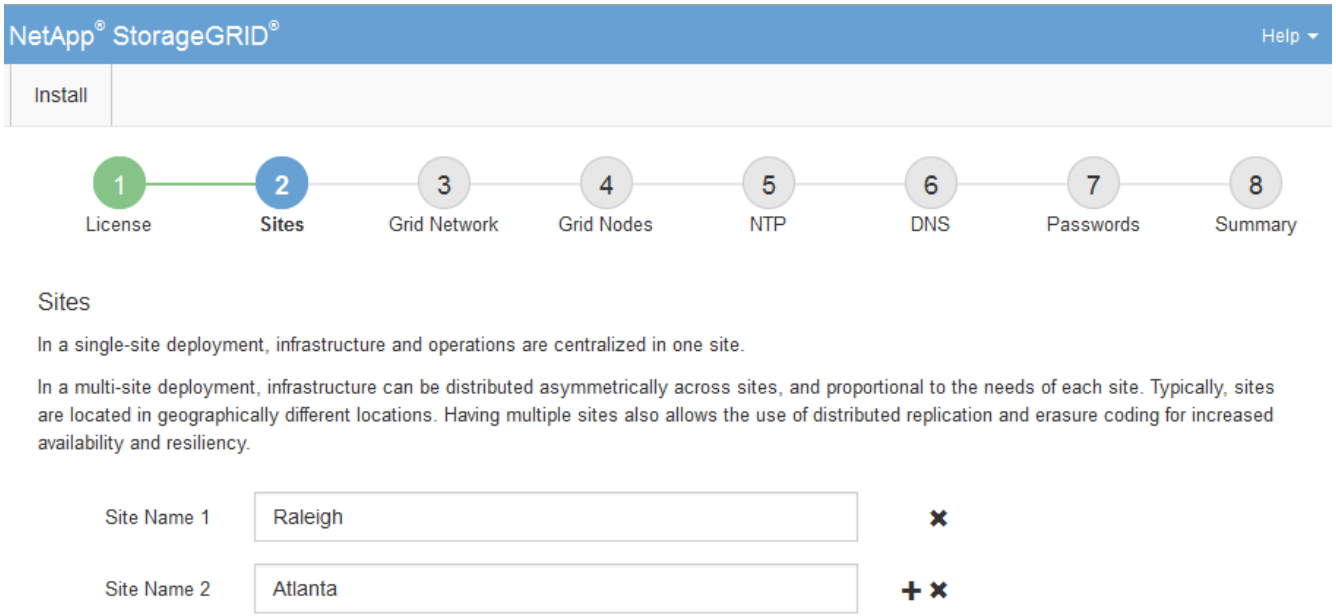
Websites hinzufügen

Sie müssen mindestens eine Site erstellen, wenn Sie StorageGRID installieren. Sie können zusätzliche Sites erstellen, um die Zuverlässigkeit und Speicherkapazität Ihres StorageGRID -Systems zu erhöhen.

Schritte

1. Geben Sie auf der Seite „Sites“ den **Site-Namen** ein.
2. Um weitere Sites hinzuzufügen, klicken Sie auf das Pluszeichen neben dem letzten Site-Eintrag und geben Sie den Namen in das neue Textfeld **Site-Name** ein.

   Fügen Sie so viele zusätzliche Sites hinzu, wie für Ihre Netztopologie erforderlich sind. Sie können bis zu 16 Sites hinzufügen.



3. Klicken Sie auf **Weiter**.

Grid-Netzwerk-Subnetze angeben

Sie müssen die Subnetze angeben, die im Grid-Netzwerk verwendet werden.

Informationen zu diesem Vorgang

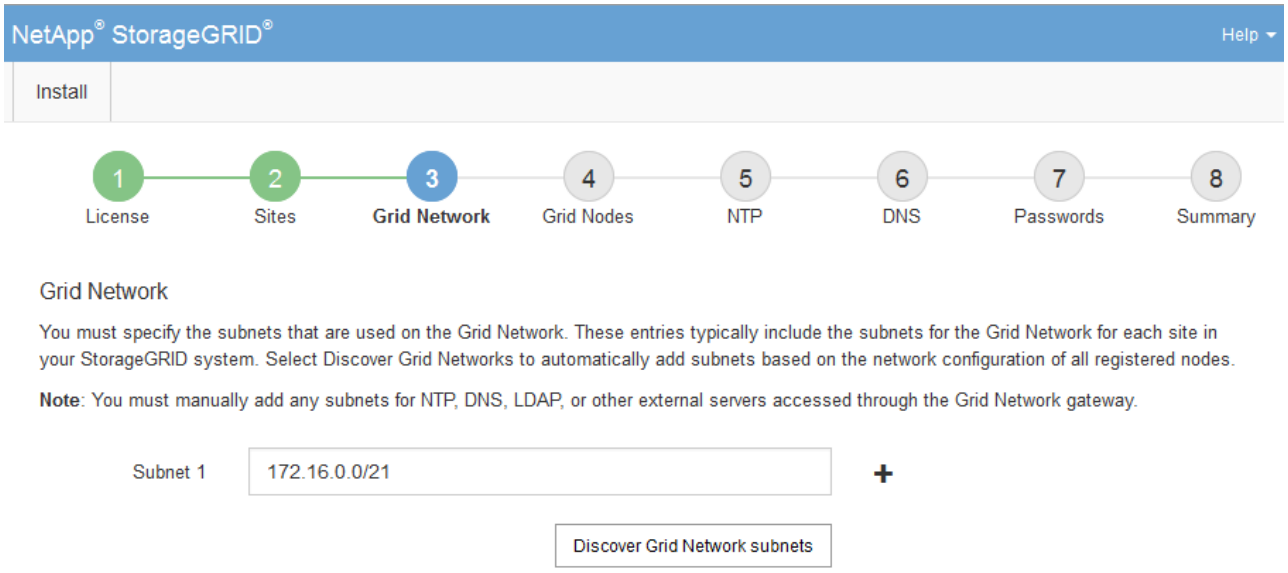
Die Subnetzeinträge umfassen die Subnetze für das Grid-Netzwerk für jeden Standort in Ihrem StorageGRID -System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen.

Wenn Sie über mehrere Grid-Subnetze verfügen, ist das Grid Network-Gateway erforderlich. Alle angegebenen Grid-Subnetze müssen über dieses Gateway erreichbar sein.

Schritte

1. Geben Sie die CIDR-Netzwerkadresse für mindestens ein Grid-Netzwerk im Textfeld **Subnetz 1** an.
2. Klicken Sie auf das Pluszeichen neben dem letzten Eintrag, um einen weiteren Netzwerkeintrag hinzuzufügen. Sie müssen alle Subnetze für alle Sites im Grid-Netzwerk angeben.

- Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf **Grid-Netzwerk-Subnetze ermitteln**, um die Grid-Netzwerk-Subnetzliste automatisch mit den Subnetzen zu füllen, die von Grid-Knoten gemeldet wurden, die beim Grid Manager registriert sind.
- Sie müssen alle Subnetze für NTP, DNS, LDAP oder andere externe Server, auf die über das Grid Network-Gateway zugegriffen wird, manuell hinzufügen.



3. Klicken Sie auf **Weiter**.

Ausstehende Rasterknoten genehmigen

Sie müssen jeden Grid-Knoten genehmigen, bevor er dem StorageGRID -System beitreten kann.

Bevor Sie beginnen

Sie haben alle virtuellen und StorageGRID -Appliance-Grid-Knoten bereitgestellt.

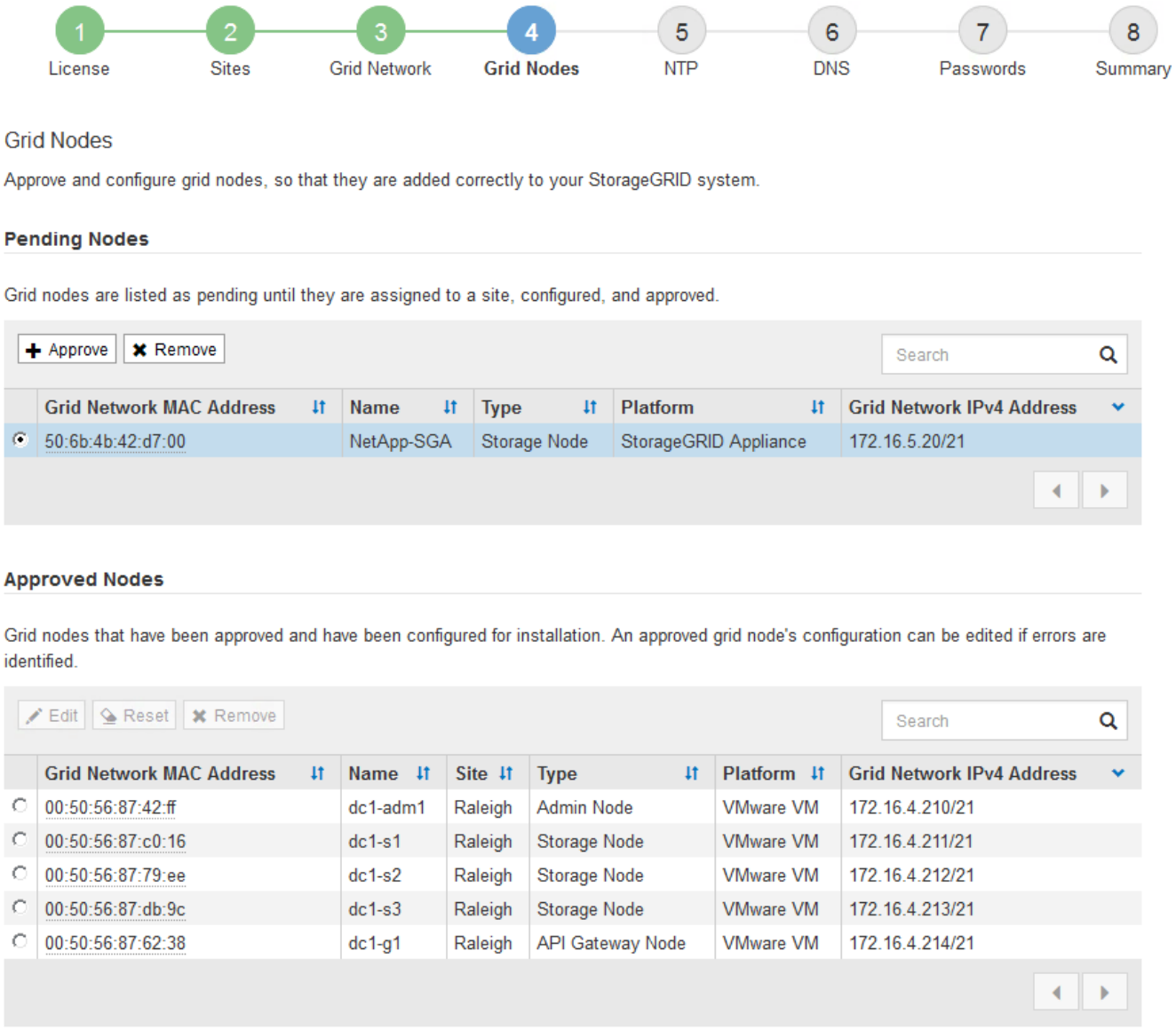
> Es ist effizienter, eine einzige Installation aller Knoten durchzuführen, als einige Knoten jetzt und einige Knoten später zu installieren.

Schritte

1. Überprüfen Sie die Liste der ausstehenden Knoten und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

> Wenn ein Grid-Knoten fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde und die richtige Grid-Netzwerk-IP des primären Admin-Knotens für ADMIN_IP festgelegt ist.

2. Wählen Sie das Optionsfeld neben einem ausstehenden Knoten aus, den Sie genehmigen möchten.



3. Klicken Sie auf **Genehmigen**.
4. Ändern Sie unter „Allgemeine Einstellungen“ nach Bedarf die Einstellungen für die folgenden Eigenschaften:
   - **Site**: Der Systemname der Site für diesen Grid-Knoten.
   - **Name**: Der Systemname für den Knoten. Der Name ist standardmäßig der Name, den Sie bei der Konfiguration des Knotens angegeben haben.

     Systemnamen sind für interne StorageGRID -Vorgänge erforderlich und können nach Abschluss der Installation nicht mehr geändert werden. Während dieses Schritts des Installationsvorgangs können Sie die Systemnamen jedoch nach Bedarf ändern.

   - **NTP-Rolle**: Die Network Time Protocol (NTP)-Rolle des Grid-Knotens. Die Optionen sind **Automatisch**, **Primär** und **Client**. Wenn Sie „**Automatisch**“ auswählen, wird die primäre Rolle den Admin-Knoten, Speicherknoten mit ADC-Diensten, Gateway-Knoten und allen Grid-Knoten mit nicht statischen IP-Adressen zugewiesen. Allen anderen Grid-Knoten wird die Client-Rolle zugewiesen.

Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.

- **Speichertyp** (nur Speicherknoten): Geben Sie an, dass ein neuer Speicherknoten ausschließlich für Daten, nur für Metadaten oder für beides verwendet werden soll. Die Optionen sind **Daten und Metadaten** („kombiniert“), **Nur Daten** und **Nur Metadaten**.

  Sehen"Arten von Speicherknoten" Informationen zu den Anforderungen für diese Knotentypen finden Sie unter.

- **ADC-Dienst** (nur Speicherknoten): Wählen Sie **Automatisch**, damit das System ermittelt, ob der Knoten den Administrative Domain Controller (ADC)-Dienst benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Diensten. Mindestens drei Speicherknoten an jedem Standort müssen den ADC-Dienst enthalten. Sie können den ADC-Dienst nach der Bereitstellung nicht mehr zu einem Knoten hinzufügen.

5. Ändern Sie im Grid-Netzwerk nach Bedarf die Einstellungen für die folgenden Eigenschaften:

   - **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Grid-Netzwerkschnittstelle (eth0 innerhalb des Containers). Beispiel: 192.168.1.234/21
   - **Gateway**: Das Grid-Netzwerk-Gateway. Beispiel: 192.168.0.1

     Das Gateway wird benötigt, wenn mehrere Grid-Subnetze vorhanden sind.

   Wenn Sie DHCP für die Grid-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

6. Wenn Sie das Admin-Netzwerk für den Grid-Knoten konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt „Admin-Netzwerk“ nach Bedarf hinzu oder aktualisieren Sie sie.

   Geben Sie die Zielsubnetze der Routen aus dieser Schnittstelle in das Textfeld **Subnetze (CIDR)** ein. Wenn mehrere Admin-Subnetze vorhanden sind, ist das Admin-Gateway erforderlich.

   Wenn Sie DHCP für die Admin-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

   Geräte: Wenn das Admin-Netzwerk für ein StorageGRID -Gerät während der Erstinstallation mit dem StorageGRID Appliance Installer nicht konfiguriert wurde, kann es in diesem Grid Manager-Dialogfeld nicht konfiguriert werden. Stattdessen müssen Sie die folgenden Schritte ausführen:

   a. Starten Sie das Gerät neu: Wählen Sie im Geräteinstallationsprogramm **Erweitert** > **Neustart**.

      Der Neustart kann mehrere Minuten dauern.

   b. Wählen Sie **Netzwerk konfigurieren** > **Linkkonfiguration** und aktivieren Sie die entsprechenden Netzwerke.

c. Wählen Sie **Netzwerk konfigurieren** > **IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.

d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

e. Im Grid Manager: Wenn der Knoten in der Tabelle „Genehmigte Knoten“ aufgeführt ist, entfernen Sie den Knoten.

f. Entfernen Sie den Knoten aus der Tabelle „Ausstehende Knoten“.

g. Warten Sie, bis der Knoten wieder in der Liste „Ausstehende Knoten“ angezeigt wird.

h. Bestätigen Sie, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt sein, die Sie auf der IP-Konfigurationsseite des Appliance-Installationsprogramms angegeben haben.

   Weitere Informationen finden Sie im "Schnellstart für die Hardwareinstallation" um Anweisungen für Ihr Gerät zu finden.

7. Wenn Sie das Client-Netzwerk für den Grid-Knoten konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt „Client-Netzwerk“ nach Bedarf hinzu oder aktualisieren Sie sie. Wenn das Client-Netzwerk konfiguriert ist, ist das Gateway erforderlich und wird nach der Installation zum Standard-Gateway für den Knoten.

   > ⓘ Wenn Sie DHCP für die Client-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

   Geräte: Wenn das Client-Netzwerk eines StorageGRID Geräts während der Erstinstallation mit dem StorageGRID -Geräteinstallationsprogramm nicht konfiguriert wurde, kann es in diesem Grid Manager-Dialogfeld nicht konfiguriert werden. Stattdessen müssen Sie die folgenden Schritte ausführen:

   a. Starten Sie das Gerät neu: Wählen Sie im Geräteinstallationsprogramm **Erweitert** > **Neustart**.

      Der Neustart kann mehrere Minuten dauern.

   b. Wählen Sie **Netzwerk konfigurieren** > **Linkkonfiguration** und aktivieren Sie die entsprechenden Netzwerke.

   c. Wählen Sie **Netzwerk konfigurieren** > **IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.

   d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

   e. Im Grid Manager: Wenn der Knoten in der Tabelle „Genehmigte Knoten“ aufgeführt ist, entfernen Sie den Knoten.

   f. Entfernen Sie den Knoten aus der Tabelle „Ausstehende Knoten“.

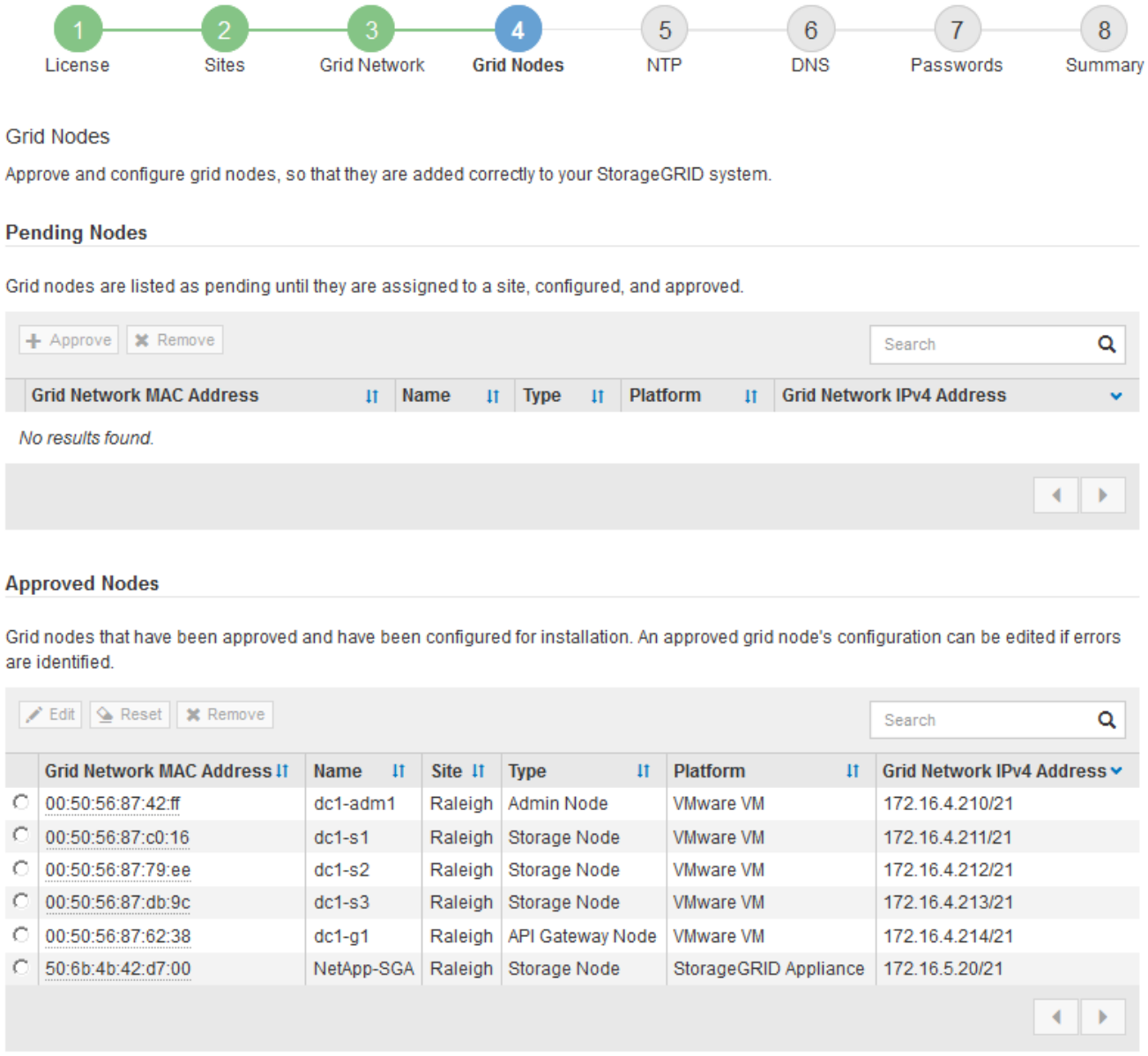
   g. Warten Sie, bis der Knoten wieder in der Liste „Ausstehende Knoten“ angezeigt wird.

   h. Bestätigen Sie, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt sein, die Sie auf der IP-Konfigurationsseite des Appliance-Installationsprogramms angegeben haben.

      Informationen zur Installation von StorageGRID -Geräten finden Sie im "Schnellstart für die Hardwareinstallation" um Anweisungen für Ihr Gerät zu finden.

8. Klicken Sie auf **Speichern**.

Der Rasterknoteneintrag wird in die Liste „Genehmigte Knoten“ verschoben.



9. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

   Sie müssen alle Knoten genehmigen, die Sie im Raster haben möchten. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Zusammenfassungsseite auf **Installieren** klicken. Sie können die Eigenschaften eines genehmigten Rasterknotens ändern, indem Sie dessen Optionsfeld auswählen und auf **Bearbeiten** klicken.

10. Wenn Sie mit der Genehmigung der Rasterknoten fertig sind, klicken Sie auf **Weiter**.

Geben Sie die Serverinformationen des Network Time Protocol an

Sie müssen die Network Time Protocol (NTP)-Konfigurationsinformationen für das StorageGRID -System angeben, damit die auf separaten Servern ausgeführten Vorgänge synchronisiert bleiben können.

Informationen zu diesem Vorgang

Sie müssen IPv4-Adressen für die NTP-Server angeben.

Sie müssen externe NTP-Server angeben. Die angegebenen NTP-Server müssen das NTP-Protokoll verwenden.

Sie müssen vier NTP-Serverreferenzen von Stratum 3 oder besser angeben, um Probleme mit Zeitabweichungen zu vermeiden.

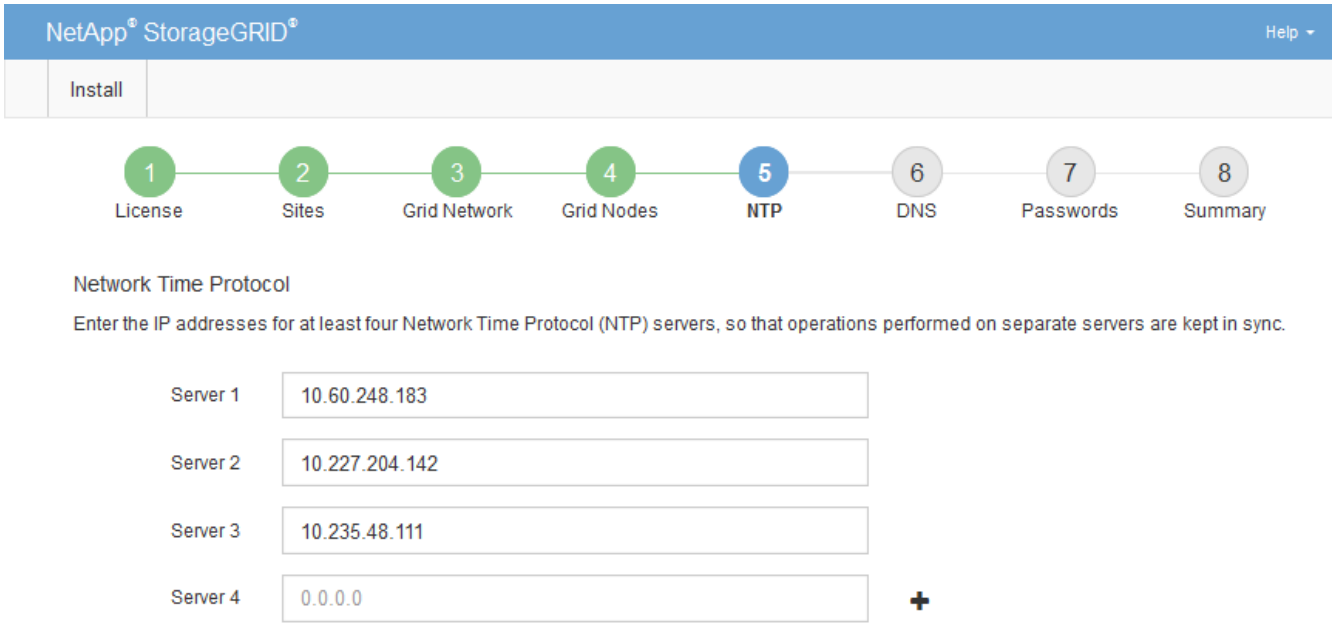
> Wenn Sie die externe NTP-Quelle für eine StorageGRID Installation auf Produktionsebene angeben, verwenden Sie den Windows-Zeitdienst (W32Time) nicht auf einer Windows-Version vor Windows Server 2016. Der Zeitdienst früherer Windows-Versionen ist nicht genau genug und wird von Microsoft für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, nicht unterstützt.
>
> "Supportgrenze zum Konfigurieren des Windows-Zeitdienstes für Umgebungen mit hoher Genauigkeit"

Die externen NTP-Server werden von den Knoten verwendet, denen Sie zuvor primäre NTP-Rollen zugewiesen haben.

> Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.

Schritte

1. Geben Sie die IPv4-Adressen für mindestens vier NTP-Server in den Textfeldern **Server 1** bis **Server 4** an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um weitere Servereinträge hinzuzufügen.



3. Wählen Sie **Weiter**.

Ähnliche Informationen

"Netzwerkrichtlinien"

DNS-Serverinformationen angeben

Sie müssen DNS-Informationen für Ihr StorageGRID -System angeben, damit Sie auf externe Server über Hostnamen statt über IP-Adressen zugreifen können.

Informationen zu diesem Vorgang

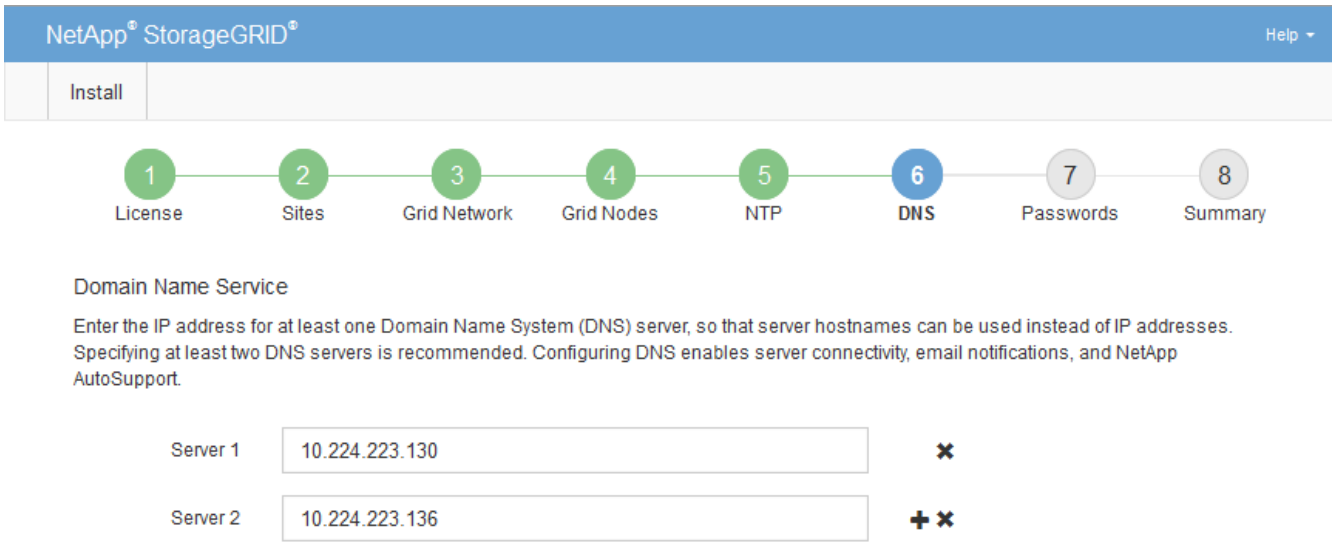
Festlegen "DNS-Serverinformationen" ermöglicht Ihnen die Verwendung von Fully Qualified Domain Name (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport.

Um einen ordnungsgemäßen Betrieb sicherzustellen, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, ist es möglich, dass aufgrund bekannter Betriebssystembeschränkungen auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie"Passen Sie die DNS-Serverliste an" für einzelne Knoten (normalerweise alle Knoten an einem Standort), einen anderen Satz von bis zu drei DNS-Servern zu verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein isolierter Standort die FQDNs für externe Ziele auflösen kann.

Schritte

1. Geben Sie im Textfeld **Server 1** die IPv4-Adresse für mindestens einen DNS-Server an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um weitere Servereinträge hinzuzufügen.



   Die beste Vorgehensweise besteht darin, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Geben Sie die StorageGRID -Systemkennwörter an

Im Rahmen der Installation Ihres StorageGRID -Systems müssen Sie die Passwörter eingeben, mit denen Sie Ihr System sichern und Wartungsaufgaben durchführen können.

Informationen zu diesem Vorgang

Verwenden Sie die Seite „Passwörter installieren“, um die Bereitstellungspassphrase und das Root-Benutzerpasswort für die Grid-Verwaltung anzugeben.

- Die Bereitstellungspassphrase wird als Verschlüsselungsschlüssel verwendet und nicht vom StorageGRID -System gespeichert.
- Sie müssen über die Bereitstellungspassphrase für Installations-, Erweiterungs- und Wartungsvorgänge verfügen, einschließlich des Herunterladens des Wiederherstellungspakets. Daher ist es wichtig, dass Sie die Bereitstellungspassphrase an einem sicheren Ort speichern.
- Sie können die Bereitstellungspassphrase im Grid Manager ändern, wenn Sie die aktuelle haben.
- Das Root-Benutzerkennwort für die Grid-Verwaltung kann mithilfe des Grid-Managers geändert werden.
- Zufällig generierte Befehlszeilenkonsolen- und SSH-Passwörter werden im `Passwords.txt` Datei im Wiederherstellungspaket.

Schritte

1. Geben Sie unter **Bereitstellungspassphrase** die Bereitstellungspassphrase ein, die zum Vornehmen von Änderungen an der Grid-Topologie Ihres StorageGRID Systems erforderlich ist.

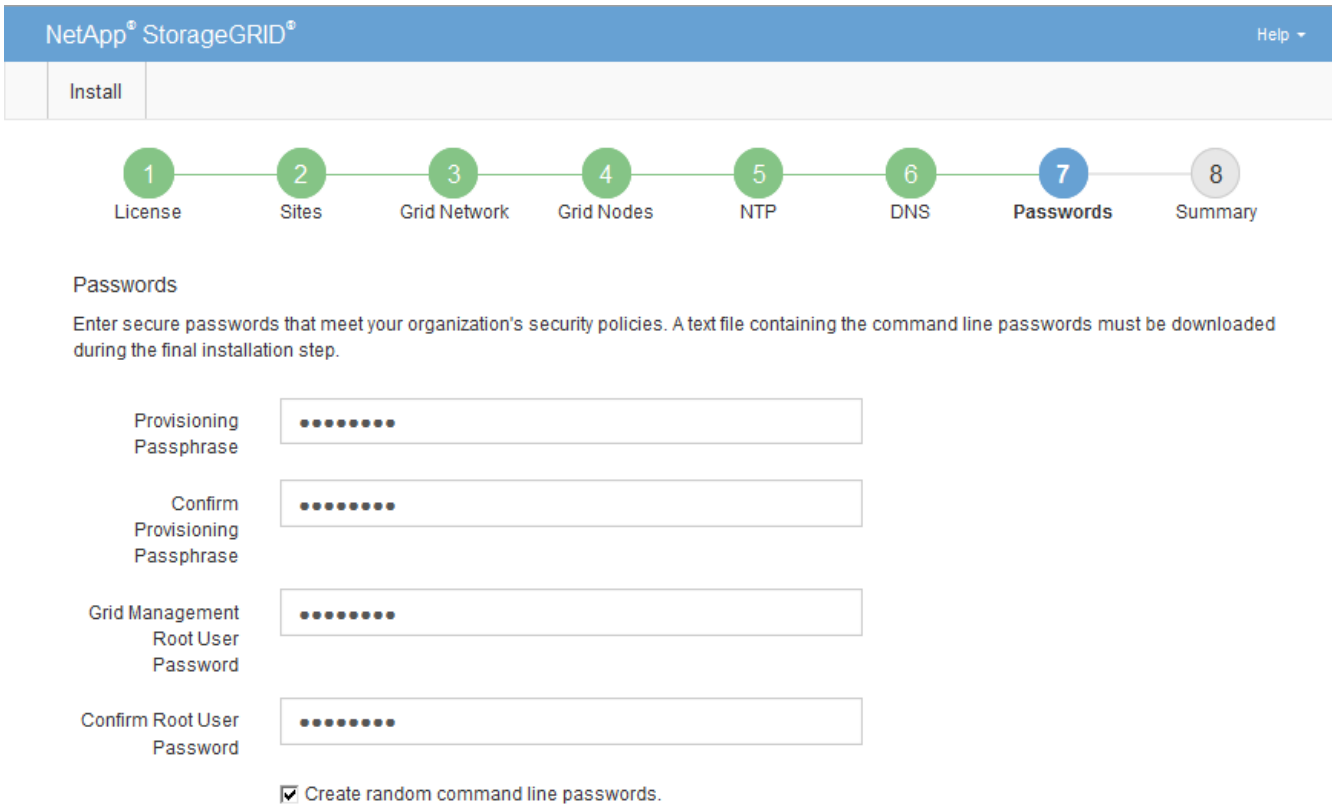
   Bewahren Sie die Bereitstellungspassphrase an einem sicheren Ort auf.

   > Wenn Sie nach Abschluss der Installation die Bereitstellungspassphrase später ändern möchten, können Sie den Grid Manager verwenden. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Grid-Passwörter**.

2. Geben Sie unter **Bereitstellungspassphrase bestätigen** die Bereitstellungspassphrase erneut ein, um sie zu bestätigen.
3. Geben Sie unter **Grid Management Root User Password** das Passwort ein, das Sie für den Zugriff auf den Grid Manager als „Root“-Benutzer verwenden möchten.

   Bewahren Sie das Passwort an einem sicheren Ort auf.

4. Geben Sie unter **Root-Benutzerkennwort bestätigen** das Grid Manager-Kennwort erneut ein, um es zu bestätigen.



5. Wenn Sie ein Grid zu Proof-of-Concept- oder Demozwecken installieren, deaktivieren Sie optional das Kontrollkästchen **Zufällige Befehlszeilenkennwörter erstellen**.

   Bei Produktionsbereitstellungen sollten aus Sicherheitsgründen immer zufällige Passwörter verwendet werden. Deaktivieren Sie **Zufällige Befehlszeilenkennwörter erstellen** nur für Demo-Raster, wenn Sie Standardkennwörter verwenden möchten, um über die Befehlszeile mit dem Konto „root“ oder „admin“ auf Rasterknoten zuzugreifen.

   > Sie werden aufgefordert, die Wiederherstellungspaketdatei herunterzuladen(`sgws-recovery-package-id-revision.zip`), nachdem Sie auf der Seite „Zusammenfassung“ auf **Installieren** geklickt haben. Sie müssen"Laden Sie diese Datei herunter" um die Installation abzuschließen. Die für den Zugriff auf das System erforderlichen Passwörter sind im `Passwords.txt` Datei, die in der Wiederherstellungspaketdatei enthalten ist.

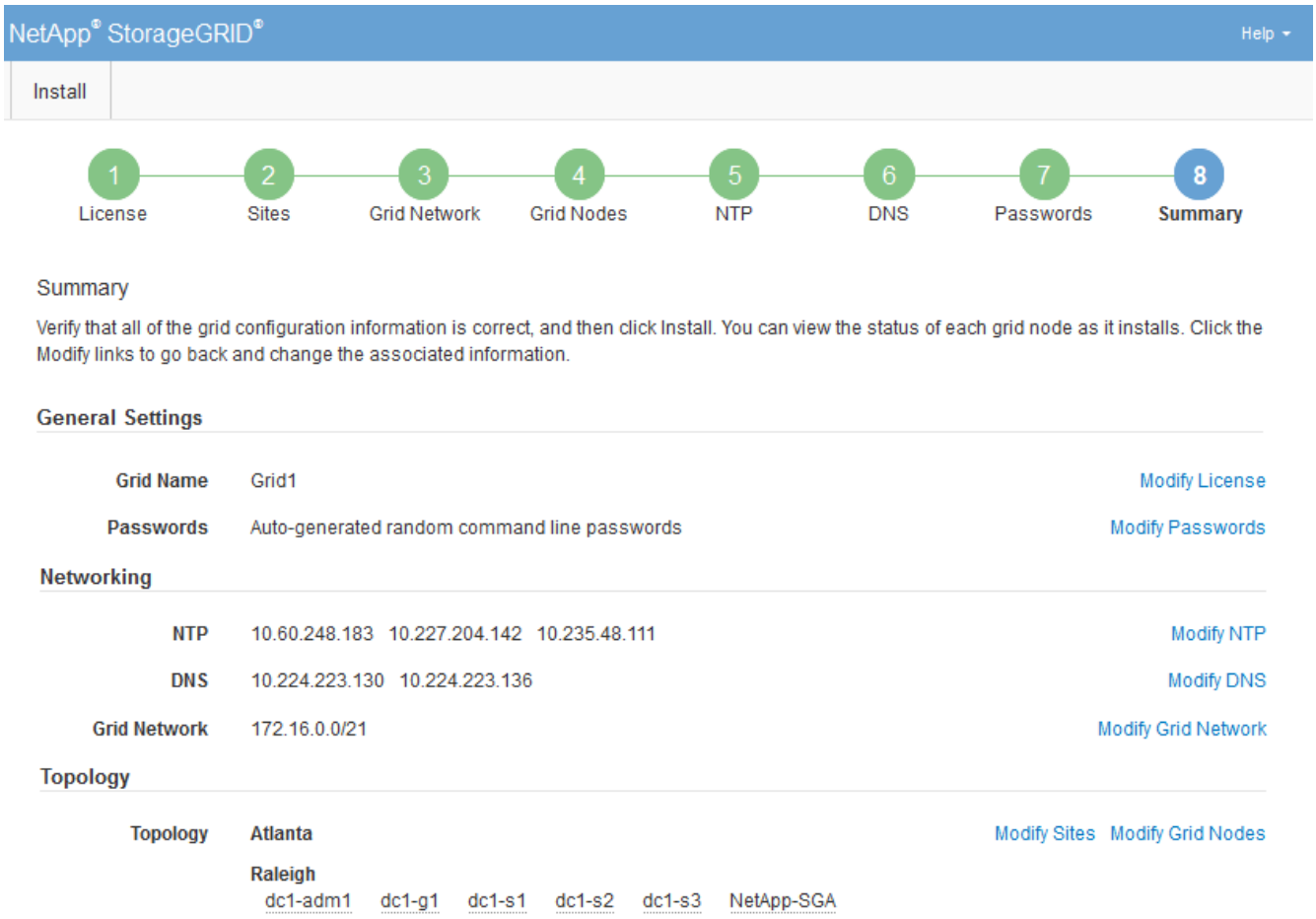
6. Klicken Sie auf **Weiter**.

Überprüfen Sie Ihre Konfiguration und schließen Sie die Installation ab

Sie müssen die eingegebenen Konfigurationsinformationen sorgfältig prüfen, um sicherzustellen, dass die Installation erfolgreich abgeschlossen wird.

Schritte

1. Sehen Sie sich die Seite **Zusammenfassung** an.



2. Überprüfen Sie, ob alle Informationen zur Netzkonfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite „Zusammenfassung“, um zurückzugehen und etwaige Fehler zu korrigieren.
3. Klicken Sie auf **Installieren**.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf **Installieren** klicken. Wenn die Verbindung verloren geht, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Knoten zugreifen. Sehen"Netzwerkrichtlinien" für Details.

4. Klicken Sie auf **Wiederherstellungspaket herunterladen**.

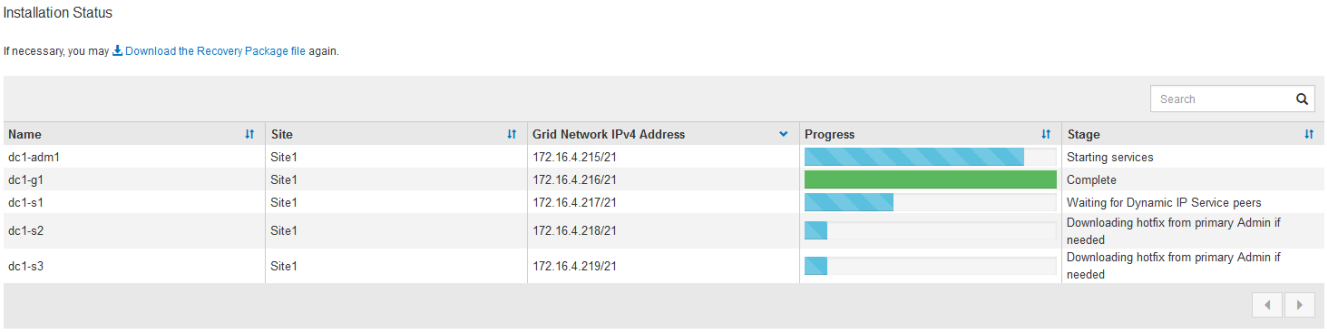
   Wenn die Installation bis zu dem Punkt fortschreitet, an dem die Grid-Topologie definiert ist, werden Sie aufgefordert, die Datei Recovery Package herunterzuladen(`.zip`) und bestätigen Sie, dass Sie erfolgreich auf den Inhalt dieser Datei zugreifen können. Sie müssen die Wiederherstellungspaketdatei herunterladen, damit Sie das StorageGRID -System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Die Installation wird im Hintergrund fortgesetzt, Sie können die Installation jedoch erst abschließen und auf das StorageGRID -System zugreifen, wenn Sie diese Datei heruntergeladen und überprüft haben.

5. Überprüfen Sie, ob Sie den Inhalt der `.zip` Datei und speichern Sie sie dann an zwei sicheren und getrennten Orten.

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

6. Aktivieren Sie das Kontrollkästchen **Ich habe die Wiederherstellungspaketdatei erfolgreich heruntergeladen und überprüft** und klicken Sie auf **Weiter**.

   Wenn die Installation noch läuft, wird die Statusseite angezeigt. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



   Wenn für alle Grid-Knoten die Phase „Abgeschlossen“ erreicht ist, wird die Anmeldeseite für den Grid Manager angezeigt.

7. Sign in beim Grid Manager mit dem Benutzer „root“ und dem Kennwort an, das Sie während der Installation angegeben haben.

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Bereitstellung und Konfiguration des Grid-Knotens diese Richtlinien für DHCP-Adressierung und Netzwerkkonfigurationsänderungen.

- Wenn DHCP zum Zuweisen von IP-Adressen verwendet wurde, konfigurieren Sie eine DHCP-Reservierung für jede IP-Adresse in den verwendeten Netzwerken.

  Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten.

  Knoten werden neu gestartet, wenn die Grid-Netzwerkkonfiguration per DHCP geändert wird. Dies kann zu Ausfällen führen, wenn eine DHCP-Änderung mehrere Knoten gleichzeitig betrifft.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmasken und Standard-Gateways für einen Grid-Knoten ändern möchten. Sehen "Konfigurieren von IP-Adressen" .
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin-Knoten und anderen Grid-Knoten verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Installation der REST-API

StorageGRID bietet die StorageGRID -Installations-API zum Ausführen von

Installationsaufgaben.

Die API verwendet die Open-Source-API-Plattform Swagger, um die API-Dokumentation bereitzustellen. Swagger ermöglicht sowohl Entwicklern als auch Nicht-Entwicklern die Interaktion mit der API in einer Benutzeroberfläche, die veranschaulicht, wie die API auf Parameter und Optionen reagiert. Diese Dokumentation setzt voraus, dass Sie mit Standard-Webtechnologien und dem JSON-Datenformat vertraut sind.

> 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.

Jeder REST-API-Befehl enthält die URL der API, eine HTTP-Aktion, alle erforderlichen oder optionalen URL-Parameter und eine erwartete API-Antwort.

StorageGRID Installations-API

Die StorageGRID Installations-API ist nur verfügbar, wenn Sie Ihr StorageGRID -System zum ersten Mal konfigurieren und eine Wiederherstellung des primären Admin-Knotens durchführen müssen. Auf die Installations-API kann über HTTPS vom Grid Manager aus zugegriffen werden.

Um auf die API-Dokumentation zuzugreifen, gehen Sie zur Installationswebseite auf dem primären Admin-Knoten und wählen Sie in der Menüleiste **Hilfe** > **API-Dokumentation**.

Die StorageGRID -Installations-API umfasst die folgenden Abschnitte:

- **config** – Vorgänge im Zusammenhang mit der Produktversion und den Versionen der API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **grid** – Konfigurationsvorgänge auf Grid-Ebene. Sie können Grid-Einstellungen abrufen und aktualisieren, einschließlich Grid-Details, Grid-Netzwerk-Subnetze, Grid-Passwörter sowie NTP- und DNS-Server-IP-Adressen.
- **Knoten** – Konfigurationsvorgänge auf Knotenebene. Sie können eine Liste von Grid-Knoten abrufen, einen Grid-Knoten löschen, einen Grid-Knoten konfigurieren, einen Grid-Knoten anzeigen und die Konfiguration eines Grid-Knotens zurücksetzen.
- **Bereitstellung** – Bereitstellungsvorgänge. Sie können den Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** – Wiederherstellungsvorgänge für den primären Admin-Knoten. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **recovery-package** – Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **Sites** – Konfigurationsvorgänge auf Site-Ebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.
- **temporäres Passwort** – Vorgänge für das temporäre Passwort, um die Mgmt-API während der Installation zu sichern.

Ähnliche Informationen

"Automatisieren der Installation"

Wohin als nächstes?

Führen Sie nach Abschluss einer Installation die erforderlichen Integrations- und Konfigurationsaufgaben durch. Sie können die optionalen Aufgaben nach Bedarf ausführen.

Erforderliche Aufgaben

- "Erstellen Sie ein Mieterkonto"für das S3-Clientprotokoll, das zum Speichern von Objekten auf Ihrem StorageGRID System verwendet wird.
- "Kontrollsystemzugriff"durch Konfigurieren von Gruppen und Benutzerkonten. Optional können Sie"Konfigurieren einer föderierten Identitätsquelle" (wie Active Directory oder OpenLDAP), sodass Sie Administrationsgruppen und Benutzer importieren können. Oder Sie können"Erstellen Sie lokale Gruppen und Benutzer" .
- Integrieren und testen Sie die"S3 API" Clientanwendungen, die Sie zum Hochladen von Objekten in Ihr StorageGRID System verwenden.
- "Konfigurieren der Regeln und Richtlinien für das Information Lifecycle Management (ILM)"Sie zum Schutz der Objektdaten verwenden möchten.
- Wenn Ihre Installation Appliance-Speicherknoten umfasst, verwenden Sie SANtricity OS, um die folgenden Aufgaben auszuführen:
  - Stellen Sie eine Verbindung zu jedem StorageGRID Gerät her.
  - Überprüfen Sie den Erhalt der AutoSupport -Daten.

    Sehen "Hardware einrichten" .
- Überprüfen und befolgen Sie die"Richtlinien zur Systemhärtung von StorageGRID" um Sicherheitsrisiken auszuschließen.
- "Konfigurieren Sie E-Mail-Benachrichtigungen für Systemwarnungen" .

Optionale Aufgaben

- "Aktualisieren Sie die IP-Adressen der Grid-Knoten"ob sie sich seit der Planung Ihrer Bereitstellung und der Generierung des Wiederherstellungspakets geändert haben.
- "Konfigurieren der Speicherverschlüsselung", falls erforderlich.
- "Konfigurieren der Speicherkomprimierung"um die Größe gespeicherter Objekte bei Bedarf zu reduzieren.
- "Konfigurieren von VLAN-Schnittstellen"um den Netzwerkverkehr bei Bedarf zu isolieren und zu partitionieren.
- "Konfigurieren von Hochverfügbarkeitsgruppen"um bei Bedarf die Verbindungsverfügbarkeit für Grid Manager, Tenant Manager und S3-Clients zu verbessern.
- "Konfigurieren von Load Balancer-Endpunkten"für S3-Client-Konnektivität, falls erforderlich.

Beheben von Installationsproblemen

Wenn bei der Installation Ihres StorageGRID -Systems Probleme auftreten, können Sie auf die Installationsprotokolldateien zugreifen. Der technische Support muss möglicherweise auch die Installationsprotokolldateien verwenden, um Probleme zu lösen.

Die folgenden Installationsprotokolldateien sind aus dem Container verfügbar, in dem jeder Knoten ausgeführt wird:

- `/var/local/log/install.log`(auf allen Grid-Knoten zu finden)
- `/var/local/log/gdu-server.log`(auf dem primären Admin-Knoten zu finden)

Die folgenden Installationsprotokolldateien sind vom Host verfügbar:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

Informationen zum Zugriff auf die Protokolldateien finden Sie unter"Erfassen von Protokolldateien und Systemdaten" .

Ähnliche Informationen

"Fehlerbehebung bei einem StorageGRID -System"

Beispiel /etc/network/interfaces

Der `/etc/network/interfaces` Die Datei enthält drei Abschnitte, die die physischen Schnittstellen, die Bond-Schnittstelle und die VLAN-Schnittstellen definieren. Sie können die drei Beispielabschnitte in einer einzigen Datei kombinieren, die vier physische Linux-Schnittstellen in einer einzigen LACP-Verbindung zusammenfasst und dann drei VLAN-Schnittstellen einrichtet, die die Verbindung zur Verwendung als StorageGRID Grid-, Admin- und Client-Netzwerkschnittstellen unterteilen.

Physikalische Schnittstellen

Beachten Sie, dass die Switches an den anderen Enden der Links die vier Ports ebenfalls als einen einzigen LACP-Trunk oder Port-Kanal behandeln und mindestens die drei referenzierten VLANs mit Tags übergeben müssen.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Bond-Schnittstelle

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

VLAN-Schnittstellen

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Installieren Sie StorageGRID auf VMware

Schnellstart zur Installation von StorageGRID auf VMware

Befolgen Sie diese allgemeinen Schritte, um einen VMware StorageGRID Knoten zu installieren.

1 **Vorbereitung**

- Erfahren Sie mehr über"StorageGRID -Architektur und Netzwerktopologie" .
- Erfahren Sie mehr über die Besonderheiten von"StorageGRID Netzwerk" .
- Sammeln und vorbereiten Sie die"Benötigte Informationen und Materialien" .
- Installieren und Konfigurieren"VMware vSphere Hypervisor, vCenter und die ESX-Hosts" .
- Bereiten Sie die erforderlichen"CPU und RAM" .
- Sorgen für"Speicher- und Leistungsanforderungen" .

2 **Einsatz**

Stellen Sie Grid-Knoten bereit. Wenn Sie Grid-Knoten bereitstellen, werden diese als Teil des StorageGRID -Systems erstellt und mit einem oder mehreren Netzwerken verbunden.

- Verwenden Sie den VMware vSphere Web Client, eine .vmdk-Datei und eine Reihe von .ovf-Dateivorlagen, um"Stellen Sie die softwarebasierten Knoten als virtuelle Maschinen (VMs) bereit." auf den Servern, die Sie in Schritt 1 vorbereitet haben.
- Um StorageGRID Appliance-Knoten bereitzustellen, folgen Sie den "Schnellstart für die Hardwareinstallation" .

3 **Konfiguration**

Wenn alle Knoten bereitgestellt wurden, verwenden Sie den Grid Manager, um"Konfigurieren Sie das Grid und schließen Sie die Installation ab" .

Automatisieren Sie die Installation

Um Zeit zu sparen und Konsistenz zu gewährleisten, können Sie die Bereitstellung und Konfiguration von Grid-Knoten und die Konfiguration des StorageGRID Systems automatisieren.

- "Automatisieren Sie die Bereitstellung von Grid-Knoten mit VMware vSphere" .
- Nachdem Sie Grid-Knoten bereitgestellt haben,"Automatisieren Sie die Konfiguration des StorageGRID -Systems" mithilfe des im Installationsarchiv bereitgestellten Python-Konfigurationsskripts.
- "Automatisieren Sie die Installation und Konfiguration von Appliance-Grid-Knoten"
- Wenn Sie ein fortgeschrittener Entwickler von StorageGRID Bereitstellungen sind, automatisieren Sie die Installation von Grid-Knoten mithilfe der"Installation der REST-API" .

Planen und Vorbereiten der Installation auf VMware

Benötigte Informationen und Materialien

Bevor Sie StorageGRID installieren, sammeln und bereiten Sie die erforderlichen Informationen und Materialien vor.

Erforderliche Informationen

Netzwerkplan

Welche Netzwerke Sie an jeden StorageGRID Knoten anschließen möchten. StorageGRID unterstützt mehrere Netzwerke zur Verkehrstrennung, Sicherheit und Verwaltungsfreundlichkeit.

Zum StorageGRID"Netzwerkrichtlinien" .

Netzwerkinformationen

Jedem Grid-Knoten zuzuweisende IP-Adressen und die IP-Adressen der DNS- und NTP-Server.

Server für Grid-Knoten

Identifizieren Sie eine Reihe von Servern (physisch, virtuell oder beides), die insgesamt ausreichend Ressourcen bereitstellen, um die Anzahl und Art der StorageGRID Knoten zu unterstützen, die Sie bereitstellen möchten.

> ⓘ Wenn Ihre StorageGRID Installation keine StorageGRID Appliance-(Hardware-)Speicherknoten verwendet, müssen Sie Hardware-RAID-Speicher mit batteriegepuffertem Schreibcache (BBWC) verwenden. StorageGRID unterstützt nicht die Verwendung von virtuellen Storage Area Networks (vSANs), Software-RAID oder keinen RAID-Schutz.

Ähnliche Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Benötigtes Material

NetApp StorageGRID -Lizenz

Sie müssen über eine gültige, digital signierte NetApp -Lizenz verfügen.

Eine Nicht-Produktionslizenz, die zum Testen und Proof-of-Concept-Grids verwendet werden kann, ist im StorageGRID -Installationsarchiv enthalten.

StorageGRID -Installationsarchiv

"Laden Sie das StorageGRID Installationsarchiv herunter und extrahieren Sie die Dateien" .

Service-Laptop

Die Installation des StorageGRID -Systems erfolgt über einen Service-Laptop.

Der Dienstlaptop muss über Folgendes verfügen:

- Netzwerkanschluss
- SSH-Client (z. B. PuTTY)
- "Unterstützte Webbrowser"

StorageGRID -Dokumentation

- "Versionshinweise"
- "Anleitung zur Administration von StorageGRID"

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Sie müssen die StorageGRID Installationsarchive herunterladen und die Dateien extrahieren. Optional können Sie die Dateien im Installationspaket manuell überprüfen.

Schritte

1. Gehen Sie zum "NetApp -Downloadseite für StorageGRID" .
2. Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version oder wählen Sie eine andere Version aus dem Dropdown-Menü und wählen Sie **Los**.
3. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Ihr NetApp -Konto an .
4. Wenn eine Warnung/ein unbedingt zu lesender Hinweis erscheint, lesen Sie ihn und aktivieren Sie das Kontrollkästchen.

   Sie müssen alle erforderlichen Hotfixes anwenden, nachdem Sie die StorageGRID Version installiert haben. Weitere Informationen finden Sie im"Hotfix-Verfahren in den Wiederherstellungs- und Wartungsanweisungen"

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.
6. Wählen Sie in der Spalte **Install StorageGRID** das .tgz- oder .zip-Installationsarchiv für VMware aus.

   Verwenden Sie die `.zip` Datei, wenn Sie Windows auf dem Service-Laptop ausführen.

7. Speichern Sie das Installationsarchiv.
8. Wenn Sie das Installationsarchiv überprüfen müssen:
   a. Laden Sie das StorageGRID -Codesignaturüberprüfungspaket herunter. Der Dateiname für dieses Paket verwendet das Format `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , Wo `<version-number>` ist die

StorageGRID -Softwareversion.

b. Folgen Sie den Schritten, um"Überprüfen Sie die Installationsdateien manuell" .

9. Extrahieren Sie die Dateien aus dem Installationsarchiv.
10. Wählen Sie die benötigten Dateien aus.

    Welche Dateien Sie benötigen, hängt von Ihrer geplanten Grid-Topologie und der Art und Weise ab, wie Sie Ihr StorageGRID -System bereitstellen.

> Die in der Tabelle aufgeführten Pfade beziehen sich auf das oberste Verzeichnis, das durch das extrahierte Installationsarchiv installiert wird.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet.
	Die Festplattendatei der virtuellen Maschine, die als Vorlage zum Erstellen virtueller Grid-Knotenmaschinen verwendet wird.
	Die Open Virtualization Format-Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen des primären Admin-Knotens.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen nicht primärer Admin-Knoten.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Gateway-Knoten.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Speicherknoten auf Basis virtueller Maschinen.
Bereitstellungsskripttool	Beschreibung
	Ein Bash-Shell-Skript zur Automatisierung der Bereitstellung virtueller Grid-Knoten.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `deploy-vsphere-ovftool.sh` Skript.
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.

Pfad und Dateiname	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On (SSO) aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

Installationsdateien manuell überprüfen (optional)

Bei Bedarf können Sie die Dateien im StorageGRID Installationsarchiv manuell überprüfen.

Bevor Sie beginnen

Du hast"das Verifizierungspaket heruntergeladen" aus dem "NetApp -Downloadseite für StorageGRID" .

Schritte

1. Extrahieren Sie die Artefakte aus dem Verifizierungspaket:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Stellen Sie sicher, dass diese Artefakte extrahiert wurden:
   - Blattzertifikat: `Leaf-Cert.pem`
   - Zertifikatskette: `CA-Int-Cert.pem`
   - Zeitstempel-Antwortkette: `TS-Cert.pem`
   - Prüfsummendatei: `sha256sum`
   - Prüfsummensignatur: `sha256sum.sig`
   - Zeitstempel-Antwortdatei: `sha256sum.sig.tsr`
3. Verwenden Sie die Kette, um zu überprüfen, ob das Blattzertifikat gültig ist.

   Beispiel: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

   Erwartete Ausgabe: `Leaf-Cert.pem: OK`

4. Wenn Schritt *2* aufgrund eines abgelaufenen Blattzertifikats fehlgeschlagen ist, verwenden Sie die `tsr` zu überprüfende Datei.

   Beispiel: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

   Die erwartete Ausgabe umfasst: `Verification: OK`

5. Erstellen Sie eine öffentliche Schlüsseldatei aus dem Blattzertifikat.

   Beispiel: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

   Erwartete Ausgabe: *keine*

6. Verwenden Sie den öffentlichen Schlüssel, um die `sha256sum` Datei gegen `sha256sum.sig` .

   Beispiel: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   Erwartete Ausgabe: `Verified OK`

7. Überprüfen Sie die `sha256sum` Dateiinhalte mit neu erstellten Prüfsummen vergleichen.

   Beispiel: `sha256sum -c sha256sum`

   Erwartete Ausgabe: *<filename>*`: OK`
   <filename> ist der Name der Archivdatei, die Sie heruntergeladen haben.

8. "Führen Sie die restlichen Schritte aus"um die entsprechenden Installationsdateien zu extrahieren und auszuwählen.

Softwareanforderungen für VMware

Sie können eine virtuelle Maschine verwenden, um jeden StorageGRID Knotentyp zu hosten. Sie benötigen eine virtuelle Maschine für jeden Grid-Knoten.

VMware vSphere Hypervisor

Sie müssen VMware vSphere Hypervisor auf einem vorbereiteten physischen Server installieren. Die Hardware muss richtig konfiguriert sein (einschließlich Firmware-Versionen und BIOS-Einstellungen), bevor Sie die VMware-Software installieren.

- Konfigurieren Sie die Vernetzung im Hypervisor nach Bedarf, um die Vernetzung für das StorageGRID -System zu unterstützen, das Sie installieren.

  "Netzwerkrichtlinien"

- Stellen Sie sicher, dass der Datenspeicher groß genug für die virtuellen Maschinen und virtuellen Datenträger ist, die zum Hosten der Grid-Knoten erforderlich sind.
- Wenn Sie mehr als einen Datenspeicher erstellen, benennen Sie jeden Datenspeicher, damit Sie beim Erstellen virtueller Maschinen leicht erkennen können, welcher Datenspeicher für welchen Grid-Knoten verwendet werden soll.

ESX-Host-Konfigurationsanforderungen

Sie müssen das Network Time Protocol (NTP) auf jedem ESX-Host richtig konfigurieren. Wenn die Hostzeit falsch ist, können negative Auswirkungen bis hin zum Datenverlust auftreten.

VMware-Konfigurationsanforderungen

Sie müssen VMware vSphere und vCenter installieren und konfigurieren, bevor Sie StorageGRID -Knoten bereitstellen.

Informationen zu unterstützten Versionen der VMware vSphere Hypervisor- und VMware vCenter Server-Software finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Die zur Installation dieser VMware-Produkte erforderlichen Schritte finden Sie in der VMware-Dokumentation.

CPU- und RAM-Anforderungen

Überprüfen und konfigurieren Sie vor der Installation der StorageGRID -Software die Hardware, sodass sie das StorageGRID -System unterstützen kann.

Jeder StorageGRID -Knoten benötigt die folgenden Mindestressourcen:

- CPU-Kerne: 8 pro Knoten
- RAM: Abhängig vom insgesamt verfügbaren RAM und der Menge der auf dem System ausgeführten Nicht-StorageGRID -Software
  - Im Allgemeinen mindestens 24 GB pro Knoten und 2 bis 16 GB weniger als der gesamte System-RAM
  - Mindestens 64 GB für jeden Mandanten mit etwa 5.000 Buckets

Softwarebasierte Knotenressourcen, die nur Metadaten enthalten, müssen mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:

- Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
  - 128 GB RAM

    - 8-Kern-CPU
    - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)
- Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).

Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

VMware unterstützt einen Knoten pro virtueller Maschine. Stellen Sie sicher, dass der StorageGRID Knoten den verfügbaren physischen RAM nicht überschreitet. Jede virtuelle Maschine muss ausschließlich für die Ausführung von StorageGRID vorgesehen sein.

> Überwachen Sie regelmäßig Ihre CPU- und Speichernutzung, um sicherzustellen, dass diese Ressourcen weiterhin Ihrer Arbeitslast gerecht werden. Beispielsweise würde eine Verdoppelung der RAM- und CPU-Zuweisung für virtuelle Speicherknoten ähnliche Ressourcen bereitstellen wie für StorageGRID Appliance-Knoten. Wenn die Menge der Metadaten pro Knoten 500 GB übersteigt, sollten Sie außerdem eine Erhöhung des RAM pro Knoten auf 48 GB oder mehr in Betracht ziehen. Informationen zum Verwalten des Objektmetadatenspeichers, zum Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten und zum Überwachen der CPU- und Speicherauslastung finden Sie in den Anweisungen für"Verabreichung" ,"Überwachung" , Und"Upgrade" StorageGRID.

Wenn Hyperthreading auf den zugrunde liegenden physischen Hosts aktiviert ist, können Sie 8 virtuelle Kerne (4 physische Kerne) pro Knoten bereitstellen. Wenn Hyperthreading auf den zugrunde liegenden physischen Hosts nicht aktiviert ist, müssen Sie 8 physische Kerne pro Knoten bereitstellen.

Wenn Sie virtuelle Maschinen als Hosts verwenden und die Kontrolle über die Größe und Anzahl der VMs haben, sollten Sie für jeden StorageGRID Knoten eine einzelne VM verwenden und die VM entsprechend dimensionieren.

Siehe auch "Speicher- und Leistungsanforderungen".

Speicher- und Leistungsanforderungen

Sie müssen die Speicher- und Leistungsanforderungen für StorageGRID -Knoten verstehen, die von virtuellen Maschinen gehostet werden, damit Sie genügend Speicherplatz bereitstellen können, um die Erstkonfiguration und zukünftige Speichererweiterungen zu unterstützen.

Leistungsanforderungen

Die Leistung des Betriebssystem-Volumes und des ersten Speicher-Volumes hat erhebliche Auswirkungen auf die Gesamtleistung des Systems. Stellen Sie sicher, dass diese hinsichtlich Latenz, Eingabe-/Ausgabevorgängen pro Sekunde (IOPS) und Durchsatz eine ausreichende Festplattenleistung bieten.

Für alle StorageGRID -Knoten muss auf dem Betriebssystemlaufwerk und allen Speichervolumes das Write-Back-Caching aktiviert sein. Der Cache muss sich auf einem geschützten oder dauerhaften Medium befinden.

Anforderungen für virtuelle Maschinen, die NetApp ONTAP -Speicher verwenden

Wenn Sie einen StorageGRID -Knoten als virtuelle Maschine mit zugewiesenem Speicher aus einem NetApp ONTAP System bereitstellen, haben Sie bestätigt, dass für das Volume keine FabricPool -Tiering-Richtlinie aktiviert ist. Wenn beispielsweise ein StorageGRID Knoten als virtuelle Maschine auf einem VMware-Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datenspeicher für den Knoten unterstützt, keine FabricPool -Tiering-Richtlinie aktiviert ist. Das Deaktivieren der FabricPool Tiering-Funktion für Volumes, die mit StorageGRID -Knoten verwendet werden, vereinfacht die Fehlerbehebung und Speichervorgänge.

> Verwenden Sie FabricPool niemals, um Daten im Zusammenhang mit StorageGRID zurück auf StorageGRID selbst zu verschieben. Das Zurückführen von StorageGRID -Daten in StorageGRID erhöht die Fehlerbehebung und die Betriebskomplexität.

Anzahl der benötigten virtuellen Maschinen

Jeder StorageGRID Standort benötigt mindestens drei Speicherknoten.

Speicheranforderungen nach Knotentyp

In einer Produktionsumgebung müssen die virtuellen Maschinen für StorageGRID -Knoten je nach Knotentyp unterschiedliche Anforderungen erfüllen.

> Festplatten-Snapshots können nicht zum Wiederherstellen von Grid-Knoten verwendet werden. Beziehen Sie sich stattdessen auf die"Wiederherstellung von Grid-Knoten" Verfahren für jeden Knotentyp.

Knotentyp	Storage
Admin-Knoten	100 GB LUN für Betriebssystem 200 GB LUN für Admin-Knotentabellen 200 GB LUN für das Audit-Protokoll des Admin-Knotens
Speicherknoten	100 GB LUN für Betriebssystem 3 LUNs für jeden Speicherknoten auf diesem Host **Hinweis**: Ein Speicherknoten kann 1 bis 16 Speicher-LUNs haben; mindestens 3 Speicher-LUNs werden empfohlen. Mindestgröße pro LUN: 4 TB Maximal getestete LUN-Größe: 39 TB.

Knotentyp	Storage
Speicherknoten (nur Metadaten)	100 GB LUN für Betriebssystem 1 LUN Mindestgröße pro LUN: 4 TB Maximal getestete LUN-Größe: 39 TB. **Hinweis**: Für reine Metadaten-Speicherknoten ist nur eine Rangedb erforderlich.
Gateway-Knoten	100 GB LUN für Betriebssystem

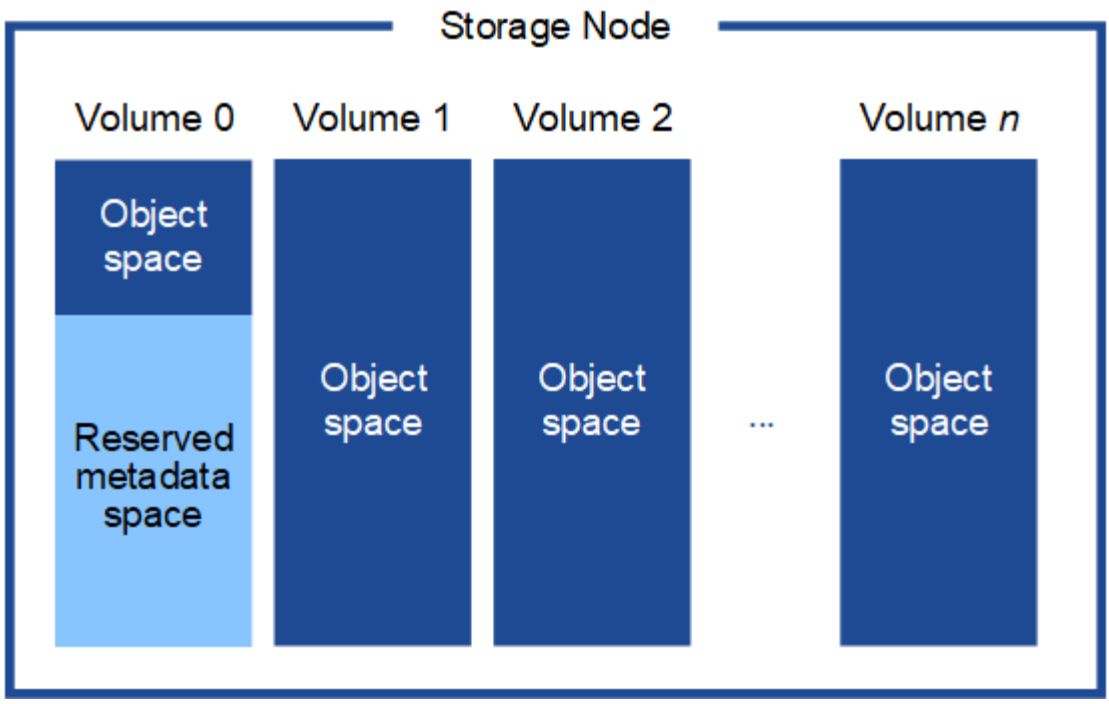
Abhängig von der konfigurierten Prüfebene, der Größe der Benutzereingaben wie dem S3-Objektschlüsselnamen und der Menge der zu bewahrenden Prüfprotokolldaten müssen Sie möglicherweise die Größe der Prüfprotokoll-LUN auf jedem Admin-Knoten erhöhen. Im Allgemeinen generiert ein Grid ungefähr 1 KB Prüfdaten pro S3-Vorgang, was bedeuten würde, dass ein 200 GB großes LUN 70 Millionen Vorgänge pro Tag oder 800 Vorgänge pro Sekunde für zwei bis drei Tage unterstützen würde.

Speicheranforderungen für Speicherknoten

Ein softwarebasierter Speicherknoten kann 1 bis 16 Speichervolumes haben; 3 oder mehr Speichervolumes werden empfohlen. Jedes Speichervolumen sollte mindestens 4 TB groß sein.

Ein Appliance-Speicherknoten kann außerdem über bis zu 48 Speichervolumes verfügen.

Wie in der Abbildung gezeigt, reserviert StorageGRID Speicherplatz für Objektmetadaten auf Speichervolume 0 jedes Speicherknotens. Der verbleibende Speicherplatz auf Speichervolume 0 und allen anderen Speichervolumes im Speicherknoten wird ausschließlich für Objektdaten verwendet.



Um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen, speichert StorageGRID an jedem Standort drei Kopien der Metadaten für alle Objekte im System. Die drei Kopien der Objektmetadaten werden gleichmäßig auf alle Speicherknoten an jedem Standort verteilt.

Wenn Sie ein Grid mit reinen Metadaten-Speicherknoten installieren, muss das Grid auch eine Mindestanzahl von Knoten für die Objektspeicherung enthalten. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

- Für ein Single-Site-Grid werden mindestens zwei Storage Nodes für Objekte und Metadaten konfiguriert.
- Für ein Multi-Site-Grid wird mindestens ein Storage Node pro Site für Objekte und Metadaten konfiguriert.

Wenn Sie dem Datenträger 0 eines neuen Speicherknotens Speicherplatz zuweisen, müssen Sie sicherstellen, dass für den Teil aller Objektmetadaten dieses Knotens ausreichend Speicherplatz vorhanden ist.

- Sie müssen dem Volume 0 mindestens 4 TB zuweisen.

  Wenn Sie für einen Speicherknoten nur ein Speichervolume verwenden und dem Volume 4 TB oder weniger zuweisen, wechselt der Speicherknoten beim Start möglicherweise in den schreibgeschützten Speicherzustand und speichert nur Objektmetadaten.

  Wenn Sie Volume 0 (nur für nicht produktive Verwendung) weniger als 500 GB zuweisen, werden 10 % der Kapazität des Speichervolumes für Metadaten reserviert.

- Softwarebasierte Knotenressourcen, die nur Metadaten enthalten, müssen mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:
  - Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
    - 128 GB RAM
    - 8-Kern-CPU
    - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)

- Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).

  Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

- Wenn Sie ein neues System (StorageGRID 11.6 oder höher) installieren und jeder Speicherknoten über 128 GB oder mehr RAM verfügt, weisen Sie Volume 0 8 TB oder mehr zu. Durch die Verwendung eines größeren Werts für Volume 0 kann der für Metadaten auf jedem Speicherknoten zulässige Speicherplatz erhöht werden.
- Wenn Sie verschiedene Speicherknoten für eine Site konfigurieren, verwenden Sie nach Möglichkeit dieselbe Einstellung für Volume 0. Wenn eine Site Speicherknoten unterschiedlicher Größe enthält, bestimmt der Speicherknoten mit dem kleinsten Volume 0 die Metadatenkapazität dieser Site.

Weitere Informationen finden Sie unter"Verwalten des Objektmetadatenspeichers" .

Automatisieren Sie die Installation (VMware)

Sie können das VMware OVF-Tool verwenden, um die Bereitstellung von Grid-Knoten zu automatisieren. Sie können die Konfiguration von StorageGRID auch automatisieren.

Automatisieren Sie die Bereitstellung von Grid-Knoten

Verwenden Sie das VMware OVF-Tool, um die Bereitstellung von Grid-Knoten zu automatisieren.

Bevor Sie beginnen

- Sie haben Zugriff auf ein Linux/Unix-System mit Bash 3.2 oder höher.
- Sie verfügen über VMware vSphere mit vCenter
- Sie haben VMware OVF Tool 4.1 installiert und richtig konfiguriert.
- Sie kennen den Benutzernamen und das Kennwort für den Zugriff auf VMware vSphere mithilfe des OVF-Tools
- Sie verfügen über ausreichende Berechtigungen, um VMs aus OVF-Dateien bereitzustellen und einzuschalten, sowie über die Berechtigung, zusätzliche Volumes zum Anhängen an die VMs zu erstellen. Siehe die `ovftool` Einzelheiten finden Sie in der Dokumentation.
- Sie kennen die URL der virtuellen Infrastruktur (VI) für den Speicherort in vSphere, an dem Sie die virtuellen StorageGRID -Maschinen bereitstellen möchten. Bei dieser URL handelt es sich normalerweise um eine vApp oder einen Ressourcenpool. Beispiel: `vi://vcenter.example.com/vi/sgws`

  Sie können die VMware `ovftool` Dienstprogramm, um diesen Wert zu bestimmen (siehe `ovftool` Einzelheiten finden Sie in der Dokumentation).

  Wenn Sie die Bereitstellung in einer vApp durchführen, werden die virtuellen Maschinen beim ersten Mal nicht automatisch gestartet und Sie müssen sie manuell einschalten.

- Sie haben alle erforderlichen Informationen für die Bereitstellungskonfigurationsdatei gesammelt. Sehen"Sammeln Sie Informationen zu Ihrer Bereitstellungsumgebung" für weitere Informationen.
- Sie haben Zugriff auf die folgenden Dateien aus dem VMware-Installationsarchiv für StorageGRID:

Dateiname	Beschreibung
NetApp-SG-version-SHA.vmdk	Die Festplattendatei der virtuellen Maschine, die als Vorlage zum Erstellen virtueller Grid-Knotenmaschinen verwendet wird. **Hinweis:** Diese Datei muss sich im selben Ordner befinden wie die `.ovf` Und `.mf` Dateien.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Die Open Virtualization Format-Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen des primären Admin-Knotens.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen nicht primärer Admin-Knoten.
vsphere-gateway.ovf vsphere-gateway.mf	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Gateway-Knoten.
vsphere-storage.ovf vsphere-storage.mf	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Speicherknoten auf Basis virtueller Maschinen.
deploy-vsphere-ovftool.sh	Das Bash-Shell-Skript wird zur Automatisierung der Bereitstellung virtueller Grid-Knoten verwendet.
Deploy-vsphere-ovftool-sample.ini	Die Beispielkonfigurationsdatei zur Verwendung mit dem `deploy-vsphere-ovftool.sh` Skript.

Definieren Sie die Konfigurationsdatei für Ihre Bereitstellung

Sie geben die Informationen an, die zum Bereitstellen virtueller Grid-Knoten für StorageGRID erforderlich sind, in einer Konfigurationsdatei, die von der `deploy-vsphere-ovftool.sh` Bash-Skript. Sie können eine Beispielkonfigurationsdatei ändern, sodass Sie die Datei nicht von Grund auf neu erstellen müssen.

Schritte

1. Erstellen Sie eine Kopie der Beispielkonfigurationsdatei(`deploy-vsphere-ovftool.sample.ini`). Speichern Sie die neue Datei unter `deploy-vsphere-ovftool.ini` im selben Verzeichnis wie `deploy-vsphere-ovftool.sh` .
2. Offen `deploy-vsphere-ovftool.ini` .
3. Geben Sie alle Informationen ein, die zum Bereitstellen virtueller VMware-Grid-Knoten erforderlich sind.

   SehenEinstellungen der Konfigurationsdatei für weitere Informationen.

4. Wenn Sie alle erforderlichen Informationen eingegeben und überprüft haben, speichern und schließen Sie die Datei.

Einstellungen der Konfigurationsdatei

Der `deploy-vsphere-ovftool.ini` Die Konfigurationsdatei enthält die Einstellungen, die zum Bereitstellen virtueller Grid-Knoten erforderlich sind.

Die Konfigurationsdatei listet zunächst globale Parameter auf und listet dann knotenspezifische Parameter in Abschnitten auf, die durch den Knotennamen definiert sind. Wenn die Datei verwendet wird:

- *Globale Parameter* werden auf alle Rasterknoten angewendet.
- *Knotenspezifische Parameter* überschreiben globale Parameter.

Globale Parameter

Globale Parameter werden auf alle Rasterknoten angewendet, sofern sie nicht durch Einstellungen in einzelnen Abschnitten überschrieben werden. Platzieren Sie die Parameter, die für mehrere Knoten gelten, im Abschnitt „Globale Parameter“ und überschreiben Sie diese Einstellungen dann nach Bedarf in den Abschnitten für einzelne Knoten.

- **OVFTOOL_ARGUMENTS**: Sie können OVFTOOL_ARGUMENTS als globale Einstellungen angeben oder Argumente einzeln auf bestimmte Knoten anwenden. Beispiel:

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  Sie können die `--powerOffTarget` Und `--overwrite` Optionen zum Herunterfahren und Ersetzen vorhandener virtueller Maschinen.

  > ⚠ Sie sollten Knoten in verschiedenen Datenspeichern bereitstellen und OVFTOOL_ARGUMENTS für jeden Knoten angeben, anstatt global.

- **QUELLE**: Der Pfad zur StorageGRID -Vorlage für virtuelle Maschinen(`.vmdk`) Datei und die `.ovf` Und `.mf` Dateien für einzelne Grid-Knoten. Standardmäßig ist dies das aktuelle Verzeichnis.

  ```
  SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
  ```

- **ZIEL**: Die URL der virtuellen VMware vSphere-Infrastruktur (vi) für den Speicherort, an dem StorageGRID bereitgestellt wird. Beispiel:

  ```
  TARGET = vi://vcenter.example.com/vm/sgws
  ```

- **GRID_NETWORK_CONFIG**: Die zum Abrufen von IP-Adressen verwendete Methode, entweder STATIC oder DHCP. Der Standardwert ist STATIC. Wenn alle oder die meisten Knoten dieselbe Methode zum Abrufen von IP-Adressen verwenden, können Sie diese Methode hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET**: Der Name eines vorhandenen VMware-Netzwerks, das für das Grid-Netzwerk verwendet werden soll. Wenn alle oder die meisten Knoten denselben Netzwerknamen verwenden, können Sie ihn hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK**: Die Netzwerkmaske für das Grid-Netzwerk. Wenn alle oder die meisten Knoten dieselbe Netzwerkmaske verwenden, können Sie diese hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY**: Das Netzwerk-Gateway für das Grid-Netzwerk. Wenn alle oder die meisten Knoten dasselbe Netzwerk-Gateway verwenden, können Sie es hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU**: Optional. Die maximale Übertragungseinheit (MTU) im Grid-Netzwerk. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Beispiel:

```
GRID_NETWORK_MTU = 9000
```

  Wenn es weggelassen wird, wird 1400 verwendet.

  Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei.

  > Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem virtuellen Switch-Port in vSphere konfiguriert ist, mit dem der Knoten verbunden ist. Andernfalls kann es zu Problemen mit der Netzwerkleistung oder zu Paketverlusten kommen.

  > Für eine optimale Netzwerkleistung sollten alle Knoten mit ähnlichen MTU-Werten auf ihren Grid-Netzwerkschnittstellen konfiguriert werden. Die Warnung **MTU-Fehlanpassung des Grid-Netzwerks** wird ausgelöst, wenn es bei den MTU-Einstellungen für das Grid-Netzwerk auf einzelnen Knoten einen signifikanten Unterschied gibt. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.

- **ADMIN_NETWORK_CONFIG**: Die zum Abrufen von IP-Adressen verwendete Methode, entweder DEAKTIVIERT, STATISCH oder DHCP. Die Standardeinstellung ist DEAKTIVIERT. Wenn alle oder die

meisten Knoten dieselbe Methode zum Abrufen von IP-Adressen verwenden, können Sie diese Methode hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET**: Der Name eines vorhandenen VMware-Netzwerks, das für das Admin-Netzwerk verwendet werden soll. Diese Einstellung ist erforderlich, sofern das Admin-Netzwerk nicht deaktiviert ist. Wenn alle oder die meisten Knoten denselben Netzwerknamen verwenden, können Sie ihn hier angeben. Anders als beim Grid-Netzwerk müssen nicht alle Knoten mit demselben Admin-Netzwerk verbunden sein. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK**: Die Netzwerkmaske für das Admin-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie eine statische IP-Adressierung verwenden. Wenn alle oder die meisten Knoten dieselbe Netzwerkmaske verwenden, können Sie diese hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY**: Das Netzwerk-Gateway für das Admin-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie eine statische IP-Adressierung verwenden und in der Einstellung ADMIN_NETWORK_ESL externe Subnetze angeben. (Das heißt, es ist nicht erforderlich, wenn ADMIN_NETWORK_ESL leer ist.) Wenn alle oder die meisten Knoten dasselbe Netzwerk-Gateway verwenden, können Sie es hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL**: Die externe Subnetzliste (Routen) für das Admin-Netzwerk, angegeben als durch Kommas getrennte Liste von CIDR-Routenzielen. Wenn alle oder die meisten Knoten dieselbe externe Subnetzliste verwenden, können Sie dies hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU**: Optional. Die maximale Übertragungseinheit (MTU) im Admin-Netzwerk. Nicht angeben, wenn ADMIN_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1400 verwendet. Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei. Wenn alle oder die meisten Knoten dieselbe MTU für das Admin-Netzwerk verwenden, können Sie sie hier angeben. Sie können die globale Einstellung dann

überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG**: Die zum Abrufen von IP-Adressen verwendete Methode, entweder DEAKTIVIERT, STATISCH oder DHCP. Die Standardeinstellung ist DEAKTIVIERT. Wenn alle oder die meisten Knoten dieselbe Methode zum Abrufen von IP-Adressen verwenden, können Sie diese Methode hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET**: Der Name eines vorhandenen VMware-Netzwerks, das für das Client-Netzwerk verwendet werden soll. Diese Einstellung ist erforderlich, sofern das Client-Netzwerk nicht deaktiviert ist. Wenn alle oder die meisten Knoten denselben Netzwerknamen verwenden, können Sie ihn hier angeben. Anders als beim Grid-Netzwerk müssen nicht alle Knoten mit demselben Client-Netzwerk verbunden sein. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK**: Die Netzwerkmaske für das Client-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie eine statische IP-Adressierung verwenden. Wenn alle oder die meisten Knoten dieselbe Netzwerkmaske verwenden, können Sie diese hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY**: Das Netzwerk-Gateway für das Client-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie eine statische IP-Adressierung verwenden. Wenn alle oder die meisten Knoten dasselbe Netzwerk-Gateway verwenden, können Sie es hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU**: Optional. Die maximale Übertragungseinheit (MTU) im Client-Netzwerk. Nicht angeben, wenn CLIENT_NETWORK_CONFIG = DHCP. Falls angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn es weggelassen wird, wird 1400 verwendet. Wenn Sie Jumbo-Frames verwenden möchten, legen Sie die MTU auf einen für Jumbo-Frames geeigneten Wert fest, beispielsweise 9000. Andernfalls behalten Sie den Standardwert bei. Wenn alle oder die meisten Knoten dieselbe MTU für das Client-Netzwerk verwenden, können Sie sie hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie für einen oder mehrere einzelne Knoten unterschiedliche Einstellungen angeben. Beispiel:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP**: Ordnet jeden Port neu zu, der von einem Knoten für die interne oder externe Kommunikation des Grid-Knotens verwendet wird. Eine Neuzuordnung der Ports ist erforderlich, wenn die Netzwerkrichtlinien des Unternehmens einen oder mehrere von StorageGRID verwendete Ports einschränken. Eine Liste der von StorageGRID verwendeten Ports finden Sie unter „Interne Grid-Knotenkommunikation“ und „Externe Kommunikation“ in"Netzwerkrichtlinien" .

  Ordnen Sie die Ports, die Sie zum Konfigurieren der Endpunkte des Lastenausgleichs verwenden möchten, nicht neu zu.

  Wenn nur PORT_REMAP festgelegt ist, wird die von Ihnen angegebene Zuordnung sowohl für eingehende als auch für ausgehende Kommunikation verwendet. Wenn auch PORT_REMAP_INBOUND angegeben ist, gilt PORT_REMAP nur für ausgehende Kommunikation.

  Das verwendete Format ist: *network type/protocol/default port used by grid node/new port* , wobei der Netzwerktyp Grid, Admin oder Client und das Protokoll TCP oder UDP ist.

  Beispiel:

```
PORT_REMAP = client/tcp/18082/443
```

  Bei alleiniger Verwendung ordnet diese Beispieleinstellung sowohl eingehende als auch ausgehende Kommunikationen für den Grid-Knoten symmetrisch von Port 18082 auf Port 443 zu. Bei Verwendung in Verbindung mit PORT_REMAP_INBOUND ordnet diese Beispieleinstellung ausgehende Kommunikationen von Port 18082 Port 443 zu.

  Sie können auch mehrere Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen.

  Beispiel:

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- **PORT_REMAP_INBOUND**: Ordnet eingehende Kommunikationen für den angegebenen Port neu zu. Wenn Sie PORT_REMAP_INBOUND angeben, aber keinen Wert für PORT_REMAP angeben, bleibt die ausgehende Kommunikation für den Port unverändert.

  Ordnen Sie die Ports, die Sie zum Konfigurieren der Endpunkte des Lastenausgleichs verwenden möchten, nicht neu zu.

  Das verwendete Format ist: *network type/protocol/_default port used by grid node/new port* , wobei der Netzwerktyp Grid, Admin oder Client und das Protokoll TCP oder UDP ist.

  Beispiel:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

In diesem Beispiel wird der an Port 443 gesendete Datenverkehr durch eine interne Firewall geleitet und an Port 18082 weitergeleitet, wo der Grid-Knoten auf S3-Anfragen wartet.

Sie können auch mehrere eingehende Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen.

Beispiel:

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **TEMPORARY_PASSWORD_TYPE**: Der Typ des temporären Installationskennworts, das beim Zugriff auf die VM-Konsole oder die StorageGRID -Installations-API oder bei Verwendung von SSH verwendet werden soll, bevor der Knoten dem Grid beitritt.

  Wenn alle oder die meisten Knoten denselben Typ eines temporären Installationskennworts verwenden, geben Sie den Typ im Abschnitt mit den globalen Parametern an. Verwenden Sie dann optional eine andere Einstellung für einen einzelnen Knoten. Wenn Sie beispielsweise global **Benutzerdefiniertes Kennwort verwenden** auswählen, können Sie **CUSTOM_TEMPORARY_PASSWORD=<Kennwort>** verwenden, um das Kennwort für jeden Knoten festzulegen.

  TEMPORARY_PASSWORD_TYPE kann einer der folgenden sein:

  - **Knotennamen verwenden**: Der Knotenname wird als temporäres Installationskennwort verwendet und bietet Zugriff auf die VM-Konsole, die StorageGRID -Installations-API und SSH.
  - **Passwort deaktivieren**: Es wird kein temporäres Installationspasswort verwendet. Wenn Sie auf die VM zugreifen müssen, um Installationsprobleme zu beheben, lesen Sie"Beheben von Installationsproblemen" .
  - **Benutzerdefiniertes Passwort verwenden**: Der mit **CUSTOM_TEMPORARY_PASSWORD=<Passwort>** angegebene Wert wird als temporäres Installationspasswort verwendet und bietet Zugriff auf die VM-Konsole, die StorageGRID -Installations -API und SSH.

    Optional können Sie den Parameter **TEMPORARY_PASSWORD_TYPE** weglassen und nur **CUSTOM_TEMPORARY_PASSWORD=<Passwort>** angeben.

- **CUSTOM_TEMPORARY_PASSWORD=<Passwort>** Optional. Das temporäre Kennwort, das während der Installation beim Zugriff auf die VM-Konsole, die StorageGRID -Installations-API und SSH verwendet werden soll. Wird ignoriert, wenn **TEMPORARY_PASSWORD_TYPE** auf **Knotennamen verwenden** oder **Passwort deaktivieren** gesetzt ist.

Knotenspezifische Parameter

Jeder Knoten befindet sich in seinem eigenen Abschnitt der Konfigurationsdatei. Jeder Knoten erfordert die folgenden Einstellungen:

- Der Abschnittskopf definiert den Knotennamen, der im Grid Manager angezeigt wird. Sie können diesen Wert überschreiben, indem Sie den optionalen NODE_NAME-Parameter für den Knoten angeben.

- **NODE_TYPE**: VM_Admin_Node, VM_Storage_Node oder VM_API_Gateway_Node
- **STORAGE_TYPE**: kombiniert, Daten oder Metadaten. Dieser optionale Parameter für Speicherknoten wird standardmäßig auf „Kombiniert (Daten und Metadaten)“ gesetzt, wenn er nicht angegeben wird. Weitere Informationen finden Sie unter "Arten von Speicherknoten" .
- **GRID_NETWORK_IP**: Die IP-Adresse für den Knoten im Grid-Netzwerk.
- **ADMIN_NETWORK_IP**: Die IP-Adresse für den Knoten im Admin-Netzwerk. Nur erforderlich, wenn der Knoten an das Admin-Netzwerk angeschlossen ist und ADMIN_NETWORK_CONFIG auf STATIC gesetzt ist.
- **CLIENT_NETWORK_IP**: Die IP-Adresse für den Knoten im Client-Netzwerk. Nur erforderlich, wenn der Knoten an das Client-Netzwerk angeschlossen ist und CLIENT_NETWORK_CONFIG für diesen Knoten auf STATIC gesetzt ist.
- **ADMIN_IP**: Die IP-Adresse für den primären Admin-Knoten im Grid-Netzwerk. Verwenden Sie den Wert, den Sie als GRID_NETWORK_IP für den primären Admin-Knoten angeben. Wenn Sie diesen Parameter weglassen, versucht der Knoten, die primäre Admin-Knoten-IP mithilfe von mDNS zu ermitteln. Weitere Informationen finden Sie unter "So erkennen Grid-Knoten den primären Admin-Knoten" .

  Der ADMIN_IP-Parameter wird für den primären Admin-Knoten ignoriert.

- Alle Parameter, die nicht global festgelegt wurden. Wenn beispielsweise ein Knoten an das Admin-Netzwerk angeschlossen ist und Sie die ADMIN_NETWORK-Parameter nicht global angegeben haben, müssen Sie sie für den Knoten angeben.

Primärer Admin-Knoten

Für den primären Admin-Knoten sind folgende zusätzliche Einstellungen erforderlich:

- **KNOTENTYP**: VM_Admin_Knoten
- **ADMIN_ROLE**: Primär

Dieser Beispieleintrag gilt für einen primären Admin-Knoten, der sich in allen drei Netzwerken befindet:

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node
  TEMPORARY_PASSWORD_TYPE = Use custom password
  CUSTOM_TEMPORARY_PASSWORD = Passw0rd

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

Die folgende zusätzliche Einstellung ist für den primären Admin-Knoten optional:

- **DISK**: Standardmäßig werden Admin-Knoten zwei zusätzliche 200-GB-Festplatten für die Prüfung und Datenbanknutzung zugewiesen. Sie können diese Einstellungen mit dem DISK-Parameter erhöhen. Beispiel:

```
DISK = INSTANCES=2, CAPACITY=300
```

Für Admin-Knoten muss INSTANCES immer gleich 2 sein.

Speicherknoten

Für Storage Nodes ist folgende zusätzliche Einstellung erforderlich:

- **KNOTENTYP**: VM_Speicherknoten

  Dieser Beispieleintrag gilt für einen Speicherknoten, der sich im Grid- und Admin-Netzwerk, aber nicht im Client-Netzwerk befindet. Dieser Knoten verwendet die ADMIN_IP-Einstellung, um die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk anzugeben.

```
[DC1-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.0.3
  ADMIN_NETWORK_IP = 10.3.0.3

  ADMIN_IP = 10.1.0.2
```

  Dieser zweite Beispieleintrag gilt für einen Speicherknoten in einem Clientnetzwerk, bei dem die Unternehmensnetzwerkrichtlinie des Kunden besagt, dass eine S3-Clientanwendung nur über Port 80 oder 443 auf den Speicherknoten zugreifen darf. Die Beispielkonfigurationsdatei verwendet PORT_REMAP, um dem Speicherknoten das Senden und Empfangen von S3-Nachrichten über Port 443 zu ermöglichen.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

  Das letzte Beispiel erstellt eine symmetrische Neuzuordnung für SSH-Verkehr von Port 22 zu Port 3022, legt die Werte jedoch explizit für eingehenden und ausgehenden Verkehr fest.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

Die folgenden zusätzlichen Einstellungen sind für Speicherknoten optional:

- **DISK**: Standardmäßig werden Speicherknoten drei 4-TB-Festplatten für die RangeDB-Nutzung zugewiesen. Sie können diese Einstellungen mit dem DISK-Parameter erhöhen. Beispiel:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE**: Standardmäßig sind alle neuen Speicherknoten so konfiguriert, dass sie sowohl Objektdaten als auch Metadaten speichern. Dies wird als *kombinierter* Speicherknoten bezeichnet. Sie können den Speicherknotentyp mit dem Parameter STORAGE_TYPE so ändern, dass nur Daten oder Metadaten gespeichert werden. Beispiel:

```
STORAGE_TYPE = data
```

Gateway-Knoten

Für Gateway-Knoten ist folgende zusätzliche Einstellung erforderlich:

- **NODE_TYPE**: VM_API_Gateway

Dieser Beispieleintrag gilt für einen Beispiel-Gateway-Knoten in allen drei Netzwerken. In diesem Beispiel wurden im globalen Abschnitt der Konfigurationsdatei keine Client-Netzwerkparameter angegeben, daher müssen sie für den Knoten angegeben werden:

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG Client Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

Nicht-primärer Admin-Knoten

Für nicht primäre Admin-Knoten sind die folgenden zusätzlichen Einstellungen erforderlich:

- **KNOTENTYP**: VM_Admin_Knoten
- **ADMIN_ROLE**: Nicht primär

Dieser Beispieleintrag gilt für einen nicht primären Admin-Knoten, der sich nicht im Client-Netzwerk befindet:

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG Grid Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

Die folgende zusätzliche Einstellung ist für nicht primäre Admin-Knoten optional:

- **DISK**: Standardmäßig werden Admin-Knoten zwei zusätzliche 200-GB-Festplatten für die Prüfung und Datenbanknutzung zugewiesen. Sie können diese Einstellungen mit dem DISK-Parameter erhöhen. Beispiel:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Für Admin-Knoten muss INSTANCES immer gleich 2 sein.

Führen Sie das Bash-Skript aus

Sie können die `deploy-vsphere-ovftool.sh` Bash-Skript und die von Ihnen geänderte Konfigurationsdatei deploy-vsphere-ovftool.ini, um die Bereitstellung von StorageGRID Knoten in VMware vSphere zu automatisieren.

Bevor Sie beginnen

Sie haben eine deploy-vsphere-ovftool.ini-Konfigurationsdatei für Ihre Umgebung erstellt.

Sie können die mit dem Bash-Skript verfügbare Hilfe verwenden, indem Sie die Hilfebefehle eingeben(`-h/ --help`). Beispiel:

```
./deploy-vsphere-ovftool.sh -h
```

oder

```
./deploy-vsphere-ovftool.sh --help
```

Schritte

1. Melden Sie sich bei dem Linux-Computer an, den Sie zum Ausführen des Bash-Skripts verwenden.
2. Wechseln Sie in das Verzeichnis, in das Sie das Installationsarchiv extrahiert haben.

   Beispiel:

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. Um alle Grid-Knoten bereitzustellen, führen Sie das Bash-Skript mit den entsprechenden Optionen für Ihre Umgebung aus.

   Beispiel:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
   vsphere-ovftool.ini
   ```

4. Wenn die Bereitstellung eines Grid-Knotens aufgrund eines Fehlers fehlgeschlagen ist, beheben Sie den Fehler und führen Sie das Bash-Skript nur für diesen Knoten erneut aus.

   Beispiel:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
   -node="DC1-S3" ./deploy-vsphere-ovftool.ini
   ```

Die Bereitstellung ist abgeschlossen, wenn der Status für jeden Knoten „Bestanden“ lautet.

```
Deployment Summary
+-----------------------------+----------+----------------------+
| node                        | attempts | status               |
+-----------------------------+----------+----------------------+
| DC1-ADM1                    |        1 | Passed               |
| DC1-G1                      |        1 | Passed               |
| DC1-S1                      |        1 | Passed               |
| DC1-S2                      |        1 | Passed               |
| DC1-S3                      |        1 | Passed               |
+-----------------------------+----------+----------------------+
```

Automatisieren Sie die Konfiguration von StorageGRID

Nach der Bereitstellung der Grid-Knoten können Sie die Konfiguration des StorageGRID Systems automatisieren.

Bevor Sie beginnen

- Den Speicherort der folgenden Dateien kennen Sie aus dem Installationsarchiv.

Dateiname	Beschreibung
configure-storagegrid.py	Python-Skript zur Automatisierung der Konfiguration
configure-storagegrid.sample.json	Beispielkonfigurationsdatei zur Verwendung mit dem Skript
configure-storagegrid.blank.json	Leere Konfigurationsdatei zur Verwendung mit dem Skript

- Sie haben eine `configure-storagegrid.json` Konfigurationsdatei. Um diese Datei zu erstellen, können Sie die Beispielkonfigurationsdatei ändern(`configure-storagegrid.sample.json`) oder die leere Konfigurationsdatei(`configure-storagegrid.blank.json`).

  Sie können die `configure-storagegrid.py` Python-Skript und das `configure-storagegrid.json` Grid-Konfigurationsdatei zur Automatisierung der Konfiguration Ihres StorageGRID -Systems.

  > Sie können das System auch mit dem Grid Manager oder der Installations-API konfigurieren.

Schritte

1. Melden Sie sich bei dem Linux-Computer an, den Sie zum Ausführen des Python-Skripts verwenden.
2. Wechseln Sie in das Verzeichnis, in das Sie das Installationsarchiv extrahiert haben.

   Beispiel:

```
cd StorageGRID-Webscale-version/platform
```

Wo `platform` ist debs, rpms oder vsphere.

3. Führen Sie das Python-Skript aus und verwenden Sie die von Ihnen erstellte Konfigurationsdatei.

   Beispiel:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Ergebnis

Ein Wiederherstellungspaket `.zip` Die Datei wird während des Konfigurationsprozesses generiert und in das Verzeichnis heruntergeladen, in dem Sie den Installations- und Konfigurationsprozess ausführen. Sie müssen die Wiederherstellungspaketdatei sichern, damit Sie das StorageGRID -System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Kopieren Sie es beispielsweise an einen sicheren, gesicherten Netzwerkspeicherort und an einen sicheren Cloud-Speicherort.

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

Wenn Sie angegeben haben, dass zufällige Passwörter generiert werden sollen, öffnen Sie das `Passwords.txt` und suchen Sie nach den Passwörtern, die für den Zugriff auf Ihr StorageGRID -System erforderlich sind.

```
######################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Ihr StorageGRID -System ist installiert und konfiguriert, wenn eine Bestätigungsmeldung angezeigt wird.

```
StorageGRID has been configured and installed.
```

Ähnliche Informationen

- "Navigieren Sie zum Grid Manager"
- "Installation der REST-API"

Bereitstellen von Grid-Knoten virtueller Maschinen (VMware)

Sammeln Sie Informationen zu Ihrer Bereitstellungsumgebung

Bevor Sie Grid-Knoten bereitstellen, müssen Sie Informationen zu Ihrer Netzwerkkonfiguration und VMware-Umgebung sammeln.

> Es ist effizienter, eine einzige Installation aller Knoten durchzuführen, als einige Knoten jetzt und einige Knoten später zu installieren.

VMware-Informationen

Sie müssen auf die Bereitstellungsumgebung zugreifen und Informationen zur VMware-Umgebung sammeln, zu den Netzwerken, die für die Grid-, Admin- und Client-Netzwerke erstellt wurden, und zu den Speichervolume-Typen, die Sie für Speicherknoten verwenden möchten.

Sie müssen Informationen zu Ihrer VMware-Umgebung sammeln, darunter Folgendes:

- Der Benutzername und das Kennwort für ein VMware vSphere-Konto, das über die entsprechenden Berechtigungen zum Abschließen der Bereitstellung verfügt.
- Host-, Datenspeicher- und Netzwerkkonfigurationsinformationen für jede virtuelle StorageGRID Knotenmaschine.

> VMware Live vMotion führt zu Zeitsprüngen bei der virtuellen Maschine und wird für Grid-Knoten jeglicher Art nicht unterstützt. Obwohl es selten vorkommt, können falsche Uhrzeiten zum Verlust von Daten oder Konfigurationsaktualisierungen führen.

Informationen zum Netz

Sie müssen Informationen über das für das StorageGRID Grid Network erstellte VMware-Netzwerk sammeln (erforderlich), darunter:

- Der Netzwerkname.
- Die zum Zuweisen von IP-Adressen verwendete Methode ist entweder statisch oder DHCP.
  - Wenn Sie statische IP-Adressen verwenden, die erforderlichen Netzwerkdetails für jeden Grid-Knoten (IP-Adresse, Gateway, Netzwerkmaske).
  - Wenn Sie DHCP verwenden, die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk. Sehen "So erkennen Grid-Knoten den primären Admin-Knoten" für weitere Informationen.

Informationen zum Admin-Netzwerk

Für Knoten, die mit dem optionalen StorageGRID Admin-Netzwerk verbunden werden, müssen Sie Informationen über das für dieses Netzwerk erstellte VMware-Netzwerk erfassen, darunter:

- Der Netzwerkname.
- Die zum Zuweisen von IP-Adressen verwendete Methode ist entweder statisch oder DHCP.
  - Wenn Sie statische IP-Adressen verwenden, die erforderlichen Netzwerkdetails für jeden Grid-Knoten (IP-Adresse, Gateway, Netzwerkmaske).
  - Wenn Sie DHCP verwenden, die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk. Sehen "So erkennen Grid-Knoten den primären Admin-Knoten" für weitere Informationen.
- Die externe Subnetzliste (ESL) für das Admin-Netzwerk.

Client-Netzwerkinformationen

Für Knoten, die mit dem optionalen StorageGRID -Clientnetzwerk verbunden werden, müssen Sie Informationen über das für dieses Netzwerk erstellte VMware-Netzwerk erfassen, darunter:

- Der Netzwerkname.
- Die zum Zuweisen von IP-Adressen verwendete Methode ist entweder statisch oder DHCP.
- Wenn Sie statische IP-Adressen verwenden, die erforderlichen Netzwerkdetails für jeden Grid-Knoten (IP-Adresse, Gateway, Netzwerkmaske).

Informationen zu zusätzlichen Schnittstellen

Sie können der VM in vCenter optional Trunk- oder Zugriffsschnittstellen hinzufügen, nachdem Sie den Knoten installiert haben. Sie möchten beispielsweise möglicherweise einem Admin- oder Gateway-Knoten eine Trunk-Schnittstelle hinzufügen, sodass Sie mithilfe von VLAN-Schnittstellen den Datenverkehr verschiedener Anwendungen oder Mandanten trennen können. Oder Sie möchten möglicherweise eine Zugriffsschnittstelle zur Verwendung in einer Hochverfügbarkeitsgruppe (HA) hinzufügen.

Die von Ihnen hinzugefügten Schnittstellen werden auf der Seite „VLAN-Schnittstellen“ und auf der Seite „HA-Gruppen“ im Grid Manager angezeigt.

- Wenn Sie eine Trunk-Schnittstelle hinzufügen, konfigurieren Sie für jede neue übergeordnete Schnittstelle eine oder mehrere VLAN-Schnittstellen. Sehen "VLAN-Schnittstellen konfigurieren" .
- Wenn Sie eine Zugriffsschnittstelle hinzufügen, müssen Sie sie direkt zu HA-Gruppen hinzufügen. Sehen "Konfigurieren von Hochverfügbarkeitsgruppen" .

Speichervolumes für virtuelle Speicherknoten

Sie müssen die folgenden Informationen für auf virtuellen Maschinen basierende Speicherknoten erfassen:

- Die Anzahl und Größe der Speichervolumes (Speicher-LUNs), die Sie hinzufügen möchten. Siehe"Speicher- und Leistungsanforderungen" .

Informationen zur Netzkonfiguration

Sie müssen Informationen sammeln, um Ihr Raster zu konfigurieren:

- Grid-Lizenz
- IP-Adressen des Network Time Protocol (NTP)-Servers
- DNS-Server-IP-Adressen

So erkennen Grid-Knoten den primären Admin-Knoten

Grid-Knoten kommunizieren zur Konfiguration und Verwaltung mit dem primären Admin-Knoten. Jeder Grid-Knoten muss die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk kennen.

Um sicherzustellen, dass ein Grid-Knoten auf den primären Admin-Knoten zugreifen kann, können Sie beim Bereitstellen des Knotens einen der folgenden Schritte ausführen:

- Sie können den Parameter ADMIN_IP verwenden, um die IP-Adresse des primären Admin-Knotens manuell einzugeben.

- Sie können den Parameter ADMIN_IP weglassen, damit der Grid-Knoten den Wert automatisch erkennt. Die automatische Erkennung ist besonders nützlich, wenn das Grid-Netzwerk DHCP verwendet, um dem primären Admin-Knoten die IP-Adresse zuzuweisen.

Die automatische Erkennung des primären Admin-Knotens erfolgt mithilfe eines Multicast-Domain-Name-Systems (mDNS). Wenn der primäre Admin-Knoten zum ersten Mal gestartet wird, veröffentlicht er seine IP-Adresse mithilfe von mDNS. Andere Knoten im selben Subnetz können dann die IP-Adresse abfragen und automatisch abrufen. Da Multicast-IP-Verkehr jedoch normalerweise nicht über Subnetze hinweg geroutet werden kann, können Knoten in anderen Subnetzen die IP-Adresse des primären Admin-Knotens nicht direkt abrufen.

Wenn Sie die automatische Erkennung verwenden:

- Sie müssen die ADMIN_IP-Einstellung für mindestens einen Grid-Knoten in allen Subnetzen einschließen, an die der primäre Admin-Knoten nicht direkt angeschlossen ist. Dieser Grid-Knoten veröffentlicht dann die IP-Adresse des primären Admin-Knotens, damit andere Knoten im Subnetz sie mit mDNS erkennen können.
- Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur die Weiterleitung von Multicast-IP-Verkehr innerhalb eines Subnetzes unterstützt.

Bereitstellen eines StorageGRID -Knotens als virtuelle Maschine

Sie verwenden den VMware vSphere Web Client, um jeden Grid-Knoten als virtuelle Maschine bereitzustellen. Während der Bereitstellung wird jeder Grid-Knoten erstellt und mit einem oder mehreren StorageGRID Netzwerken verbunden.

Wenn Sie StorageGRID -Geräte-Speicherknoten bereitstellen müssen, lesen Sie "Bereitstellen des Appliance-Speicherknotens" .

Optional können Sie Knotenports neu zuordnen oder die CPU- oder Speichereinstellungen für den Knoten erhöhen, bevor Sie ihn einschalten.

Bevor Sie beginnen

- Sie haben überprüft, wie"Planen und Vorbereiten der Installation" , und Sie verstehen die Anforderungen an Software, CPU und RAM sowie Speicher und Leistung.
- Sie sind mit VMware vSphere Hypervisor vertraut und haben Erfahrung mit der Bereitstellung virtueller Maschinen in dieser Umgebung.

Der `open-vm-tools` Das Paket, eine Open-Source-Implementierung ähnlich den VMware Tools, ist in der virtuellen StorageGRID Maschine enthalten. Sie müssen VMware Tools nicht manuell installieren.

- Sie haben die richtige Version des StorageGRID Installationsarchivs für VMware heruntergeladen und extrahiert.

Wenn Sie den neuen Knoten im Rahmen einer Erweiterungs- oder Wiederherstellungsoperation bereitstellen, müssen Sie die Version von StorageGRID verwenden, die derzeit im Grid ausgeführt wird.

- Sie verfügen über die StorageGRID Virtual Machine Disk(`.vmdk`) Datei:

```
NetApp-SG-version-SHA.vmdk
```

- Sie haben die `.ovf` Und `.mf` Dateien für jeden Grid-Knotentyp, den Sie bereitstellen:

Dateiname	Beschreibung
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Die Vorlagendatei und Manifestdatei für den primären Admin-Knoten.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Die Vorlagendatei und Manifestdatei für einen nicht primären Admin-Knoten.
vsphere-storage.ovf vsphere-storage.mf	Die Vorlagendatei und Manifestdatei für einen Speicherknoten.
vsphere-gateway.ovf vsphere-gateway.mf	Die Vorlagendatei und Manifestdatei für einen Gateway-Knoten.

- Der `.vdmk` , `.ovf` , Und `.mf` Dateien befinden sich alle im selben Verzeichnis.
- Sie haben einen Plan zur Minimierung von Fehlerdomänen. Sie sollten beispielsweise nicht alle Gateway-Knoten auf einem einzigen vSphere ESXi-Host bereitstellen.

> Führen Sie bei einer Produktionsbereitstellung nicht mehr als einen Speicherknoten auf einer einzelnen virtuellen Maschine aus. Führen Sie nicht mehrere virtuelle Maschinen auf demselben ESXi-Host aus, wenn dies zu einem inakzeptablen Fehlerdomänenproblem führen würde.

- Wenn Sie einen Knoten als Teil einer Erweiterungs- oder Wiederherstellungsoperation bereitstellen, haben Sie die"Anleitung zur Erweiterung eines StorageGRID -Systems" oder die"Wiederherstellungs- und Wartungsanweisungen" .
- Wenn Sie einen StorageGRID -Knoten als virtuelle Maschine mit zugewiesenem Speicher aus einem NetApp ONTAP System bereitstellen, haben Sie bestätigt, dass für das Volume keine FabricPool -Tiering -Richtlinie aktiviert ist. Wenn beispielsweise ein StorageGRID Knoten als virtuelle Maschine auf einem VMware-Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datenspeicher für den Knoten unterstützt, keine FabricPool -Tiering-Richtlinie aktiviert ist. Das Deaktivieren der FabricPool Tiering-Funktion für Volumes, die mit StorageGRID -Knoten verwendet werden, vereinfacht die Fehlerbehebung und Speichervorgänge.

> Verwenden Sie FabricPool niemals, um Daten im Zusammenhang mit StorageGRID zurück auf StorageGRID selbst zu verschieben. Das Zurückführen von StorageGRID -Daten in StorageGRID erhöht die Fehlerbehebung und die Betriebskomplexität.

Informationen zu diesem Vorgang

Befolgen Sie diese Anweisungen, um VMware-Knoten erstmals bereitzustellen, einen neuen VMware-Knoten in einer Erweiterung hinzuzufügen oder einen VMware-Knoten im Rahmen eines Wiederherstellungsvorgangs zu ersetzen. Sofern in den Schritten nicht anders angegeben, ist das Verfahren zur Knotenbereitstellung für alle Knotentypen, einschließlich Admin-Knoten, Speicherknoten und Gateway-Knoten, gleich.

Wenn Sie ein neues StorageGRID -System installieren:

- Sie können Knoten in beliebiger Reihenfolge bereitstellen.
- Sie müssen sicherstellen, dass jede virtuelle Maschine über das Grid-Netzwerk eine Verbindung zum primären Admin-Knoten herstellen kann.
- Sie müssen alle Grid-Knoten bereitstellen, bevor Sie das Grid konfigurieren.

Wenn Sie einen Erweiterungs- oder Wiederherstellungsvorgang durchführen:

- Sie müssen sicherstellen, dass die neue virtuelle Maschine über das Grid-Netzwerk eine Verbindung zu allen anderen Knoten herstellen kann.

Wenn Sie einen der Ports des Knotens neu zuordnen müssen, schalten Sie den neuen Knoten erst ein, wenn die Konfiguration der Portneuzuordnung abgeschlossen ist.

Schritte

1. Stellen Sie mithilfe von VCenter eine OVF-Vorlage bereit.

   Wenn Sie eine URL angeben, verweisen Sie auf einen Ordner, der die folgenden Dateien enthält. Andernfalls wählen Sie jede dieser Dateien aus einem lokalen Verzeichnis aus.

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-node.ovf
   vsphere-node.mf
   ```

   Wenn dies beispielsweise der erste Knoten ist, den Sie bereitstellen, verwenden Sie diese Dateien, um den primären Admin-Knoten für Ihr StorageGRID System bereitzustellen:

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-primary-admin.ovf
   vsphere-primary-admin.mf
   ```

2. Geben Sie einen Namen für die virtuelle Maschine ein.

   Die Standardpraxis besteht darin, für die virtuelle Maschine und den Grid-Knoten denselben Namen zu verwenden.

3. Platzieren Sie die virtuelle Maschine in der entsprechenden vApp oder im entsprechenden Ressourcenpool.
4. Wenn Sie den primären Admin-Knoten bereitstellen, lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.

   Abhängig von Ihrer vCenter-Version variiert die Reihenfolge der Schritte zum Akzeptieren der Endbenutzer-Lizenzvereinbarung, zum Angeben des Namens der virtuellen Maschine und zum Auswählen eines Datenspeichers.

5. Wählen Sie Speicher für die virtuelle Maschine aus.

   Wenn Sie einen Knoten als Teil einer Wiederherstellungsoperation bereitstellen, befolgen Sie die

Anweisungen imSchritt zur Speicherwiederherstellung um neue virtuelle Laufwerke hinzuzufügen, virtuelle Festplatten vom ausgefallenen Grid-Knoten erneut anzuschließen oder beides.

Verwenden Sie beim Bereitstellen eines Speicherknotens drei oder mehr Speichervolumes, wobei jedes Speichervolume mindestens 4 TB groß sein muss. Sie müssen dem Volume 0 mindestens 4 TB zuweisen.

> Die OVF-Datei des Speicherknotens definiert mehrere VMDKs für die Speicherung. Sofern diese VMDKs Ihren Speicheranforderungen nicht entsprechen, sollten Sie sie entfernen und vor dem Einschalten des Knotens entsprechende VMDKs oder RDMs zur Speicherung zuweisen. VMDKs werden häufiger in VMware-Umgebungen verwendet und sind einfacher zu verwalten, während RDMs möglicherweise eine bessere Leistung für Workloads bieten, die größere Objektgrößen verwenden (z. B. größer als 100 MB).

> Einige StorageGRID Installationen verwenden möglicherweise größere, aktivere Speichervolumes als typische virtualisierte Workloads. Möglicherweise müssen Sie einige Hypervisor-Parameter anpassen, wie zum Beispiel `MaxAddressableSpaceTB` , um eine optimale Leistung zu erzielen. Wenn Sie eine schlechte Leistung feststellen, wenden Sie sich an Ihren Virtualisierungs-Support, um festzustellen, ob Ihre Umgebung von einer arbeitslastspezifischen Konfigurationsoptimierung profitieren könnte.

6. Wählen Sie Netzwerke aus.

   Bestimmen Sie, welche StorageGRID -Netzwerke der Knoten verwenden wird, indem Sie für jedes Quellnetzwerk ein Zielnetzwerk auswählen.

   - Das Grid-Netzwerk ist erforderlich. Sie müssen ein Zielnetzwerk in der vSphere-Umgebung auswählen. + 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. Alle Knoten im Grid-Netzwerk müssen mit allen anderen Knoten kommunizieren können.
   - Wenn Sie das Admin-Netzwerk verwenden, wählen Sie in der vSphere-Umgebung ein anderes Zielnetzwerk aus. Wenn Sie das Admin-Netzwerk nicht verwenden, wählen Sie dasselbe Ziel aus, das Sie für das Grid-Netzwerk ausgewählt haben.
   - Wenn Sie das Client-Netzwerk verwenden, wählen Sie in der vSphere-Umgebung ein anderes Zielnetzwerk aus. Wenn Sie das Client-Netzwerk nicht verwenden, wählen Sie dasselbe Ziel aus, das Sie für das Grid-Netzwerk ausgewählt haben.
   - Wenn Sie ein Admin- oder Client-Netzwerk verwenden, müssen sich die Knoten nicht im selben Admin- oder Client-Netzwerk befinden.

7. Konfigurieren Sie für **Vorlage anpassen** die erforderlichen StorageGRID -Knoteneigenschaften.

   a. Geben Sie den **Knotennamen** ein.

      > Wenn Sie einen Grid-Knoten wiederherstellen, müssen Sie den Namen des Knotens eingeben, den Sie wiederherstellen.

   b. Verwenden Sie das Dropdown-Menü **Temporäres Installationskennwort**, um ein temporäres Installationskennwort anzugeben, damit Sie auf die VM-Konsole oder die StorageGRID -Installations -API zugreifen oder SSH verwenden können, bevor der neue Knoten dem Grid beitritt.

Das temporäre Installationskennwort wird nur während der Knoteninstallation verwendet. Nachdem ein Knoten zum Raster hinzugefügt wurde, können Sie darauf zugreifen, indem Sie"Kennwort der Knotenkonsole" , das in der `Passwords.txt` Datei im Wiederherstellungspaket.

- **Knotennamen verwenden**: Der von Ihnen für das Feld **Knotenname** angegebene Wert wird als temporäres Installationskennwort verwendet.
- **Benutzerdefiniertes Passwort verwenden**: Als temporäres Installationspasswort wird ein benutzerdefiniertes Passwort verwendet.
- **Passwort deaktivieren**: Es wird kein temporäres Installationspasswort verwendet. Wenn Sie auf die VM zugreifen müssen, um Installationsprobleme zu beheben, lesen Sie"Beheben von Installationsproblemen" .

c. Wenn Sie **Benutzerdefiniertes Kennwort verwenden** ausgewählt haben, geben Sie im Feld **Benutzerdefiniertes Kennwort** das temporäre Installationskennwort an, das Sie verwenden möchten.

d. Wählen Sie im Abschnitt **Grid-Netzwerk (eth0)** STATIC oder DHCP für die **Grid-Netzwerk-IP-Konfiguration**.

- Wenn Sie STATISCH auswählen, geben Sie die **Grid-Netzwerk-IP**, **Grid-Netzwerkmaske**, **Grid-Netzwerk-Gateway** und **Grid-Netzwerk-MTU** ein.
- Wenn Sie DHCP auswählen, werden die **Grid-Netzwerk-IP**, die **Grid-Netzwerkmaske** und das **Grid-Netzwerk-Gateway** automatisch zugewiesen.

e. Geben Sie im Feld **Primäre Admin-IP** die IP-Adresse des primären Admin-Knotens für das Grid-Netzwerk ein.

Dieser Schritt gilt nicht, wenn der Knoten, den Sie bereitstellen, der primäre Admin-Knoten ist.

Wenn Sie die IP-Adresse des primären Admin-Knotens weglassen, wird die IP-Adresse automatisch ermittelt, wenn der primäre Admin-Knoten oder mindestens ein anderer Grid-Knoten mit konfigurierter ADMIN_IP im selben Subnetz vorhanden ist. Es wird jedoch empfohlen, hier die primäre IP-Adresse des Admin-Knotens festzulegen.

a. Wählen Sie im Abschnitt **Admin-Netzwerk (eth1)** für die **IP-Konfiguration des Admin-Netzwerks** STATIC, DHCP oder DISABLED aus.

- Wenn Sie das Admin-Netzwerk nicht verwenden möchten, wählen Sie DEAKTIVIERT und geben Sie **0.0.0.0** für die Admin-Netzwerk-IP ein. Die anderen Felder können Sie leer lassen.
- Wenn Sie STATISCH auswählen, geben Sie die **Admin-Netzwerk-IP**, **Admin-Netzwerkmaske**, **Admin-Netzwerk-Gateway** und **Admin-Netzwerk-MTU** ein.
- Wenn Sie STATIC auswählen, geben Sie die **externe Subnetzliste des Admin-Netzwerks** ein. Sie müssen auch ein Gateway konfigurieren.
- Wenn Sie DHCP auswählen, werden die **Admin-Netzwerk-IP**, die **Admin-Netzwerkmaske** und das **Admin-Netzwerk-Gateway** automatisch zugewiesen.

b. Wählen Sie im Abschnitt **Client-Netzwerk (eth2)** für die **Client-Netzwerk-IP-Konfiguration** STATIC, DHCP oder DISABLED aus.

- Wenn Sie das Client-Netzwerk nicht verwenden möchten, wählen Sie DEAKTIVIERT und geben Sie **0.0.0.0** für die Client-Netzwerk-IP ein. Die anderen Felder können Sie leer lassen.
- Wenn Sie STATISCH auswählen, geben Sie die **Client-Netzwerk-IP**, **Client-Netzwerkmaske**, **Client-Netzwerk-Gateway** und **Client-Netzwerk-MTU** ein.

- Wenn Sie DHCP auswählen, werden die **Client-Netzwerk-IP**, die **Client-Netzwerkmaske** und das **Client-Netzwerk-Gateway** automatisch zugewiesen.

8. Überprüfen Sie die Konfiguration der virtuellen Maschine und nehmen Sie alle erforderlichen Änderungen vor.
9. Wenn Sie zum Abschluss bereit sind, wählen Sie **Fertig**, um den Upload der virtuellen Maschine zu starten.
10. Wenn Sie diesen Knoten als Teil eines Wiederherstellungsvorgangs bereitgestellt haben und es sich nicht um eine vollständige Knotenwiederherstellung handelt, führen Sie nach Abschluss der Bereitstellung die folgenden Schritte aus:
    a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
    b. Wählen Sie jede virtuelle Standardfestplatte aus, die für die Speicherung vorgesehen ist, und wählen Sie **Entfernen**.
    c. Fügen Sie je nach den Umständen Ihrer Datenwiederherstellung neue virtuelle Festplatten entsprechend Ihren Speicheranforderungen hinzu, schließen Sie alle virtuellen Festplatten, die vom zuvor entfernten ausgefallenen Grid-Knoten erhalten geblieben sind, erneut an oder beides.

       Beachten Sie die folgenden wichtigen Richtlinien:

       - Wenn Sie neue Festplatten hinzufügen, sollten Sie denselben Speichergerätetyp verwenden, der vor der Knotenwiederherstellung verwendet wurde.
       - Die OVF-Datei des Speicherknotens definiert mehrere VMDKs für die Speicherung. Sofern diese VMDKs Ihren Speicheranforderungen nicht entsprechen, sollten Sie sie entfernen und vor dem Einschalten des Knotens entsprechende VMDKs oder RDMs zur Speicherung zuweisen. VMDKs werden häufiger in VMware-Umgebungen verwendet und sind einfacher zu verwalten, während RDMs möglicherweise eine bessere Leistung für Workloads bieten, die größere Objektgrößen verwenden (z. B. größer als 100 MB).
11. Wenn Sie die von diesem Knoten verwendeten Ports neu zuordnen müssen, führen Sie die folgenden Schritte aus.

    Möglicherweise müssen Sie einen Port neu zuordnen, wenn die Netzwerkrichtlinien Ihres Unternehmens den Zugriff auf einen oder mehrere von StorageGRID verwendete Ports einschränken. Siehe die"Netzwerkrichtlinien" für die von StorageGRID verwendeten Ports.

    > ⓘ Ordnen Sie die in den Endpunkten des Lastenausgleichs verwendeten Ports nicht neu zu.

    a. Wählen Sie die neue VM aus.
    b. Wählen Sie auf der Registerkarte „Konfigurieren“ **Einstellungen** > **vApp-Optionen**. Der Speicherort der **vApp-Optionen** hängt von der vCenter-Version ab.
    c. Suchen Sie in der Tabelle **Eigenschaften** nach PORT_REMAP_INBOUND und PORT_REMAP.
    d. Um sowohl eingehende als auch ausgehende Kommunikation für einen Port symmetrisch zuzuordnen, wählen Sie **PORT_REMAP**.

    > ⓘ Wenn nur PORT_REMAP festgelegt ist, gilt die von Ihnen angegebene Zuordnung sowohl für eingehende als auch für ausgehende Kommunikation. Wenn auch PORT_REMAP_INBOUND angegeben ist, gilt PORT_REMAP nur für ausgehende Kommunikation.

i. Wählen Sie **Wert festlegen**.

ii. Geben Sie die Portzuordnung ein:

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

`<network type>`ist Grid, Admin oder Client und `<protocol>` ist TCP oder UDP.

Um beispielsweise den SSH-Verkehr von Port 22 auf Port 3022 umzuleiten, geben Sie Folgendes ein:

```
client/tcp/22/3022
```

Sie können mehrere Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen.

Beispiel:

```
client/tcp/18082/443, client/tcp/18083/80
```

i. Wählen Sie **OK**.

e. Um den für die eingehende Kommunikation mit dem Knoten verwendeten Port anzugeben, wählen Sie **PORT_REMAP_INBOUND**.

> Wenn Sie PORT_REMAP_INBOUND angeben und keinen Wert für PORT_REMAP angeben, bleibt die ausgehende Kommunikation für den Port unverändert.

i. Wählen Sie **Wert festlegen**.

ii. Geben Sie die Portzuordnung ein:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port
used by grid node>
```

`<network type>`ist Grid, Admin oder Client und `<protocol>` ist TCP oder UDP.

Um beispielsweise eingehenden SSH-Verkehr, der an Port 3022 gesendet wird, so neu zuzuordnen, dass er vom Grid-Knoten an Port 22 empfangen wird, geben Sie Folgendes ein:

```
client/tcp/3022/22
```

Sie können mehrere eingehende Ports mithilfe einer durch Kommas getrennten Liste neu zuordnen.

Beispiel:

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. Wählen Sie **OK**

12. Wenn Sie die CPU oder den Speicher für den Knoten gegenüber den Standardeinstellungen erhöhen möchten:

a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

b. Ändern Sie die Anzahl der CPUs oder die Speichermenge nach Bedarf.

Stellen Sie die **Speicherreservierung** auf dieselbe Größe ein wie den der virtuellen Maschine zugewiesenen **Speicher**.

c. Wählen Sie **OK**.

13. Schalten Sie die virtuelle Maschine ein.

Nach Abschluss

Wenn Sie diesen Knoten als Teil eines Erweiterungs- oder Wiederherstellungsverfahrens bereitgestellt haben, kehren Sie zu diesen Anweisungen zurück, um das Verfahren abzuschließen.

Konfigurieren Sie das Grid und schließen Sie die Installation ab (VMware)

Navigieren Sie zum Grid Manager

Mit dem Grid Manager definieren Sie alle erforderlichen Informationen zur Konfiguration Ihres StorageGRID Systems.

Bevor Sie beginnen

Der primäre Admin-Knoten muss bereitgestellt sein und die anfängliche Startsequenz abgeschlossen haben.

Schritte

1. Öffnen Sie Ihren Webbrowser und navigieren Sie zu:

   `https://primary_admin_node_ip`

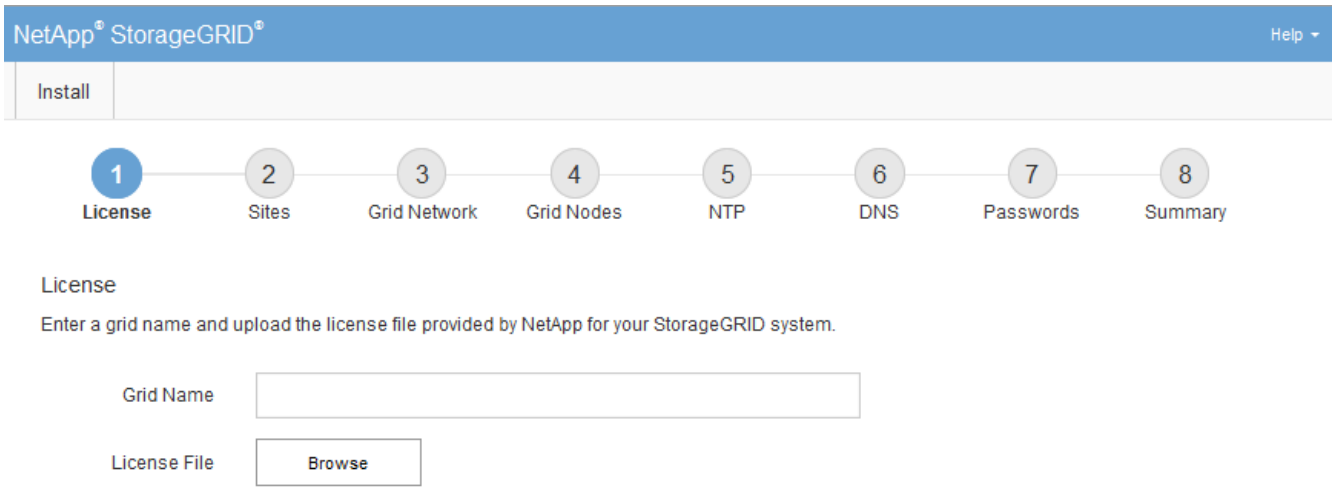
   Alternativ können Sie über Port 8443 auf den Grid Manager zugreifen:

   `https://primary_admin_node_ip:8443`

   Sie können die IP-Adresse für die primäre Admin-Knoten-IP im Grid-Netzwerk oder im Admin-Netzwerk verwenden, je nachdem, was für Ihre Netzwerkkonfiguration angemessen ist. Möglicherweise müssen Sie die Sicherheits-/Erweitert-Option in Ihrem Browser verwenden, um zu einem nicht vertrauenswürdigen Zertifikat zu navigieren.

2. Verwalten Sie bei Bedarf ein temporäres Installateurkennwort:
   - Wenn mit einer dieser Methoden bereits ein Kennwort festgelegt wurde, geben Sie das Kennwort ein, um fortzufahren.
     - Ein Benutzer hat das Kennwort beim Zugriff auf das Installationsprogramm zuvor festgelegt
     - Das SSH-/Konsolenkennwort wurde automatisch aus den OVF-Eigenschaften importiert
   - Wenn kein Kennwort festgelegt wurde, legen Sie optional ein Kennwort fest, um das StorageGRID Installationsprogramm zu sichern.
3. Wählen Sie **Installieren Sie ein StorageGRID -System**.

   Die Seite zum Konfigurieren eines StorageGRID Grids wird angezeigt.



Geben Sie die StorageGRID -Lizenzinformationen an

Sie müssen den Namen für Ihr StorageGRID -System angeben und die von NetApp bereitgestellte Lizenzdatei hochladen.

Schritte

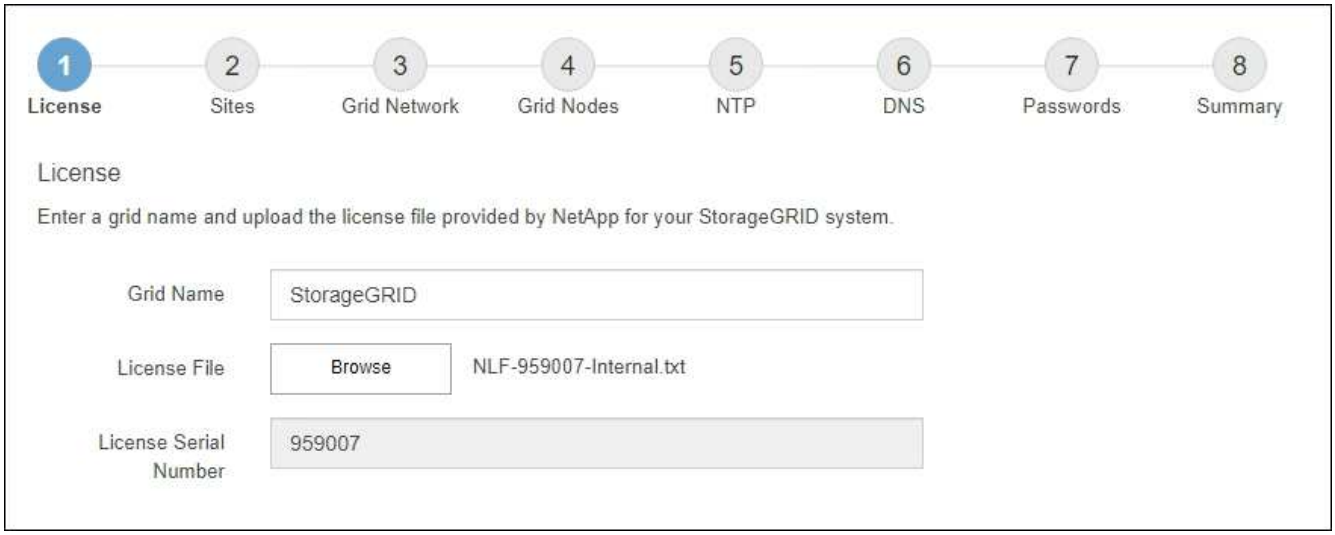
1. Geben Sie auf der Lizenzseite im Feld **Grid-Name** einen aussagekräftigen Namen für Ihr StorageGRID -System ein.

   Nach der Installation wird der Name oben im Knotenmenü angezeigt.

2. Wählen Sie **Durchsuchen**, suchen Sie die NetApp -Lizenzdatei(`NLF-unique-id.txt`) und wählen Sie **Öffnen**.

   Die Lizenzdatei wird validiert und die Seriennummer angezeigt.

   > Das StorageGRID -Installationsarchiv enthält eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet. Sie können auf eine Lizenz aktualisieren, die nach der Installation Support bietet.



3. Wählen Sie **Weiter**.

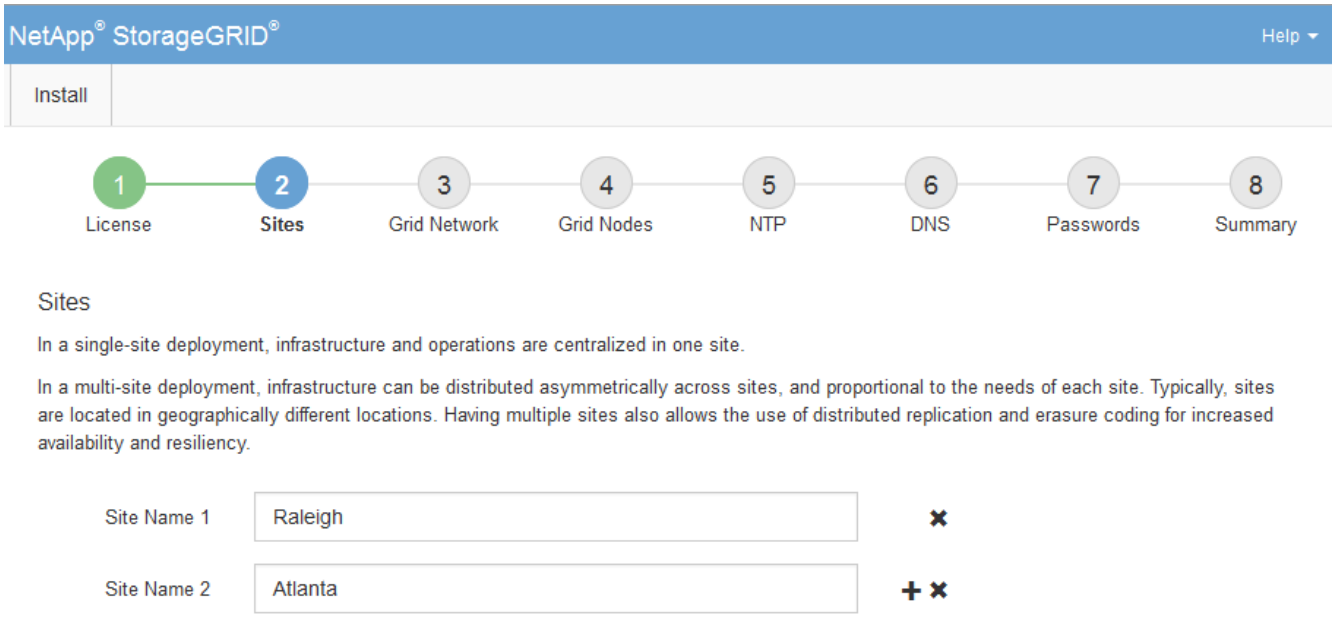
Websites hinzufügen

Sie müssen mindestens eine Site erstellen, wenn Sie StorageGRID installieren. Sie können zusätzliche Sites erstellen, um die Zuverlässigkeit und Speicherkapazität Ihres StorageGRID -Systems zu erhöhen.

Schritte

1. Geben Sie auf der Seite „Sites“ den **Site-Namen** ein.
2. Um weitere Sites hinzuzufügen, klicken Sie auf das Pluszeichen neben dem letzten Site-Eintrag und geben Sie den Namen in das neue Textfeld **Site-Name** ein.

   Fügen Sie so viele zusätzliche Sites hinzu, wie für Ihre Netztopologie erforderlich sind. Sie können bis zu 16 Sites hinzufügen.



3. Klicken Sie auf **Weiter**.

Grid-Netzwerk-Subnetze angeben

Sie müssen die Subnetze angeben, die im Grid-Netzwerk verwendet werden.

Informationen zu diesem Vorgang

Die Subnetzeinträge umfassen die Subnetze für das Grid-Netzwerk für jeden Standort in Ihrem StorageGRID -System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen.

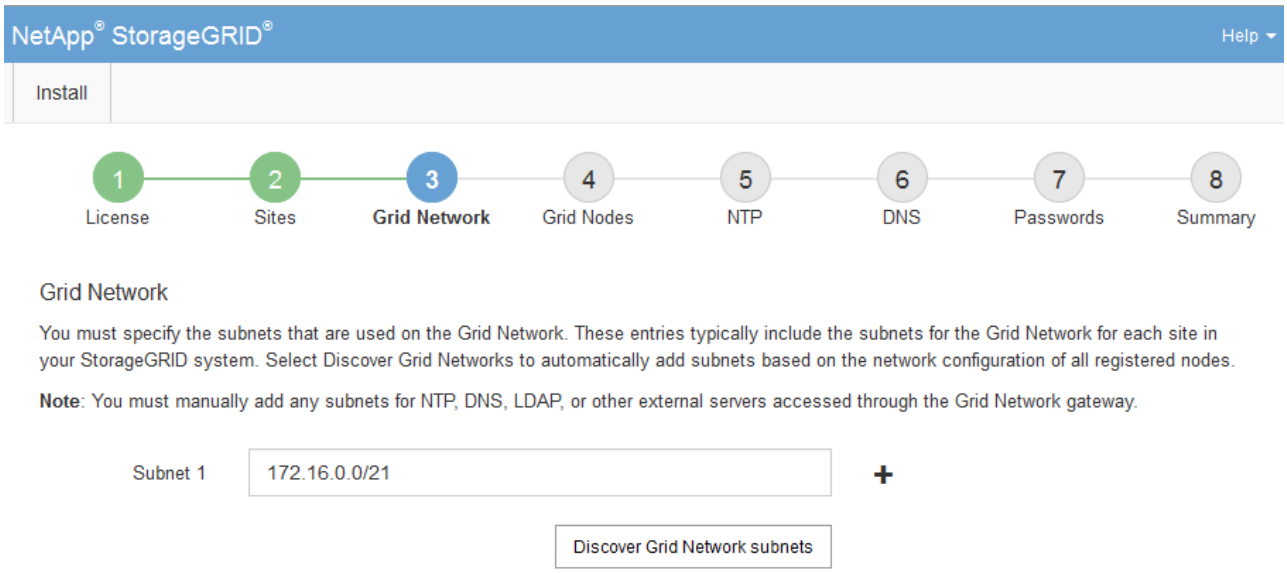
Wenn Sie über mehrere Grid-Subnetze verfügen, ist das Grid Network-Gateway erforderlich. Alle angegebenen Grid-Subnetze müssen über dieses Gateway erreichbar sein.

Schritte

1. Geben Sie die CIDR-Netzwerkadresse für mindestens ein Grid-Netzwerk im Textfeld **Subnetz 1** an.
2. Klicken Sie auf das Pluszeichen neben dem letzten Eintrag, um einen weiteren Netzwerkeintrag hinzuzufügen. Sie müssen alle Subnetze für alle Sites im Grid-Netzwerk angeben.
   - Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf **Grid-Netzwerk-Subnetze ermitteln**, um die Grid-Netzwerk-Subnetzliste automatisch mit den Subnetzen zu füllen, die

von Grid-Knoten gemeldet wurden, die beim Grid Manager registriert sind.

- Sie müssen alle Subnetze für NTP, DNS, LDAP oder andere externe Server, auf die über das Grid Network-Gateway zugegriffen wird, manuell hinzufügen.



3. Klicken Sie auf **Weiter**.

Ausstehende Rasterknoten genehmigen

Sie müssen jeden Grid-Knoten genehmigen, bevor er dem StorageGRID -System beitreten kann.

Bevor Sie beginnen

Sie haben alle virtuellen und StorageGRID -Appliance-Grid-Knoten bereitgestellt.

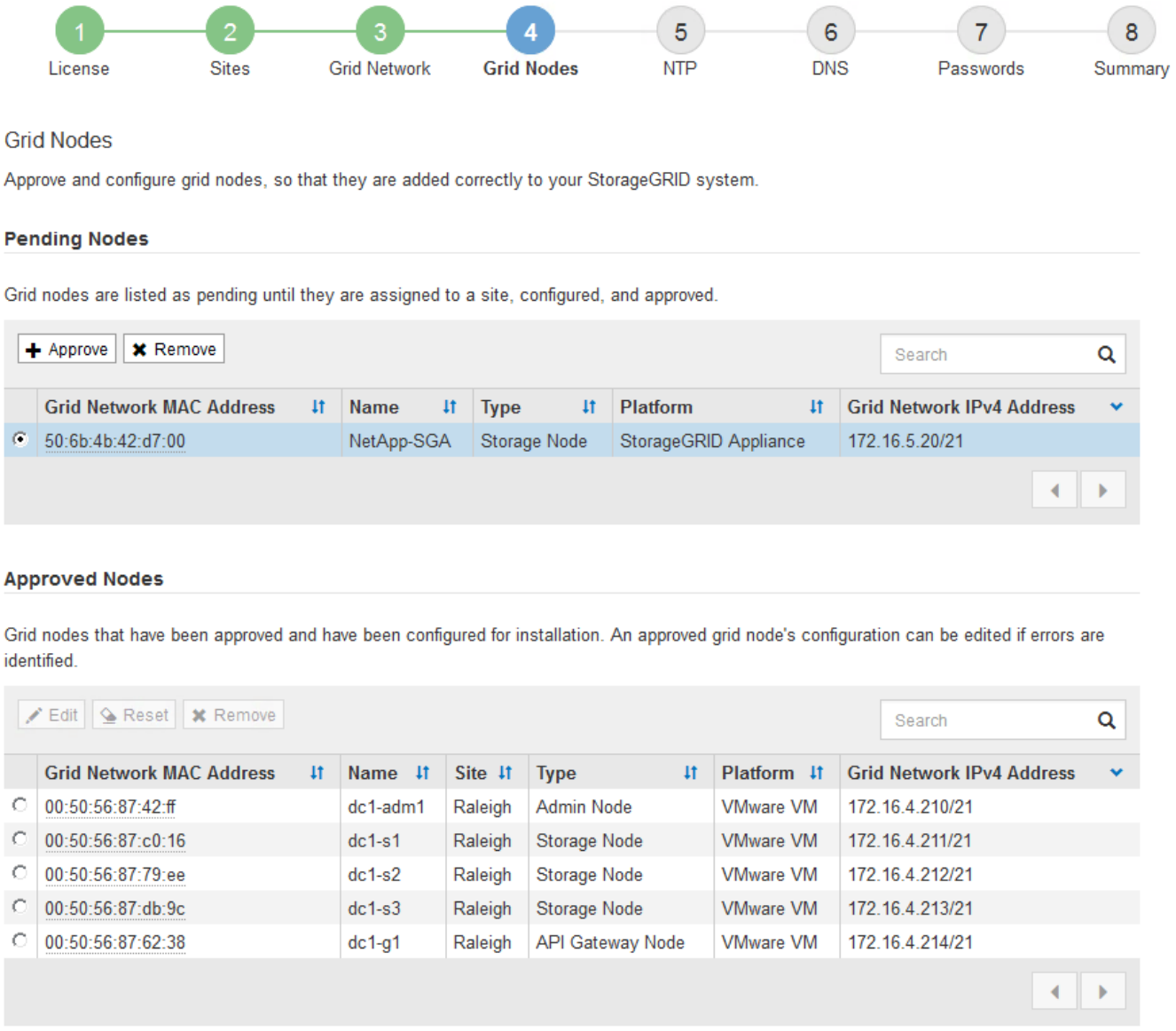
> Es ist effizienter, eine einzige Installation aller Knoten durchzuführen, als einige Knoten jetzt und einige Knoten später zu installieren.

Schritte

1. Überprüfen Sie die Liste der ausstehenden Knoten und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

> Wenn ein Grid-Knoten fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde und die richtige Grid-Netzwerk-IP des primären Admin-Knotens für ADMIN_IP festgelegt ist.

2. Wählen Sie das Optionsfeld neben einem ausstehenden Knoten aus, den Sie genehmigen möchten.



3. Klicken Sie auf **Genehmigen**.
4. Ändern Sie unter „Allgemeine Einstellungen“ nach Bedarf die Einstellungen für die folgenden Eigenschaften:

   - **Site**: Der Systemname der Site für diesen Grid-Knoten.
   - **Name**: Der Systemname für den Knoten. Der Name ist standardmäßig der Name, den Sie bei der Konfiguration des Knotens angegeben haben.

     Systemnamen sind für interne StorageGRID -Vorgänge erforderlich und können nach Abschluss der Installation nicht mehr geändert werden. Während dieses Schritts des Installationsvorgangs können Sie die Systemnamen jedoch nach Bedarf ändern.

     Bei einem VMware-Knoten können Sie hier den Namen ändern, diese Aktion ändert jedoch nicht den Namen der virtuellen Maschine in vSphere.

   - **NTP-Rolle**: Die Network Time Protocol (NTP)-Rolle des Grid-Knotens. Die Optionen sind **Automatisch**, **Primär** und **Client**. Wenn Sie „**Automatisch**“ auswählen, wird die primäre Rolle den Admin-Knoten, Speicherknoten mit ADC-Diensten, Gateway-Knoten und allen Grid-Knoten mit nicht

statischen IP-Adressen zugewiesen. Allen anderen Grid-Knoten wird die Client-Rolle zugewiesen.

> Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.

- **Speichertyp** (nur Speicherknoten): Geben Sie an, dass ein neuer Speicherknoten ausschließlich für Daten, nur für Metadaten oder für beides verwendet werden soll. Die Optionen sind **Daten und Metadaten** („kombiniert“), **Nur Daten** und **Nur Metadaten**.

  > Sehen"Arten von Speicherknoten" Informationen zu den Anforderungen für diese Knotentypen finden Sie unter.

- **ADC-Dienst** (nur Speicherknoten): Wählen Sie **Automatisch**, damit das System ermittelt, ob der Knoten den Administrative Domain Controller (ADC)-Dienst benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Diensten. Mindestens drei Speicherknoten an jedem Standort müssen den ADC-Dienst enthalten. Sie können den ADC-Dienst nach der Bereitstellung nicht mehr zu einem Knoten hinzufügen.

5. Ändern Sie im Grid-Netzwerk nach Bedarf die Einstellungen für die folgenden Eigenschaften:

   - **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Grid-Netzwerkschnittstelle (eth0 innerhalb des Containers). Beispiel: 192.168.1.234/21
   - **Gateway**: Das Grid-Netzwerk-Gateway. Beispiel: 192.168.0.1

     > Das Gateway wird benötigt, wenn mehrere Grid-Subnetze vorhanden sind.

   > Wenn Sie DHCP für die Grid-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

6. Wenn Sie das Admin-Netzwerk für den Grid-Knoten konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt „Admin-Netzwerk“ nach Bedarf hinzu oder aktualisieren Sie sie.

   Geben Sie die Zielsubnetze der Routen aus dieser Schnittstelle in das Textfeld **Subnetze (CIDR)** ein. Wenn mehrere Admin-Subnetze vorhanden sind, ist das Admin-Gateway erforderlich.

   > Wenn Sie DHCP für die Admin-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

   Geräte: Wenn das Admin-Netzwerk für ein StorageGRID -Gerät während der Erstinstallation mit dem StorageGRID Appliance Installer nicht konfiguriert wurde, kann es in diesem Grid Manager-Dialogfeld nicht konfiguriert werden. Stattdessen müssen Sie die folgenden Schritte ausführen:

   a. Starten Sie das Gerät neu: Wählen Sie im Geräteinstallationsprogramm **Erweitert** > **Neustart**.

      Der Neustart kann mehrere Minuten dauern.

b. Wählen Sie **Netzwerk konfigurieren** > **Linkkonfiguration** und aktivieren Sie die entsprechenden Netzwerke.

c. Wählen Sie **Netzwerk konfigurieren** > **IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.

d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

e. Im Grid Manager: Wenn der Knoten in der Tabelle „Genehmigte Knoten“ aufgeführt ist, entfernen Sie den Knoten.

f. Entfernen Sie den Knoten aus der Tabelle „Ausstehende Knoten“.

g. Warten Sie, bis der Knoten wieder in der Liste „Ausstehende Knoten“ angezeigt wird.

h. Bestätigen Sie, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt sein, die Sie auf der IP-Konfigurationsseite des Appliance-Installationsprogramms angegeben haben.

   Weitere Informationen finden Sie im "Schnellstart für die Hardwareinstallation" um Anweisungen für Ihr Gerät zu finden.

7. Wenn Sie das Client-Netzwerk für den Grid-Knoten konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt „Client-Netzwerk“ nach Bedarf hinzu oder aktualisieren Sie sie. Wenn das Client-Netzwerk konfiguriert ist, ist das Gateway erforderlich und wird nach der Installation zum Standard-Gateway für den Knoten.

   > ⓘ Wenn Sie DHCP für die Client-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die konfigurierte IP-Adresse nicht in einem DHCP-Adresspool befindet.

   Geräte: Wenn das Client-Netzwerk eines StorageGRID Geräts während der Erstinstallation mit dem StorageGRID -Geräteinstallationsprogramm nicht konfiguriert wurde, kann es in diesem Grid Manager-Dialogfeld nicht konfiguriert werden. Stattdessen müssen Sie die folgenden Schritte ausführen:

   a. Starten Sie das Gerät neu: Wählen Sie im Geräteinstallationsprogramm **Erweitert** > **Neustart**.

      Der Neustart kann mehrere Minuten dauern.

   b. Wählen Sie **Netzwerk konfigurieren** > **Linkkonfiguration** und aktivieren Sie die entsprechenden Netzwerke.

   c. Wählen Sie **Netzwerk konfigurieren** > **IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.

   d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

   e. Im Grid Manager: Wenn der Knoten in der Tabelle „Genehmigte Knoten“ aufgeführt ist, entfernen Sie den Knoten.

   f. Entfernen Sie den Knoten aus der Tabelle „Ausstehende Knoten“.

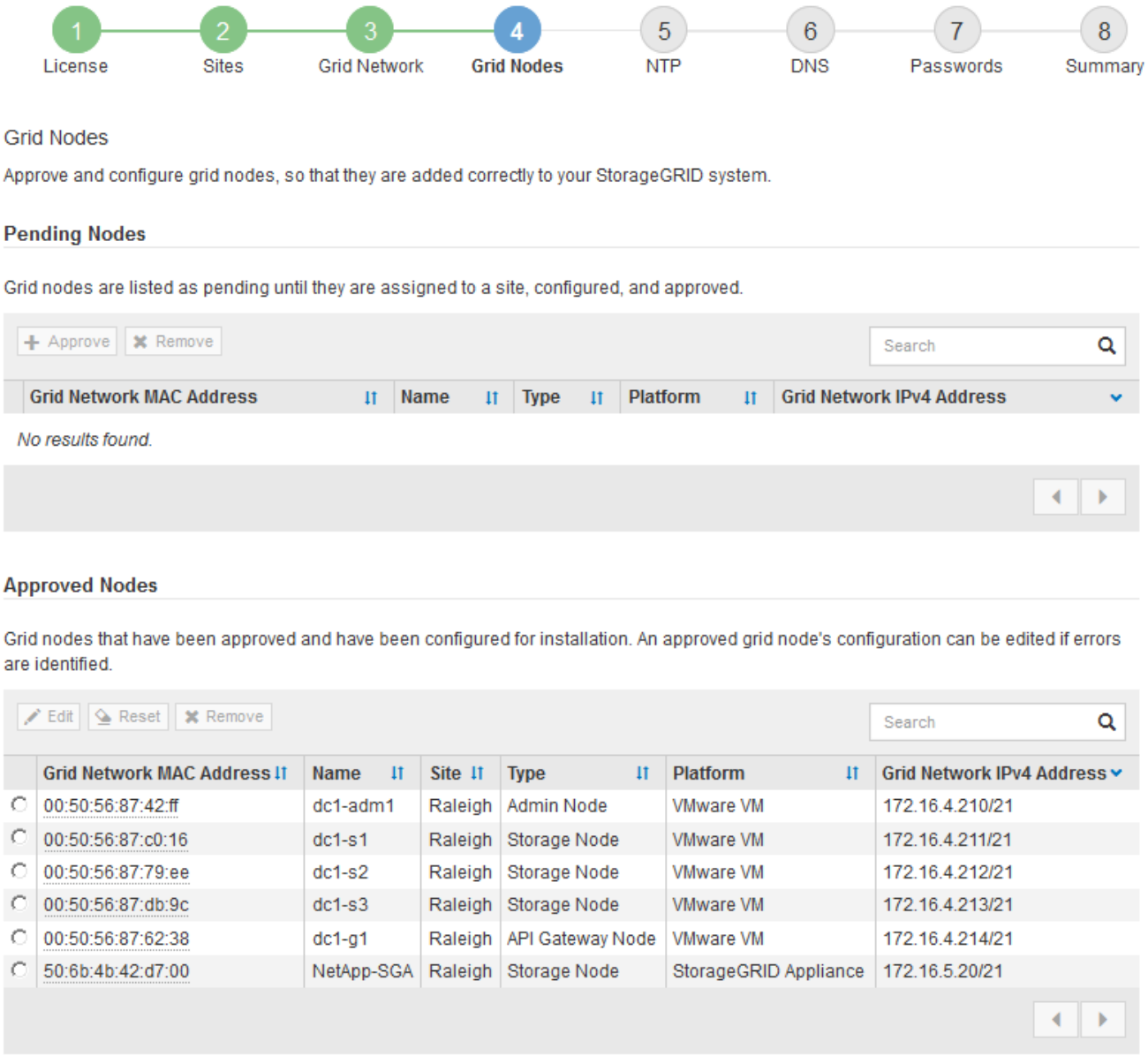
   g. Warten Sie, bis der Knoten wieder in der Liste „Ausstehende Knoten“ angezeigt wird.

   h. Bestätigen Sie, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt sein, die Sie auf der IP-Konfigurationsseite des Appliance-Installationsprogramms angegeben haben.

      Weitere Informationen finden Sie im "Schnellstart für die Hardwareinstallation" um Anweisungen für Ihr Gerät zu finden.

8. Klicken Sie auf **Speichern**.

   Der Rasterknoteneintrag wird in die Liste „Genehmigte Knoten“ verschoben.



9. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

   Sie müssen alle Knoten genehmigen, die Sie im Raster haben möchten. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Zusammenfassungsseite auf **Installieren** klicken. Sie können die Eigenschaften eines genehmigten Rasterknotens ändern, indem Sie dessen Optionsfeld auswählen und auf **Bearbeiten** klicken.

10. Wenn Sie mit der Genehmigung der Rasterknoten fertig sind, klicken Sie auf **Weiter**.

Geben Sie die Serverinformationen des Network Time Protocol an

Sie müssen die Network Time Protocol (NTP)-Konfigurationsinformationen für das StorageGRID -System angeben, damit die auf separaten Servern ausgeführten Vorgänge synchronisiert bleiben können.

Informationen zu diesem Vorgang

Sie müssen IPv4-Adressen für die NTP-Server angeben.

Sie müssen externe NTP-Server angeben. Die angegebenen NTP-Server müssen das NTP-Protokoll verwenden.

Sie müssen vier NTP-Serverreferenzen von Stratum 3 oder besser angeben, um Probleme mit Zeitabweichungen zu vermeiden.

> Wenn Sie die externe NTP-Quelle für eine StorageGRID Installation auf Produktionsebene angeben, verwenden Sie den Windows-Zeitdienst (W32Time) nicht auf einer Windows-Version vor Windows Server 2016. Der Zeitdienst früherer Windows-Versionen ist nicht genau genug und wird von Microsoft für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, nicht unterstützt.

"Supportgrenze zum Konfigurieren des Windows-Zeitdienstes für Umgebungen mit hoher Genauigkeit"

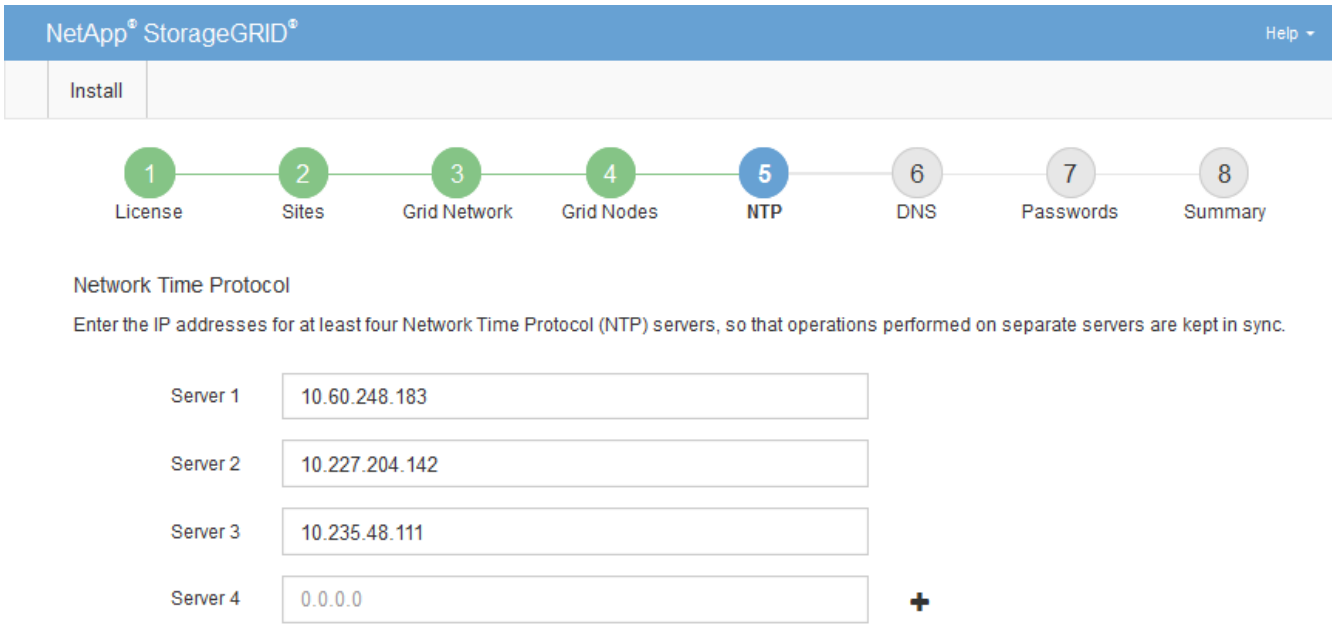
Die externen NTP-Server werden von den Knoten verwendet, denen Sie zuvor primäre NTP-Rollen zugewiesen haben.

> Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.

Führen Sie zusätzliche Prüfungen für VMware durch, z. B. stellen Sie sicher, dass der Hypervisor dieselbe NTP-Quelle wie die virtuelle Maschine verwendet, und deaktivieren Sie mithilfe von VMTools die Zeitsynchronisierung zwischen dem Hypervisor und den virtuellen StorageGRID Maschinen.

Schritte

1. Geben Sie die IPv4-Adressen für mindestens vier NTP-Server in den Textfeldern **Server 1** bis **Server 4** an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um weitere Servereinträge hinzuzufügen.



3. Wählen Sie **Weiter**.

DNS-Serverinformationen angeben

Sie müssen DNS-Informationen für Ihr StorageGRID -System angeben, damit Sie auf externe Server über Hostnamen statt über IP-Adressen zugreifen können.

Informationen zu diesem Vorgang

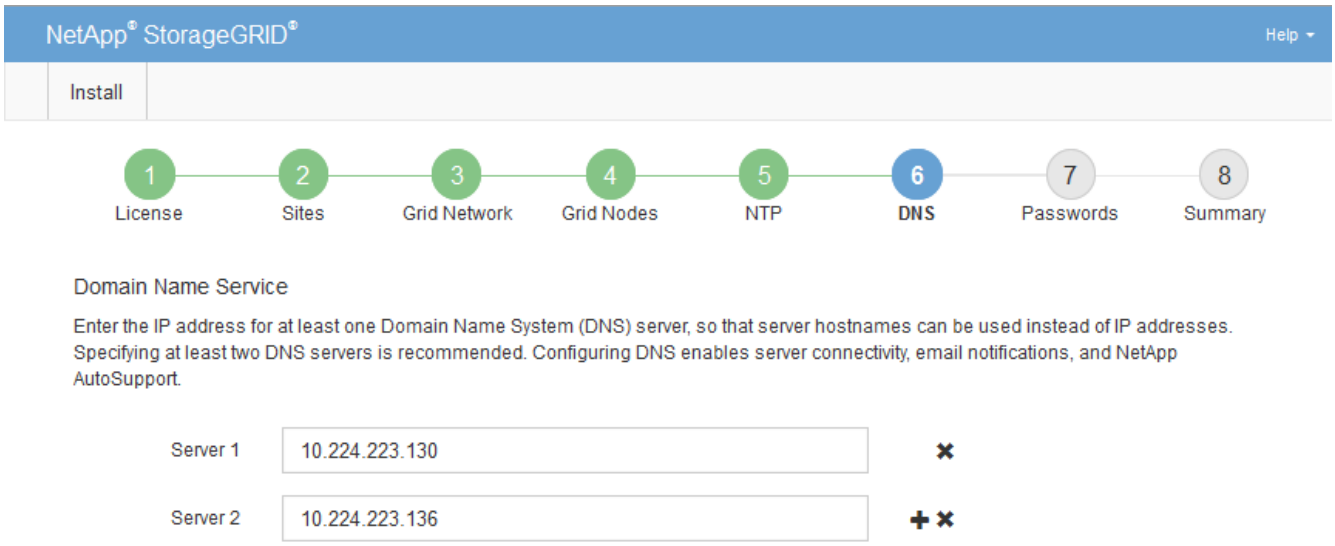
Festlegen "DNS-Serverinformationen" ermöglicht Ihnen die Verwendung von Fully Qualified Domain Name (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport.

Um einen ordnungsgemäßen Betrieb sicherzustellen, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, ist es möglich, dass aufgrund bekannter Betriebssystembeschränkungen auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie"Passen Sie die DNS-Serverliste an" für einzelne Knoten (normalerweise alle Knoten an einem Standort), einen anderen Satz von bis zu drei DNS-Servern zu verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein isolierter Standort die FQDNs für externe Ziele auflösen kann.

Schritte

1. Geben Sie im Textfeld **Server 1** die IPv4-Adresse für mindestens einen DNS-Server an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um weitere Servereinträge hinzuzufügen.



Die beste Vorgehensweise besteht darin, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Geben Sie die StorageGRID -Systemkennwörter an

Im Rahmen der Installation Ihres StorageGRID -Systems müssen Sie die Passwörter eingeben, mit denen Sie Ihr System sichern und Wartungsaufgaben durchführen können.

Informationen zu diesem Vorgang

Verwenden Sie die Seite „Passwörter installieren“, um die Bereitstellungspassphrase und das Root-Benutzerpasswort für die Grid-Verwaltung anzugeben.

- Die Bereitstellungspassphrase wird als Verschlüsselungsschlüssel verwendet und nicht vom StorageGRID -System gespeichert.
- Sie müssen über die Bereitstellungspassphrase für Installations-, Erweiterungs- und Wartungsvorgänge verfügen, einschließlich des Herunterladens des Wiederherstellungspakets. Daher ist es wichtig, dass Sie die Bereitstellungspassphrase an einem sicheren Ort speichern.
- Sie können die Bereitstellungspassphrase im Grid Manager ändern, wenn Sie die aktuelle haben.
- Das Root-Benutzerkennwort für die Grid-Verwaltung kann mithilfe des Grid-Managers geändert werden.
- Zufällig generierte Befehlszeilenkonsolen- und SSH-Passwörter werden im `Passwords.txt` Datei im Wiederherstellungspaket.

Schritte

1. Geben Sie unter **Bereitstellungspassphrase** die Bereitstellungspassphrase ein, die zum Vornehmen von Änderungen an der Grid-Topologie Ihres StorageGRID Systems erforderlich ist.

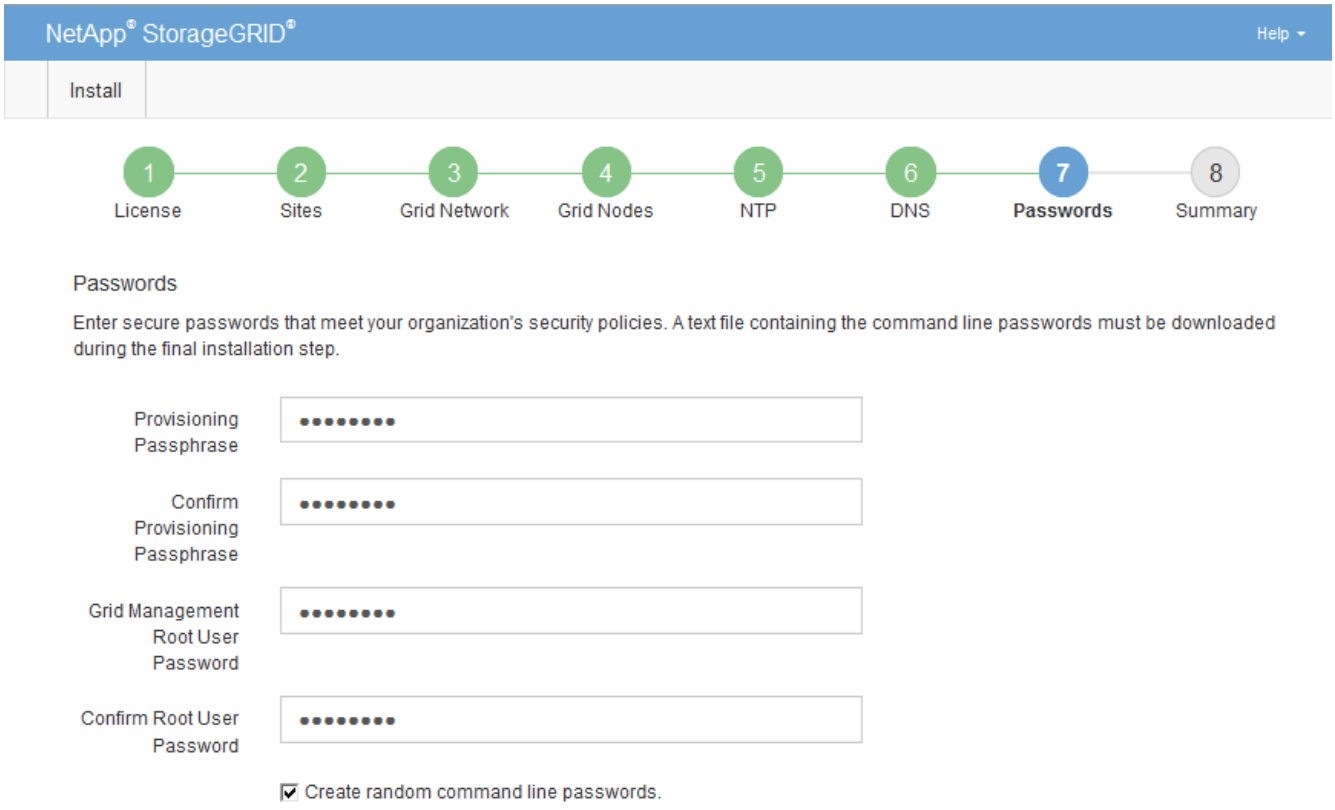
   Bewahren Sie die Bereitstellungspassphrase an einem sicheren Ort auf.

   > Wenn Sie nach Abschluss der Installation die Bereitstellungspassphrase später ändern möchten, können Sie den Grid Manager verwenden. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Grid-Passwörter**.

2. Geben Sie unter **Bereitstellungspassphrase bestätigen** die Bereitstellungspassphrase erneut ein, um sie zu bestätigen.
3. Geben Sie unter **Grid Management Root User Password** das Passwort ein, das Sie für den Zugriff auf den Grid Manager als „Root“-Benutzer verwenden möchten.

   Bewahren Sie das Passwort an einem sicheren Ort auf.

4. Geben Sie unter **Root-Benutzerkennwort bestätigen** das Grid Manager-Kennwort erneut ein, um es zu bestätigen.



5. Wenn Sie ein Grid zu Proof-of-Concept- oder Demozwecken installieren, deaktivieren Sie optional das Kontrollkästchen **Zufällige Befehlszeilenkennwörter erstellen**.

   Bei Produktionsbereitstellungen sollten aus Sicherheitsgründen immer zufällige Passwörter verwendet werden. Deaktivieren Sie **Zufällige Befehlszeilenkennwörter erstellen** nur für Demo-Raster, wenn Sie Standardkennwörter verwenden möchten, um über die Befehlszeile mit dem Konto „root“ oder „admin“ auf Rasterknoten zuzugreifen.

   > Sie werden aufgefordert, die Wiederherstellungspaketdatei herunterzuladen(`sgws-recovery-package-id-revision.zip`), nachdem Sie auf der Seite „Zusammenfassung“ auf **Installieren** geklickt haben. Sie müssen"Laden Sie diese Datei herunter" um die Installation abzuschließen. Die für den Zugriff auf das System erforderlichen Passwörter sind im `Passwords.txt` Datei, die in der Wiederherstellungspaketdatei enthalten ist.

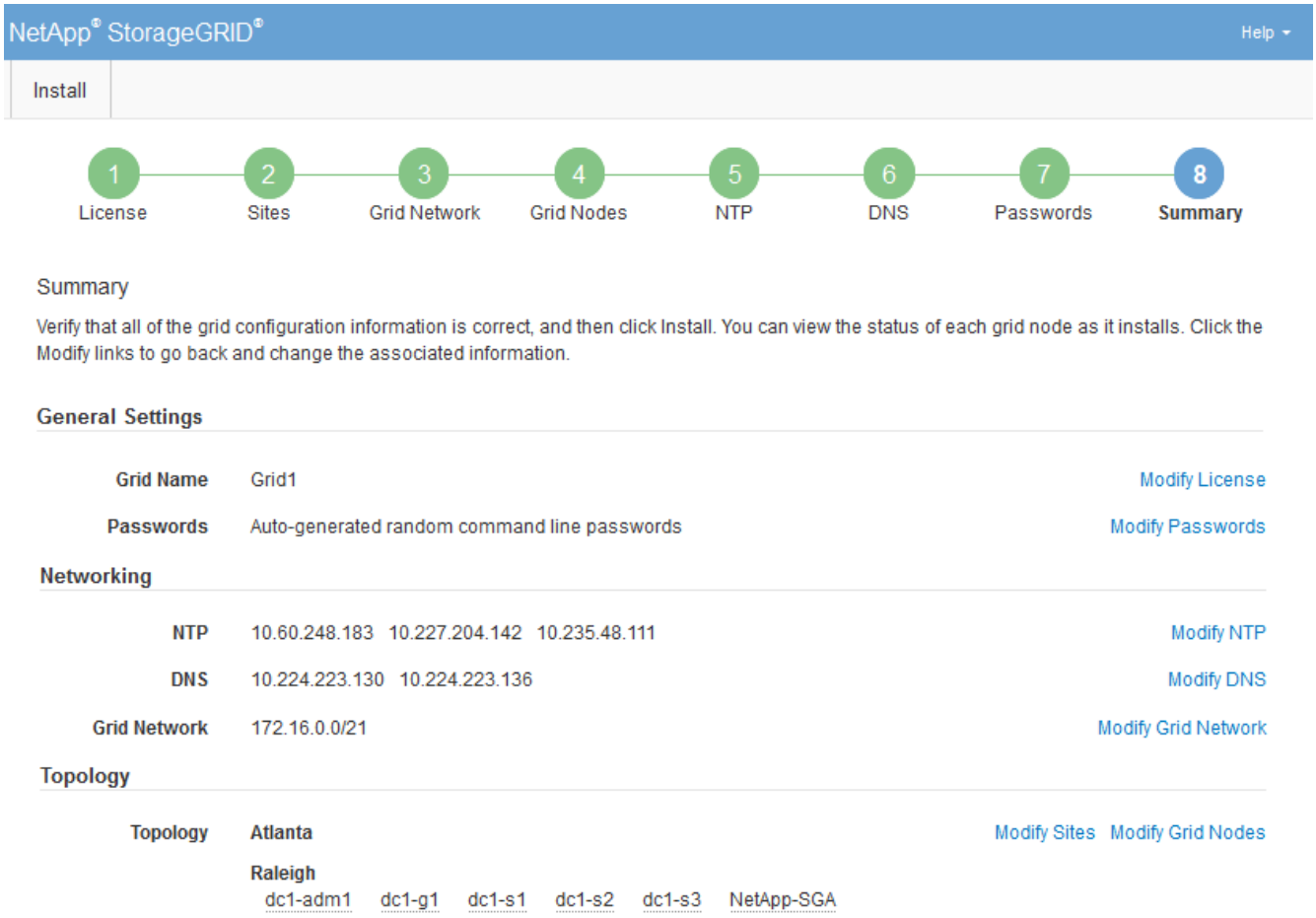
6. Klicken Sie auf **Weiter**.

Überprüfen Sie Ihre Konfiguration und schließen Sie die Installation ab

Sie müssen die eingegebenen Konfigurationsinformationen sorgfältig prüfen, um sicherzustellen, dass die Installation erfolgreich abgeschlossen wird.

Schritte

1. Sehen Sie sich die Seite **Zusammenfassung** an.



2. Überprüfen Sie, ob alle Informationen zur Netzkonfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite „Zusammenfassung“, um zurückzugehen und etwaige Fehler zu korrigieren.
3. Klicken Sie auf **Installieren**.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf **Installieren** klicken. Wenn die Verbindung verloren geht, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Knoten zugreifen. Sehen"Netzwerkrichtlinien" für Details.

4. Klicken Sie auf **Wiederherstellungspaket herunterladen**.

   Wenn die Installation bis zu dem Punkt fortschreitet, an dem die Grid-Topologie definiert ist, werden Sie aufgefordert, die Datei Recovery Package herunterzuladen(`.zip`) und bestätigen Sie, dass Sie erfolgreich auf den Inhalt dieser Datei zugreifen können. Sie müssen die Wiederherstellungspaketdatei herunterladen, damit Sie das StorageGRID -System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Die Installation wird im Hintergrund fortgesetzt, Sie können die Installation jedoch erst

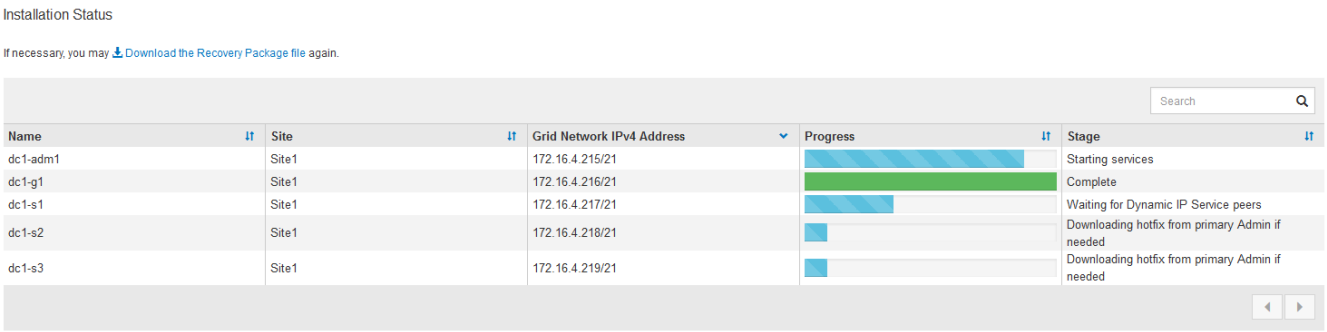
abschließen und auf das StorageGRID -System zugreifen, wenn Sie diese Datei heruntergeladen und überprüft haben.

5. Überprüfen Sie, ob Sie den Inhalt der `.zip` Datei und speichern Sie sie dann an zwei sicheren und getrennten Orten.

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

6. Aktivieren Sie das Kontrollkästchen **Ich habe die Wiederherstellungspaketdatei erfolgreich heruntergeladen und überprüft** und klicken Sie auf **Weiter**.

   Wenn die Installation noch läuft, wird die Statusseite angezeigt. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



   Wenn für alle Grid-Knoten die Phase „Abgeschlossen“ erreicht ist, wird die Anmeldeseite für den Grid Manager angezeigt.

7. Sign in beim Grid Manager mit dem Benutzer „root“ und dem Kennwort an, das Sie während der Installation angegeben haben.

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Bereitstellung und Konfiguration des Grid-Knotens diese Richtlinien für DHCP-Adressierung und Netzwerkkonfigurationsänderungen.

- Wenn DHCP zum Zuweisen von IP-Adressen verwendet wurde, konfigurieren Sie eine DHCP-Reservierung für jede IP-Adresse in den verwendeten Netzwerken.

  Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten.

> Knoten werden neu gestartet, wenn die Grid-Netzwerkkonfiguration per DHCP geändert wird. Dies kann zu Ausfällen führen, wenn eine DHCP-Änderung mehrere Knoten gleichzeitig betrifft.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmasken und Standard-Gateways für einen Grid-Knoten ändern möchten. Sehen "Konfigurieren von IP-Adressen" .
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin-Knoten und anderen Grid-Knoten verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen

möglicherweise erneut herstellen.

Installation der REST-API

StorageGRID bietet die StorageGRID -Installations-API zum Ausführen von Installationsaufgaben.

Die API verwendet die Open-Source-API-Plattform Swagger, um die API-Dokumentation bereitzustellen. Swagger ermöglicht sowohl Entwicklern als auch Nicht-Entwicklern die Interaktion mit der API in einer Benutzeroberfläche, die veranschaulicht, wie die API auf Parameter und Optionen reagiert. Diese Dokumentation setzt voraus, dass Sie mit Standard-Webtechnologien und dem JSON-Datenformat vertraut sind.

> 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.

Jeder REST-API-Befehl enthält die URL der API, eine HTTP-Aktion, alle erforderlichen oder optionalen URL-Parameter und eine erwartete API-Antwort.

StorageGRID Installations-API

Die StorageGRID Installations-API ist nur verfügbar, wenn Sie Ihr StorageGRID -System zum ersten Mal konfigurieren und eine Wiederherstellung des primären Admin-Knotens durchführen müssen. Auf die Installations-API kann über HTTPS vom Grid Manager aus zugegriffen werden.

Um auf die API-Dokumentation zuzugreifen, gehen Sie zur Installationswebseite auf dem primären Admin-Knoten und wählen Sie in der Menüleiste **Hilfe** > **API-Dokumentation**.

Die StorageGRID -Installations-API umfasst die folgenden Abschnitte:

- **config** – Vorgänge im Zusammenhang mit der Produktversion und den Versionen der API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **grid** – Konfigurationsvorgänge auf Grid-Ebene. Sie können Grid-Einstellungen abrufen und aktualisieren, einschließlich Grid-Details, Grid-Netzwerk-Subnetze, Grid-Passwörter sowie NTP- und DNS-Server-IP-Adressen.
- **Knoten** – Konfigurationsvorgänge auf Knotenebene. Sie können eine Liste von Grid-Knoten abrufen, einen Grid-Knoten löschen, einen Grid-Knoten konfigurieren, einen Grid-Knoten anzeigen und die Konfiguration eines Grid-Knotens zurücksetzen.
- **Bereitstellung** – Bereitstellungsvorgänge. Sie können den Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** – Wiederherstellungsvorgänge für den primären Admin-Knoten. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **recovery-package** – Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **Sites** – Konfigurationsvorgänge auf Site-Ebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.
- **temporäres Passwort** – Vorgänge für das temporäre Passwort, um die Mgmt-API während der Installation zu sichern.

Wohin als nächstes?

Führen Sie nach Abschluss einer Installation die erforderlichen Integrations- und Konfigurationsaufgaben durch. Sie können die optionalen Aufgaben nach Bedarf ausführen.

Erforderliche Aufgaben

- Konfigurieren Sie VMware vSphere Hypervisor für den automatischen Neustart.

  Sie müssen den Hypervisor so konfigurieren, dass die virtuellen Maschinen beim Neustart des Servers neu gestartet werden. Ohne einen automatischen Neustart bleiben die virtuellen Maschinen und Grid-Knoten nach dem Neustart des Servers heruntergefahren. Weitere Informationen finden Sie in der VMware vSphere Hypervisor-Dokumentation.

- "Erstellen Sie ein Mieterkonto"für das S3-Clientprotokoll, das zum Speichern von Objekten auf Ihrem StorageGRID System verwendet wird.
- "Kontrollsystemzugriff"durch Konfigurieren von Gruppen und Benutzerkonten. Optional können Sie"Konfigurieren einer föderierten Identitätsquelle" (wie Active Directory oder OpenLDAP), sodass Sie Administrationsgruppen und Benutzer importieren können. Oder Sie können"Erstellen Sie lokale Gruppen und Benutzer" .
- Integrieren und testen Sie die"S3 API" Clientanwendungen, die Sie zum Hochladen von Objekten in Ihr StorageGRID System verwenden.
- "Konfigurieren der Regeln und Richtlinien für das Information Lifecycle Management (ILM)"Sie zum Schutz der Objektdaten verwenden möchten.
- Wenn Ihre Installation Appliance-Speicherknoten umfasst, verwenden Sie SANtricity OS, um die folgenden Aufgaben auszuführen:
  - Stellen Sie eine Verbindung zu jedem StorageGRID Gerät her.
  - Überprüfen Sie den Erhalt der AutoSupport -Daten.

    Sehen "Hardware einrichten" .

- Überprüfen und befolgen Sie die"Richtlinien zur Systemhärtung von StorageGRID" um Sicherheitsrisiken auszuschließen.
- "Konfigurieren Sie E-Mail-Benachrichtigungen für Systemwarnungen" .

Optionale Aufgaben

- "Aktualisieren Sie die IP-Adressen der Grid-Knoten"ob sie sich seit der Planung Ihrer Bereitstellung und der Generierung des Wiederherstellungspakets geändert haben.
- "Konfigurieren der Speicherverschlüsselung", falls erforderlich.
- "Konfigurieren der Speicherkomprimierung"um die Größe gespeicherter Objekte bei Bedarf zu reduzieren.
- "Konfigurieren von VLAN-Schnittstellen"um den Netzwerkverkehr bei Bedarf zu isolieren und zu partitionieren.
- "Konfigurieren von Hochverfügbarkeitsgruppen"um bei Bedarf die Verbindungsverfügbarkeit für Grid Manager, Tenant Manager und S3-Clients zu verbessern.
- "Konfigurieren von Load Balancer-Endpunkten"für S3-Client-Konnektivität, falls erforderlich.

Beheben von Installationsproblemen

Wenn bei der Installation Ihres StorageGRID -Systems Probleme auftreten, können Sie auf die Installationsprotokolldateien zugreifen.

Nachfolgend sind die wichtigsten Installationsprotokolldateien aufgeführt, die der technische Support möglicherweise zur Lösung von Problemen benötigt.

- `/var/local/log/install.log`(auf allen Grid-Knoten zu finden)
- `/var/local/log/gdu-server.log`(auf dem primären Admin-Knoten zu finden)

Ähnliche Informationen

Informationen zum Zugriff auf die Protokolldateien finden Sie unter"Referenz zu Protokolldateien" .

Wenn Sie weitere Hilfe benötigen, wenden Sie sich an "NetApp Support" .

Die Ressourcenreservierung virtueller Maschinen muss angepasst werden

OVF-Dateien enthalten eine Ressourcenreservierung, die sicherstellen soll, dass jeder Grid-Knoten über ausreichend RAM und CPU verfügt, um effizient zu arbeiten. Wenn Sie virtuelle Maschinen erstellen, indem Sie diese OVF-Dateien auf VMware bereitstellen, und die vordefinierte Anzahl an Ressourcen nicht verfügbar ist, werden die virtuellen Maschinen nicht gestartet.

Informationen zu diesem Vorgang

Wenn Sie sicher sind, dass der VM-Host über ausreichend Ressourcen für jeden Grid-Knoten verfügt, passen Sie die den einzelnen virtuellen Maschinen zugewiesenen Ressourcen manuell an und versuchen Sie dann, die virtuellen Maschinen zu starten.

Schritte

1. Wählen Sie in der VMware vSphere Hypervisor-Clientstruktur die virtuelle Maschine aus, die nicht gestartet ist.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie im Eigenschaftenfenster der virtuellen Maschine die Registerkarte **Ressourcen** aus.
4. Passen Sie die der virtuellen Maschine zugewiesenen Ressourcen an:
   a. Wählen Sie **CPU** aus und passen Sie dann mit dem Reservierungsschieberegler die für diese virtuelle Maschine reservierte MHz-Zahl an.
   b. Wählen Sie **Speicher** aus und passen Sie dann mit dem Reservierungsregler die für diese virtuelle Maschine reservierte MB-Zahl an.
5. Klicken Sie auf **OK**.
6. Wiederholen Sie den Vorgang nach Bedarf für andere virtuelle Maschinen, die auf demselben VM-Host gehostet werden.

Das temporäre Installationskennwort wurde deaktiviert

Wenn Sie einen VMware-Knoten bereitstellen, können Sie optional ein temporäres Installationskennwort angeben. Sie müssen über dieses Kennwort verfügen, um auf die VM-Konsole zuzugreifen oder SSH zu verwenden, bevor der neue Knoten dem Grid beitritt.

Wenn Sie sich für die Deaktivierung des temporären Installationskennworts entschieden haben, müssen Sie

zusätzliche Schritte ausführen, um Installationsprobleme zu beheben.

Sie können einen der folgenden Schritte ausführen:

- Stellen Sie die VM erneut bereit, geben Sie jedoch ein temporäres Installationskennwort an, damit Sie auf die Konsole zugreifen oder SSH zum Debuggen von Installationsproblemen verwenden können.
- Verwenden Sie vCenter, um das Kennwort festzulegen:
  a. Schalten Sie die VM aus.
  b. Gehen Sie zu **VM**, wählen Sie die Registerkarte **Konfigurieren** und wählen Sie **vApp-Optionen**.
  c. Geben Sie den Typ des temporären Installationskennworts an, das festgelegt werden soll:
     - Wählen Sie **CUSTOM_TEMPORARY_PASSWORD**, um ein benutzerdefiniertes temporäres Passwort festzulegen.
     - Wählen Sie **TEMPORARY_PASSWORD_TYPE**, um den Knotennamen als temporäres Passwort zu verwenden.
  d. Wählen Sie **Wert festlegen**.
  e. Legen Sie das temporäre Passwort fest:
     - Ändern Sie **CUSTOM_TEMPORARY_PASSWORD** in einen benutzerdefinierten Kennwortwert.
     - Aktualisieren Sie **TEMPORARY_PASSWORD_TYPE** mit dem Wert **Knotennamen verwenden**.
  f. Starten Sie die VM neu, um das neue Kennwort anzuwenden.

Aktualisieren Sie die StorageGRID -Software

Aktualisieren Sie die StorageGRID -Software

Verwenden Sie diese Anweisungen, um ein StorageGRID -System auf eine neue Version zu aktualisieren.

Wenn Sie das Upgrade durchführen, werden alle Knoten in Ihrem StorageGRID -System aktualisiert.

Bevor Sie beginnen

Lesen Sie diese Themen, um mehr über die neuen Funktionen und Verbesserungen in StorageGRID 11.9 zu erfahren, festzustellen, ob Funktionen veraltet sind oder entfernt wurden, und sich über Änderungen an den StorageGRID -APIs zu informieren.

- "Was ist neu in StorageGRID 11.9"
- "Entfernte oder veraltete Funktionen"
- "Änderungen an der Grid Management API"
- "Änderungen an der Tenant Management API"

Was ist neu in StorageGRID 11.9

Diese Version von StorageGRID führt die folgenden Funktionen und Funktionsänderungen ein.

Skalierbarkeit

Reine Datenspeicherknoten

Um eine detailliertere Skalierung zu ermöglichen, können Sie jetzt installieren"Nur-Daten-Speicherknoten" . Wenn die Metadatenverarbeitung nicht kritisch ist, können Sie Ihre Infrastruktur kostengünstig optimieren. Diese Flexibilität hilft dabei, unterschiedliche Arbeitsbelastungen und Wachstumsmuster zu bewältigen.

Verbesserungen des Cloud Storage Pools

IAM-Rollen überall

StorageGRID unterstützt jetzt kurzfristige Anmeldeinformationen mit"IAM-Rollen überall in Amazon S3 für Cloud-Speicherpools" .

Die Verwendung langfristiger Anmeldeinformationen für den Zugriff auf S3-Buckets birgt Sicherheitsrisiken, wenn diese Anmeldeinformationen kompromittiert werden. Kurzzeit-Anmeldeinformationen haben eine begrenzte Lebensdauer, wodurch das Risiko eines unbefugten Zugriffs verringert wird.

S3 Object Lock-Buckets

Sie können jetzt"Konfigurieren Sie einen Cloud-Speicherpool mithilfe eines Amazon S3-Endpunkts" . S3 Object Lock hilft, das versehentliche oder böswillige Löschen von Objekten zu verhindern. Wenn Sie Daten von StorageGRID auf Amazon S3 verschieben, verbessert die Aktivierung der Objektsperre auf beiden Systemen den Datenschutz über den gesamten Lebenszyklus der Daten.

Mandantenfähigkeit

Bucket-Grenzen

Von"Festlegen von Grenzwerten für S3-Buckets" können Sie verhindern, dass Mieter Kapazitäten monopolisieren. Darüber hinaus kann unkontrolliertes Wachstum zu unerwarteten Kosten führen. Durch die Festlegung von Grenzen können Sie die Lagerkosten Ihrer Mieter besser einschätzen.

5.000 Eimer pro Mieter

Um die Skalierbarkeit zu verbessern, unterstützt StorageGRID jetzt bis zu"5.000 S3-Buckets pro Mandant" . Jedes Raster kann maximal 100.000 Buckets enthalten.

Um 5.000 Buckets zu unterstützen, muss jeder Speicherknoten im Grid über mindestens 64 GB RAM verfügen.

Verbesserungen bei S3 Object Lock

Die Konfigurationsmöglichkeiten pro Mandant bieten das richtige Gleichgewicht zwischen Flexibilität und Datensicherheit. Sie können jetzt Aufbewahrungseinstellungen pro Mandant konfigurieren, um:

- Compliance-Modus zulassen oder nicht zulassen
- Legen Sie eine maximale Aufbewahrungsdauer fest

Siehe:

- "Verwalten von Objekten mit S3 Object Lock"
- "So steuern Grid-Administratoren die Objektaufbewahrung"

- "Mieterkonto erstellen"

S3-Kompatibilität

x-amz-checksum-sha256 Prüfsumme

- Die S3 REST API bietet jetzt Unterstützung für `x-amz-checksum-sha256` Prüfsumme.
- StorageGRID bietet jetzt SHA-256-Prüfsummenunterstützung für PUT-, GET- und HEAD-Operationen. Diese Prüfsummen verbessern die Datenintegrität.

Änderungen an der S3-Protokollunterstützung

- Unterstützung für Mountpoint für Amazon S3 hinzugefügt, wodurch Anwendungen eine direkte Verbindung zu S3-Buckets herstellen können, als wären sie lokale Dateisysteme. Sie können StorageGRID jetzt mit mehr Anwendungen und mehr Anwendungsfällen verwenden.
- Im Rahmen der Unterstützung für Mountpoint enthält StorageGRID 11.9"zusätzliche Änderungen an der S3-Protokollunterstützung" .

Wartung und Support

AutoSupport

"AutoSupport"Erstellt jetzt automatisch Hardwarefehlerfälle für ältere Geräte.

Erweiterte Knotenklonvorgänge

Die Nutzbarkeit von Knotenklonen wurde erweitert, um größere Speicherknoten zu unterstützen.

Verbesserte ILM-Behandlung abgelaufener Löschmarkierungen

ILM-Aufnahmezeitregeln mit einem Zeitraum von Tagen entfernen jetzt auch abgelaufene Objektlöschmarkierungen. Löschmarkierungen werden nur entfernt, wenn ein Zeitraum von Tagen verstrichen ist und die aktuelle Löschmarkierung abgelaufen ist (es gibt keine nicht aktuellen Versionen).

Siehe"So werden versionierte S3-Objekte gelöscht" Und"Beispiel für den Bucket-Lebenszyklus, der Vorrang vor der ILM-Richtlinie hat" .

Verbesserte Knoten-Außerbetriebnahme

Um einen reibungslosen und effizienten Übergang zur StorageGRID Hardware der nächsten Generation zu gewährleisten,"Knotenstilllegung" wurde verbessert.

Syslog für Load Balancer-Endpunkte

Die Zugriffsprotokolle der Load Balancer-Endpunkte enthalten Informationen zur Fehlerbehebung, beispielsweise HTTP-Statuscodes. StorageGRID unterstützt jetzt"Exportieren dieser Protokolle auf einen externen Syslog-Server" . Diese Verbesserung ermöglicht eine effizientere Protokollverwaltung und Integration in vorhandene Überwachungs- und Warnsysteme.

Zusätzliche Verbesserungen für Wartung und Support

- Aktualisierung der Metrik-Benutzeroberfläche
- Neue Betriebssystemqualifikationen

- Unterstützung für neue Komponenten von Drittanbietern

Sicherheit

Rotation der SSH-Zugriffsschlüssel

Grid-Administratoren können jetzt"SSH-Schlüssel aktualisieren und rotieren" . Die Möglichkeit, SSH-Schlüssel zu rotieren, ist eine bewährte Sicherheitsmethode und ein proaktiver Abwehrmechanismus.

Warnungen für Root-Anmeldungen

Wenn sich eine unbekannte Entität als Root beim Grid Manager anmeldet,"ein Alarm ausgelöst wird" . Die Überwachung von Root-SSH-Anmeldungen ist ein proaktiver Schritt zum Schutz Ihrer Infrastruktur.

Grid Manager-Erweiterungen

Die Seite mit den Erasure-Coding-Profilen wurde verschoben

Die Seite mit den Erasure-Coding-Profilen befindet sich jetzt unter **KONFIGURATION** > **System** > **Erasure Coding**. Früher war es im ILM-Menü.

Suchverbesserungen

Der"Suchfeld im Grid Manager" enthält jetzt eine bessere Übereinstimmungslogik, mit der Sie Seiten finden können, indem Sie nach gängigen Abkürzungen und den Namen bestimmter Einstellungen innerhalb einer Seite suchen. Sie können auch nach weiteren Elementtypen suchen, beispielsweise nach Knoten, Benutzern und Mandantenkonten.

Entfernte oder veraltete Funktionen und Fähigkeiten

Einige Funktionen und Fähigkeiten wurden in dieser Version entfernt oder verworfen. Überprüfen Sie diese Punkte, um zu ermitteln, ob Sie Clientanwendungen aktualisieren oder Ihre Konfiguration ändern müssen, bevor Sie ein Upgrade durchführen.

Definitionen

Veraltet

Die Funktion **sollte** nicht in neuen Produktionsumgebungen verwendet werden. Vorhandene Produktionsumgebungen können die Funktion weiterhin verwenden.

Lebensende

Zuletzt ausgelieferte Version, die die Funktion unterstützt. In einigen Fällen kann die Dokumentation für die Funktion zu diesem Zeitpunkt entfernt werden.

ENTFERNT

Erste Version, die die Funktion **nicht** unterstützt.

Ende der Funktionsunterstützung für StorageGRID

Veraltete Funktionen werden in N+2 Hauptversionen entfernt. Wenn beispielsweise eine Funktion in Version N (z. B. 6.3) veraltet ist, ist die letzte Version, in der die Funktion vorhanden ist, N+1 (z. B. 6.4). Version N+2 (z. B. 6.5) ist die erste Version, bei der die Funktion im Produkt nicht vorhanden ist.

Siehe die "Supportseite für Softwareversionen" für weitere Informationen.

> In bestimmten Situationen kann es sein, dass NetApp den Support für bestimmte Funktionen früher als angegeben einstellt.

Funktion	Veraltet	Lebensende	ENTFERNT	Links zu früheren Dokumentationen
Legacy-Alarme (*keine Warnungen*)	11,7	11,8	11,9	"Alarmreferenz (StorageGRID 11.8)"
Archivknotenunterstützung	11,7	11,8	11,9	"Überlegungen zur Außerbetriebnahme von Archivknoten (StorageGRID 11.8)" **Hinweis**: Bevor Sie mit dem Upgrade beginnen, müssen Sie: 1. Alle Archivknoten außer Betrieb nehmen. Sehen "Außerbetriebnahme von Grid-Knoten (StorageGRID 11.8-Dokumentationsseite)" . 2. Entfernen Sie alle Archivknotenreferenzen aus Speicherpools und ILM-Richtlinien. Sehen "NetApp Knowledge Base: Leitfaden zur Lösung des StorageGRID 11.9-Software-Upgrades" .
Audit-Export über CIFS/Samba	11,1	11,6	11,7	
CLB-Dienst	11,4	11,6	11,7	
Docker-Container-Engine	11,8	11,9	Wird noch bekannt gegeben	Die Unterstützung für Docker als Container-Engine für reine Softwarebereitstellungen ist veraltet. Docker wird in einer zukünftigen Version durch eine andere Container-Engine ersetzt. Weitere Informationen finden Sie im"Liste der derzeit unterstützten Docker-Versionen" .
NFS-Auditexport	11,8	11,9	12,0	"Konfigurieren Sie den Audit-Client-Zugriff für NFS (StorageGRID 11.8)."
Swift-API-Unterstützung	11,7	11,9	12,0	"Verwenden Sie die Swift REST API (StorageGRID 11.8)"

Funktion	Veraltet	Lebensende	ENTFERNT	Links zu früheren Dokumentationen
RHEL 8,8	11,9	11,9	12,0	
RHEL 9,0	11,9	11,9	12,0	
RHEL 9,2	11,9	11,9	12,0	
Ubuntu 18,04	11,9	11,9	12,0	
Ubuntu 20,04	11,9	11,9	12,0	
Debian 11	11,9	11,9	12,0	

Siehe auch:

- "Änderungen an der Grid Management API"
- "Änderungen an der Tenant Management API"

Änderungen an der Grid Management API

StorageGRID 11.9 verwendet Version 4 der Grid Management API. Version 4 macht Version 3 veraltet; die Versionen 1, 2 und 3 werden jedoch weiterhin unterstützt.

> Sie können veraltete Versionen der Verwaltungs-API weiterhin mit StorageGRID 11.9 verwenden. Die Unterstützung für diese Versionen der API wird jedoch in einer zukünftigen Version von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.9 können Sie die veralteten APIs deaktivieren, indem Sie die `PUT /grid/config/management` API.

Weitere Informationen finden Sie unter"Verwenden Sie die Grid Management API" .

Überprüfen Sie die Compliance-Einstellungen, nachdem Sie die globale S3-Objektsperre aktiviert haben

Überprüfen Sie die Compliance-Einstellungen vorhandener Mandanten, nachdem Sie die globale S3-Objektsperreinstellung aktiviert haben. Wenn Sie diese Einstellung aktivieren, hängen die S3 Object Lock-Einstellungen pro Mandant von der StorageGRID Version zum Zeitpunkt der Mandantenerstellung ab.

Legacy-MGM-API-Anfragen entfernt

Diese alten Anfragen wurden entfernt:

`/grid/server-types`

`/grid/ntp-roles`

Änderungen an `GET /private/storage-usage` API

- Eine neue Immobilie, `usageCacheDuration` , wurde dem Antworttext hinzugefügt. Diese Eigenschaft gibt die Dauer (in Sekunden) an, für die der Usage Lookup Cache gültig bleibt. Dieser Wert gilt, wenn die Nutzung mit den Speicherkontingenten und Bucket-Kapazitätsgrenzen des Mandanten verglichen wird.
- Der `GET /api/v4/private/storage-usage` Das Verhalten wurde korrigiert, um der Verschachtelung aus dem Schema zu entsprechen.
- Diese Änderungen gelten nur für die private API.

Änderungen an `GET cross-grid-replication` API

Die GET-API **/org/containers/:name/cross-grid-replication** erfordert keinen Root-Zugriff mehr(`rootAccess`)-Berechtigung; Sie müssen jedoch einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten verfügt.(`manageAllContainers`) oder Alle Buckets anzeigen(`viewAllContainers`) Erlaubnis.

Die PUT-API **/org/containers/:name/cross-grid-replication** ist unverändert und erfordert weiterhin den Root-Zugriff(`rootAccess`) Erlaubnis.

Änderungen an der Tenant Management API

StorageGRID 11.9 verwendet Version 4 der Tenant Management API. Version 4 macht Version 3 veraltet; die Versionen 1, 2 und 3 werden jedoch weiterhin unterstützt.

> Sie können veraltete Versionen der Tenant Management API weiterhin mit StorageGRID 11.9 verwenden. Die Unterstützung für diese Versionen der API wird jedoch in einer zukünftigen Version von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.9 können Sie die veralteten APIs deaktivieren, indem Sie die `PUT /grid/config/management` API.

Weitere Informationen finden Sie unter"Die Tenant Management API verstehen" .

Neue API für Bucket-Kapazitätslimit

Sie können die `/org/containers/{bucketName}/quota-object-bytes` API mit GET/PUT-Operationen zum Abrufen und Festlegen des Speicherkapazitätslimits für einen Bucket.

Planen und Vorbereiten des Upgrades

Schätzen Sie die Zeit, die für die Durchführung eines Upgrades benötigt wird

Überlegen Sie, wann Sie ein Upgrade durchführen sollten, und berücksichtigen Sie dabei, wie lange das Upgrade dauern könnte. Achten Sie darauf, welche Vorgänge Sie in den einzelnen Phasen des Upgrades ausführen können und welche nicht.

Informationen zu diesem Vorgang

Die für die Durchführung eines StorageGRID -Upgrades erforderliche Zeit hängt von verschiedenen Faktoren ab, beispielsweise von der Client-Auslastung und der Hardwareleistung.

In der Tabelle sind die wichtigsten Upgrade-Aufgaben zusammengefasst und die ungefähre für jede Aufgabe erforderliche Zeit aufgeführt. Die Schritte nach der Tabelle enthalten Anweisungen, mit denen Sie die Upgrade-Zeit für Ihr System abschätzen können.

Upgrade-Aufgabe	Beschreibung	Ungefähre benötigte Zeit	Während dieser Aufgabe
Führen Sie Vorprüfungen durch und aktualisieren Sie den primären Admin-Knoten	Die Upgrade-Vorprüfungen werden ausgeführt und der primäre Admin-Knoten wird gestoppt, aktualisiert und neu gestartet.	30 Minuten bis 1 Stunde, wobei die Knoten der Service-Appliance die meiste Zeit benötigen. Ungelöste Vorprüfungsfehler verlängern diese Zeit.	Sie können nicht auf den primären Admin-Knoten zugreifen. Möglicherweise werden Verbindungsfehler gemeldet, die Sie ignorieren können. Durch Ausführen der Upgrade-Vorprüfungen vor dem Starten des Upgrades können Sie alle Fehler vor dem geplanten Wartungsfenster für das Upgrade beheben.
Upgrade-Service starten	Die Softwaredatei wird verteilt und der Upgrade-Dienst gestartet.	3 Minuten pro Grid-Knoten	
Aktualisieren Sie andere Grid-Knoten	Die Software auf allen anderen Grid-Knoten wird in der Reihenfolge aktualisiert, in der Sie die Knoten genehmigen. Jeder Knoten in Ihrem System wird einzeln heruntergefahren.	15 Minuten bis 1 Stunde pro Knoten, wobei Appliance-Knoten die meiste Zeit benötigen **Hinweis**: Für Appliance-Knoten wird das StorageGRID Appliance Installer automatisch auf die neueste Version aktualisiert.	• Ändern Sie nicht die Rasterkonfiguration. • Ändern Sie die Konfiguration der Überwachungsebene nicht. • Aktualisieren Sie die ILM-Konfiguration nicht. • Sie können keine anderen Wartungsvorgänge wie Hotfixes, Außerbetriebnahmen oder Erweiterungen durchführen. **Hinweis**: Wenn Sie eine Wiederherstellung durchführen müssen, wenden Sie sich an den technischen Support.
Funktionen aktivieren	Die neuen Funktionen für die neue Version sind aktiviert.	Weniger als 5 Minuten	• Ändern Sie nicht die Rasterkonfiguration. • Ändern Sie die Konfiguration der Überwachungsebene nicht. • Aktualisieren Sie die ILM-Konfiguration nicht. • Sie können keine weiteren Wartungsvorgänge durchführen.

Upgrade-Aufgabe	Beschreibung	Ungefähre benötigte Zeit	Während dieser Aufgabe
Datenbank aktualisieren	Der Upgrade-Prozess überprüft jeden Knoten, um sicherzustellen, dass die Cassandra-Datenbank nicht aktualisiert werden muss.	10 Sekunden pro Knoten oder einige Minuten für das gesamte Raster	Das Upgrade von StorageGRID 11.8 auf 11.9 erfordert kein Upgrade der Cassandra-Datenbank. Der Cassandra-Dienst wird jedoch auf jedem Speicherknoten gestoppt und neu gestartet. Bei zukünftigen StorageGRID Funktionsversionen kann die Aktualisierung der Cassandra-Datenbank mehrere Tage dauern.
Abschließende Upgrade-Schritte	Temporäre Dateien werden entfernt und das Upgrade auf die neue Version abgeschlossen.	5 Minuten	Wenn die Aufgabe **Letzte Upgrade-Schritte** abgeschlossen ist, können Sie alle Wartungsverfahren durchführen.

Schritte

1. Schätzen Sie die erforderliche Zeit zum Aktualisieren aller Grid-Knoten.
   a. Multiplizieren Sie die Anzahl der Knoten in Ihrem StorageGRID -System mit 1 Stunde/Knoten.

      Generell dauert die Aktualisierung von Appliance-Knoten länger als die von softwarebasierten Knoten.

   b. Fügen Sie zu dieser Zeit 1 Stunde hinzu, um die Zeit zu berücksichtigen, die zum Herunterladen der `.upgrade` Datei, führen Sie Vorabprüfungen durch und schließen Sie die letzten Upgrade-Schritte ab.
2. Wenn Sie Linux-Knoten haben, fügen Sie für jeden Knoten 15 Minuten hinzu, um die zum Herunterladen und Installieren des RPM- oder DEB-Pakets erforderliche Zeit zu berücksichtigen.
3. Berechnen Sie die geschätzte Gesamtzeit für das Upgrade, indem Sie die Ergebnisse der Schritte 1 und 2 addieren.

Beispiel: Geschätzte Zeit für das Upgrade auf StorageGRID 11.9

Angenommen, Ihr System verfügt über 14 Grid-Knoten, von denen 8 Linux-Knoten sind.

1. Multiplizieren Sie 14 mit 1 Stunde/Knoten.
2. Fügen Sie 1 Stunde hinzu, um den Download, die Vorprüfung und die letzten Schritte zu berücksichtigen.

   Die geschätzte Zeit zum Upgrade aller Knoten beträgt 15 Stunden.

3. Multiplizieren Sie 8 mit 15 Minuten/Knoten, um die Zeit für die Installation des RPM- oder DEB-Pakets auf den Linux-Knoten zu berücksichtigen.

   Die geschätzte Zeit für diesen Schritt beträgt 2 Stunden.

4. Addieren Sie die Werte.

   Sie sollten bis zu 17 Stunden einplanen, um das Upgrade Ihres Systems auf StorageGRID 11.9.0 abzuschließen.

Bei Bedarf können Sie das Wartungsfenster in kleinere Fenster aufteilen, indem Sie die Aktualisierung von Teilmengen von Grid-Knoten in mehreren Sitzungen genehmigen. Beispielsweise möchten Sie möglicherweise die Knoten an Standort A in einer Sitzung aktualisieren und dann die Knoten an Standort B in einer späteren Sitzung aktualisieren. Wenn Sie das Upgrade in mehreren Sitzungen durchführen möchten, beachten Sie, dass Sie die neuen Funktionen erst verwenden können, wenn alle Knoten aktualisiert wurden.

Auswirkungen des Upgrades auf Ihr System

Erfahren Sie, welche Auswirkungen das Upgrade auf Ihr StorageGRID -System hat.

StorageGRID -Upgrades sind unterbrechungsfrei

Das StorageGRID -System kann während des gesamten Upgrade-Prozesses Daten von Client-Anwendungen aufnehmen und abrufen. Wenn Sie die Aktualisierung aller Knoten desselben Typs genehmigen (z. B. Speicherknoten), werden die Knoten einzeln heruntergefahren, sodass es nicht vorkommt, dass alle Grid-Knoten oder alle Grid-Knoten eines bestimmten Typs nicht verfügbar sind.

Um eine kontinuierliche Verfügbarkeit zu gewährleisten, stellen Sie sicher, dass Ihre ILM-Richtlinie Regeln enthält, die das Speichern mehrerer Kopien jedes Objekts vorschreiben. Sie müssen außerdem sicherstellen, dass alle externen S3-Clients so konfiguriert sind, dass sie Anfragen an eines der folgenden Elemente senden:

- Eine virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe (HA)
- Ein hochverfügbarer Load Balancer eines Drittanbieters
- Mehrere Gateway-Knoten für jeden Client
- Mehrere Speicherknoten für jeden Client

Bei Clientanwendungen kann es zu kurzfristigen Störungen kommen

Das StorageGRID -System kann während des gesamten Upgrade-Prozesses Daten von Client-Anwendungen aufnehmen und abrufen. Allerdings können Client-Verbindungen zu einzelnen Gateway-Knoten oder Speicherknoten vorübergehend unterbrochen werden, wenn für das Upgrade ein Neustart der Dienste auf diesen Knoten erforderlich ist. Die Konnektivität wird wiederhergestellt, nachdem der Upgrade-Prozess abgeschlossen ist und die Dienste auf den einzelnen Knoten wieder aufgenommen werden.

Wenn ein kurzzeitiger Verbindungsverlust nicht akzeptabel ist, müssen Sie möglicherweise eine Ausfallzeit für die Durchführung eines Upgrades einplanen. Mithilfe der selektiven Genehmigung können Sie planen, wann bestimmte Knoten aktualisiert werden.

Sie können mehrere Gateways und Hochverfügbarkeitsgruppen (HA) verwenden, um während des Upgrade-Prozesses ein automatisches Failover bereitzustellen. Siehe die Anweisungen für"Konfigurieren von Hochverfügbarkeitsgruppen" .

Die Appliance-Firmware wird aktualisiert

Während des StorageGRID 11.9-Upgrades:

- Alle StorageGRID Appliance-Knoten werden automatisch auf die StorageGRID Appliance Installer-Firmwareversion 3.9 aktualisiert.
- SG6060- und SGF6024-Geräte werden automatisch auf die BIOS-Firmware-Version 3B08.EX und die BMC -Firmware-Version 4.00.07 aktualisiert.

- SG100- und SG1000-Geräte werden automatisch auf die BIOS-Firmware-Version 3B13.EC und die BMC -Firmware-Version 4.74.07 aktualisiert.
- Die Geräte SGF6112, SG6160, SG110 und SG1100 werden automatisch auf die BMC -Firmwareversion 3.16.07 aktualisiert.

ILM-Richtlinien werden je nach Status unterschiedlich behandelt

- Die aktive Richtlinie bleibt nach dem Upgrade unverändert.
- Beim Upgrade bleiben nur die letzten 10 historischen Richtlinien erhalten.
- Wenn eine vorgeschlagene Richtlinie vorhanden ist, wird sie während des Upgrades gelöscht.

Es können Warnungen ausgelöst werden

Warnungen können ausgelöst werden, wenn Dienste gestartet und gestoppt werden und wenn das StorageGRID -System als Umgebung mit gemischten Versionen betrieben wird (einige Grid-Knoten führen eine frühere Version aus, während andere auf eine neuere Version aktualisiert wurden). Nach Abschluss des Upgrades können weitere Warnungen ausgelöst werden.

Beispielsweise wird möglicherweise die Warnung **Kommunikation mit Knoten nicht möglich** angezeigt, wenn Dienste gestoppt werden, oder die Warnung **Cassandra-Kommunikationsfehler**, wenn einige Knoten auf StorageGRID 11.9 aktualisiert wurden, auf anderen Knoten jedoch noch StorageGRID 11.8 ausgeführt wird. Im Allgemeinen werden diese Warnungen gelöscht, wenn das Upgrade abgeschlossen ist.

Die Warnung **ILM-Platzierung nicht erreichbar** kann ausgelöst werden, wenn Speicherknoten während des Upgrades auf StorageGRID 11.9 angehalten werden. Diese Warnung bleibt möglicherweise noch einen Tag nach Abschluss des Upgrades bestehen.

Nach Abschluss des Upgrades können Sie alle Upgrade-bezogenen Warnungen überprüfen, indem Sie im Grid Manager-Dashboard **Kürzlich behobene Warnungen** oder **Aktuelle Warnungen** auswählen.

Viele SNMP-Benachrichtigungen werden generiert

Beachten Sie, dass beim Anhalten und Neustarten von Grid-Knoten während des Upgrades möglicherweise eine große Anzahl von SNMP-Benachrichtigungen generiert wird. Um übermäßige Benachrichtigungen zu vermeiden, deaktivieren Sie das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren** (**KONFIGURATION** > **Überwachung** > **SNMP-Agent**), um SNMP-Benachrichtigungen zu deaktivieren, bevor Sie mit dem Upgrade beginnen. Aktivieren Sie die Benachrichtigungen dann erneut, nachdem das Upgrade abgeschlossen ist.

Konfigurationsänderungen sind eingeschränkt

> Diese Liste gilt speziell für Upgrades von StorageGRID 11.8 auf StorageGRID 11.9. Wenn Sie auf eine andere StorageGRID Version aktualisieren, lesen Sie die Liste der eingeschränkten Änderungen in den Upgrade-Anweisungen für diese Version.

Bis die Aufgabe **Neue Funktion aktivieren** abgeschlossen ist:

- Nehmen Sie keine Änderungen an der Rasterkonfiguration vor.
- Aktivieren oder deaktivieren Sie keine neuen Funktionen.
- Aktualisieren Sie die ILM-Konfiguration nicht. Andernfalls kann es zu inkonsistentem und unerwartetem ILM-Verhalten kommen.

- Wenden Sie keinen Hotfix an und stellen Sie keinen Grid-Knoten wieder her.

> Wenden Sie sich an den technischen Support, wenn Sie während des Upgrades einen Knoten wiederherstellen müssen.

- Sie sollten während des Upgrades auf StorageGRID 11.9 keine HA-Gruppen, VLAN-Schnittstellen oder Load Balancer-Endpunkte verwalten.
- Löschen Sie keine HA-Gruppen, bis das Upgrade auf StorageGRID 11.9 abgeschlossen ist. Auf virtuelle IP-Adressen in anderen HA-Gruppen kann möglicherweise nicht mehr zugegriffen werden.

Bis die Aufgabe **Letzte Upgrade-Schritte** abgeschlossen ist:

- Führen Sie keinen Erweiterungsvorgang durch.
- Führen Sie kein Außerbetriebnahmeverfahren durch.

Sie können Bucket-Details nicht anzeigen oder Buckets vom Tenant Manager aus verwalten.

Während des Upgrades auf StorageGRID 11.9 (d. h. während das System als Umgebung mit gemischten Versionen betrieben wird) können Sie mit dem Tenant Manager keine Bucket-Details anzeigen oder Buckets verwalten. Auf der Buckets-Seite im Tenant Manager wird einer der folgenden Fehler angezeigt:

- Sie können diese API nicht verwenden, während Sie auf 11.9 aktualisieren.
- Während Sie ein Upgrade auf 11.9 durchführen, können Sie im Tenant Manager keine Bucket-Versionsdetails anzeigen.

Dieser Fehler wird behoben, nachdem das Upgrade auf 11.9 abgeschlossen ist.

Problemumgehung

Während das Upgrade auf 11.9 läuft, können Sie die folgenden Tools verwenden, um Bucket-Details anzuzeigen oder Buckets zu verwalten, anstatt den Tenant Manager zu verwenden:

- Um Standard-S3-Operationen auf einem Bucket durchzuführen, verwenden Sie entweder die"S3 REST API" oder die"Mandantenverwaltungs-API" .
- Um benutzerdefinierte StorageGRID -Vorgänge für einen Bucket auszuführen (z. B. Anzeigen und Ändern der Bucket-Konsistenz, Aktivieren oder Deaktivieren von Aktualisierungen der letzten Zugriffszeit oder Konfigurieren der Suchintegration), verwenden Sie die Tenant Management API.

Überprüfen Sie die installierte Version von StorageGRID

Stellen Sie vor dem Starten des Upgrades sicher, dass die vorherige Version von StorageGRID mit dem neuesten verfügbaren Hotfix installiert ist.

Informationen zu diesem Vorgang

Bevor Sie auf StorageGRID 11.9 aktualisieren, muss auf Ihrem Grid StorageGRID 11.8 installiert sein. Wenn Sie derzeit eine frühere Version von StorageGRID verwenden, müssen Sie alle vorherigen Upgrade-Dateien zusammen mit den neuesten Hotfixes installieren (dringend empfohlen), bis die aktuelle Version Ihres Grids StorageGRID 11.8.*x.y* ist.

Ein möglicher Upgrade-Pfad wird in derBeispiel .

NetApp empfiehlt dringend, dass Sie vor dem Upgrade auf die nächste Version den neuesten Hotfix für jede StorageGRID Version anwenden und dass Sie auch für jede neue Version, die Sie installieren, den neuesten Hotfix anwenden. In einigen Fällen müssen Sie einen Hotfix anwenden, um das Risiko eines Datenverlusts zu vermeiden. Sehen "NetApp Downloads: StorageGRID" und die Versionshinweise zu jedem Hotfix, um mehr zu erfahren.

Schritte

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Wählen Sie oben im Grid Manager **Hilfe** > **Info**.
3. Stellen Sie sicher, dass die **Version** 11.8.*x.y* ist.

   In der StorageGRID 11.8.*x.y*-Versionsnummer:

   - Die **Hauptversion** hat einen *x*-Wert von 0 (11.8.0).
   - Ein **Hotfix** hat, sofern einer angewendet wurde, einen *y*-Wert (z. B. 11.8.0.1).
4. Wenn **Version** nicht 11.8.*x.y* ist, gehen Sie zu "NetApp Downloads: StorageGRID" um die Dateien für jede vorherige Version herunterzuladen, einschließlich des neuesten Hotfixes für jede Version.
5. Erhalten Sie die Upgrade-Anweisungen für jede heruntergeladene Version. Führen Sie dann das Software-Upgrade-Verfahren für diese Version durch und wenden Sie den neuesten Hotfix für diese Version an (dringend empfohlen).

   Siehe die"StorageGRID Hotfix-Verfahren" .

Beispiel: Upgrade auf StorageGRID 11.9 von Version 11.6

Das folgende Beispiel zeigt die Schritte zum Upgrade von StorageGRID Version 11.6 auf Version 11.8 als Vorbereitung für ein StorageGRID 11.9-Upgrade.

Laden Sie die Software herunter und installieren Sie sie in der folgenden Reihenfolge, um Ihr System auf das Upgrade vorzubereiten:

1. Aktualisieren Sie auf die Hauptversion von StorageGRID 11.6.0.
2. Wenden Sie den neuesten StorageGRID 11.6.0.*y*-Hotfix an.
3. Aktualisieren Sie auf die Hauptversion von StorageGRID 11.7.0.
4. Wenden Sie den neuesten StorageGRID 11.7.0.*y*-Hotfix an.
5. Aktualisieren Sie auf die Hauptversion von StorageGRID 11.8.0.
6. Wenden Sie den neuesten StorageGRID 11.8.0.*y*-Hotfix an.

Besorgen Sie sich die erforderlichen Materialien für ein Software-Upgrade

Bevor Sie mit dem Software-Upgrade beginnen, besorgen Sie sich alle erforderlichen Materialien.

Artikel	Hinweise
Service-Laptop	Der Dienstlaptop muss über Folgendes verfügen: • Netzwerkanschluss • SSH-Client (z. B. PuTTY)
"Unterstützte Webbrowser"	Die Browserunterstützung ändert sich normalerweise für jede StorageGRID Version. Stellen Sie sicher, dass Ihr Browser mit der neuen StorageGRID -Version kompatibel ist.
Bereitstellungspassphrase	Die Passphrase wird bei der Erstinstallation des StorageGRID -Systems erstellt und dokumentiert. Die Bereitstellungspassphrase ist nicht aufgeführt in der `Passwords.txt` Datei.
Linux RPM- oder DEB-Archiv	Wenn Knoten auf Linux-Hosts bereitgestellt werden, müssen Sie"Laden Sie das RPM- oder DEB-Paket herunter und installieren Sie es auf allen Hosts" bevor Sie mit dem Upgrade beginnen. Stellen Sie sicher, dass Ihr Betriebssystem die Mindestanforderungen von StorageGRID an die Kernelversion erfüllt: • "Installieren Sie StorageGRID auf Red Hat Enterprise Linux-Hosts" • "Installieren Sie StorageGRID auf Ubuntu- oder Debian-Hosts"
StorageGRID -Dokumentation	• "Versionshinweise"für StorageGRID 11.9 (Anmeldung erforderlich). Lesen Sie diese sorgfältig durch, bevor Sie mit dem Upgrade beginnen. • "Lösungshandbuch für StorageGRID -Software-Upgrades"für die Hauptversion, auf die Sie aktualisieren (Anmeldung erforderlich) • Andere "StorageGRID -Dokumentation" , je nach Bedarf.

Überprüfen Sie den Zustand des Systems

Bevor Sie ein StorageGRID -System aktualisieren, stellen Sie sicher, dass das System für die Aktualisierung bereit ist. Stellen Sie sicher, dass das System normal läuft und alle Grid-Knoten betriebsbereit sind.

Schritte

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Suchen Sie nach aktiven Warnungen und beheben Sie diese.
3. Stellen Sie sicher, dass keine widersprüchlichen Grid-Aufgaben aktiv oder ausstehend sind.
   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
   b. Wählen Sie ***site*** > ***primärer Admin-Knoten*** > **CMN** > **Grid-Aufgaben** > **Konfiguration**.

      ILME-Aufgaben (Information Lifecycle Management Evaluation) sind die einzigen Grid-Aufgaben, die gleichzeitig mit dem Software-Upgrade ausgeführt werden können.

c. Wenn andere Grid-Aufgaben aktiv oder ausstehend sind, warten Sie, bis sie abgeschlossen sind oder ihre Sperre aufgehoben wird.

> Wenden Sie sich an den technischen Support, wenn eine Aufgabe nicht abgeschlossen oder die Sperre nicht aufgehoben wird.

4. Siehe"Interne Grid-Knoten-Kommunikation" Und"Externe Kommunikation" um sicherzustellen, dass alle erforderlichen Ports für StorageGRID 11.9 geöffnet sind, bevor Sie ein Upgrade durchführen.

> Beim Upgrade auf StorageGRID 11.9 sind keine zusätzlichen Ports erforderlich.

Der folgende erforderliche Port wurde in StorageGRID 11.7 hinzugefügt. Stellen Sie sicher, dass es verfügbar ist, bevor Sie auf StorageGRID 11.9 aktualisieren.

Hafen	Beschreibung
18086	Der TCP-Port wird für S3-Anfragen vom StorageGRID Load Balancer an LDR und den neuen LDR-Dienst verwendet. Vergewissern Sie sich vor dem Upgrade, dass dieser Port von allen Grid-Knoten zu allen Speicherknoten geöffnet ist. Das Blockieren dieses Ports führt nach dem Upgrade auf StorageGRID 11.9 zu Unterbrechungen des S3-Dienstes.

> Wenn Sie benutzerdefinierte Firewall-Ports geöffnet haben, werden Sie während der Upgrade-Vorprüfung benachrichtigt. Sie müssen sich an den technischen Support wenden, bevor Sie mit dem Upgrade fortfahren.

Software-Upgrade

Upgrade-Schnellstart

Überprüfen Sie den allgemeinen Arbeitsablauf, bevor Sie mit dem Upgrade beginnen. Die StorageGRID -Upgradeseite führt Sie durch jeden Upgrade-Schritt.

1 Vorbereiten von Linux-Hosts

Wenn StorageGRID -Knoten auf Linux-Hosts bereitgestellt werden,"Installieren Sie das RPM- oder DEB-Paket auf jedem Host" bevor Sie mit dem Upgrade beginnen.

2 Upgrade- und Hotfix-Dateien hochladen

Greifen Sie vom primären Admin-Knoten auf die StorageGRID -Upgrade-Seite zu und laden Sie die Upgrade-Datei und bei Bedarf die Hotfix-Datei hoch.

3 Wiederherstellungspaket herunterladen

Laden Sie das aktuelle Wiederherstellungspaket herunter, bevor Sie mit dem Upgrade beginnen.

4 Ausführen von Upgrade-Vorabprüfungen

Mithilfe von Upgrade-Vorabprüfungen können Sie Probleme erkennen, sodass Sie diese beheben können, bevor Sie mit dem eigentlichen Upgrade beginnen.

5 Upgrade starten

Wenn Sie das Upgrade starten, werden die Vorprüfungen erneut ausgeführt und der primäre Admin-Knoten wird automatisch aktualisiert. Sie können nicht auf den Grid Manager zugreifen, während der primäre Admin-Knoten aktualisiert wird. Auch Audit-Protokolle sind nicht verfügbar. Dieses Upgrade kann bis zu 30 Minuten dauern.

6 Wiederherstellungspaket herunterladen

Laden Sie nach dem Upgrade des primären Admin-Knotens ein neues Wiederherstellungspaket herunter.

7 Knoten genehmigen

Sie können einzelne Rasterknoten, Gruppen von Rasterknoten oder alle Rasterknoten genehmigen.

> Genehmigen Sie das Upgrade für einen Grid-Knoten nicht, es sei denn, Sie sind sicher, dass der Knoten zum Anhalten und Neustarten bereit ist.

8 Betrieb wieder aufnehmen

Wenn alle Grid-Knoten aktualisiert wurden, werden neue Funktionen aktiviert und Sie können den Betrieb wieder aufnehmen. Mit der Durchführung einer Außerbetriebnahme oder Erweiterung müssen Sie warten, bis die Hintergrundaufgabe **Datenbank aktualisieren** und die Aufgabe **Letzte Aktualisierungsschritte** abgeschlossen sind.

Ähnliche Informationen

"Schätzen Sie die Zeit, die für die Durchführung eines Upgrades benötigt wird"

Linux: Laden Sie das RPM- oder DEB-Paket herunter und installieren Sie es auf allen Hosts

Wenn StorageGRID -Knoten auf Linux-Hosts bereitgestellt werden, laden Sie vor dem Start des Upgrades ein zusätzliches RPM- oder DEB-Paket auf jeden dieser Hosts herunter und installieren Sie es.

Upgrade-, Linux- und Hotfix-Dateien herunterladen

Wenn Sie ein StorageGRID -Upgrade vom Grid Manager aus durchführen, werden Sie im ersten Schritt aufgefordert, das Upgrade-Archiv und alle erforderlichen Hotfixes herunterzuladen. Wenn Sie jedoch Dateien herunterladen müssen, um Linux-Hosts zu aktualisieren, können Sie Zeit sparen, indem Sie alle erforderlichen Dateien im Voraus herunterladen.

Schritte

1. Gehe zu "NetApp Downloads: StorageGRID" .
2. Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version oder wählen Sie eine andere Version aus dem Dropdown-Menü und wählen Sie **Los**.

   Die Softwareversionen von StorageGRID haben dieses Format: 11.*x.y*. StorageGRID -Hotfixes haben dieses Format: 11.*x.y.z*.
3. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Ihr NetApp -Konto an .
4. Wenn ein Hinweis mit der Aufschrift „Vorsicht/Muss gelesen werden“ angezeigt wird, notieren Sie sich die Hotfix-Nummer und aktivieren Sie das Kontrollkästchen.
5. Lesen Sie die Endbenutzer-Lizenzvereinbarung (EULA), aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.

   Die Downloadseite für die von Ihnen ausgewählte Version wird angezeigt. Die Seite enthält drei Spalten.
6. Laden Sie aus der zweiten Spalte (**Upgrade StorageGRID**) zwei Dateien herunter:
   - Das Upgrade-Archiv für die neueste Version (dies ist die Datei im Abschnitt mit der Bezeichnung **VMware, SG1000 oder SG100 Primary Admin Node**). Obwohl diese Datei erst nach der Aktualisierung benötigt wird, sparen Sie durch das Herunterladen jetzt Zeit.
   - Ein RPM- oder DEB-Archiv in entweder `.tgz` oder `.zip` Format. Wählen Sie die `.zip` Datei, wenn Sie Windows auf dem Service-Laptop ausführen.
     - Red Hat Enterprise Linux
       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
     - Ubuntu oder Debian
       `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
       `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
7. Wenn Sie aufgrund eines erforderlichen Hotfixes einem „Vorsicht“-/„Muss gelesen“-Hinweis zustimmen mussten, laden Sie den Hotfix herunter:
   a. Zurück zu "NetApp Downloads: StorageGRID" .
   b. Wählen Sie die Hotfixnummer aus der Dropdown-Liste aus.
   c. Stimmen Sie dem Warnhinweis und der EULA erneut zu.
   d. Laden Sie den Hotfix und seine README-Datei herunter und speichern Sie sie.

      Sie werden aufgefordert, die Hotfix-Datei auf der StorageGRID Upgrade-Seite hochzuladen, wenn Sie das Upgrade starten.

Installieren Sie das Archiv auf allen Linux-Hosts

Führen Sie diese Schritte aus, bevor Sie die StorageGRID -Software aktualisieren.

Schritte

1. Extrahieren Sie die RPM- oder DEB-Pakete aus der Installationsdatei.
2. Installieren Sie die RPM- oder DEB-Pakete auf allen Linux-Hosts.

   Die Schritte zur Installation der StorageGRID Hostdienste finden Sie in den Installationsanweisungen:

- "Red Hat Enterprise Linux: Installieren Sie StorageGRID Hostdienste"
- "Ubuntu oder Debian: Installieren Sie StorageGRID Hostdienste"

Die neuen Pakete werden als zusätzliche Pakete installiert.

Installationsarchive für frühere Versionen entfernen

Um Speicherplatz auf Linux-Hosts freizugeben, können Sie die Installationsarchive für frühere Versionen von StorageGRID entfernen, die Sie nicht mehr benötigen.

Schritte

1. Entfernen Sie die alten StorageGRID Installationsarchive.

Red Hat

1. Erfassen Sie die Liste der installierten StorageGRID -Pakete: `dnf list | grep -i storagegrid`.

   Beispiel:

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. Entfernen Sie vorherige StorageGRID -Pakete: `dnf remove` *`images-package service-package`*

   > Entfernen Sie nicht die Installationsarchive für die Version von StorageGRID , die Sie derzeit ausführen, oder für die Versionen von StorageGRID , auf die Sie ein Upgrade planen.

   Sie können die angezeigten Warnungen getrost ignorieren. Sie beziehen sich auf Dateien, die ersetzt wurden, als Sie neuere StorageGRID -Pakete installiert haben.

   Beispiel:

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.
```

```
Dependencies resolved.
================================================================================
========
Package            Architecture      Version           Repository
Size
================================================================================
========
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
================================================================================
========
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
```

```
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory

  Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64   2/2
  Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
```

```
  Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  2/2
Installed products updated.

Removed:
  StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64
  StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64

Complete!
[root@rhel-example ~]#
```

Ubuntu und Debian

1. Erfassen Sie die Liste der installierten StorageGRID -Pakete: `dpkg -l | grep storagegrid`

   Beispiel:

```
root@debian-example:~# dpkg -l | grep storagegrid
ii  storagegrid-webscale-images-11-6-0  11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale docker images for 11.6.0
ii  storagegrid-webscale-images-11-7-0  11.7.0-
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker
images for 11.7.0
ii  storagegrid-webscale-images-11-8-0  11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale docker images for 11.8.0
ii  storagegrid-webscale-images-11-9-0  11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale docker images for 11.9.0
ii  storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale host services for 11.6.0
ii  storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c
amd64 StorageGRID Webscale host services for 11.7.0
ii  storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale host services for 11.8.0
ii  storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale host services for 11.9.0
root@debian-example:~#
```

2. Entfernen Sie vorherige StorageGRID -Pakete: `dpkg -r images-package service-package`

   > Entfernen Sie nicht die Installationsarchive für die Version von StorageGRID , die Sie derzeit ausführen, oder für die Versionen von StorageGRID , auf die Sie ein Upgrade planen.

   Beispiel:

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. Entfernen Sie StorageGRID Containerbilder.

Docker

1. Erfassen Sie die Liste der installierten Container-Images: `docker images`

   Beispiel:

```
[root@docker-example ~]# docker images
REPOSITORY           TAG            IMAGE ID       CREATED
SIZE
storagegrid-11.9.0   Admin_Node     610f2595bcb4   2 days ago
2.77GB
storagegrid-11.9.0   Storage_Node   7f73d33eb880   2 days ago
2.65GB
storagegrid-11.9.0   API_Gateway    2f0bb79526e9   2 days ago
1.82GB
storagegrid-11.8.0   Storage_Node   7125480de71b   7 months ago
2.54GB
storagegrid-11.8.0   Admin_Node     404e9f1bd173   7 months ago
2.63GB
storagegrid-11.8.0   Archive_Node   c3294a29697c   7 months ago
2.39GB
storagegrid-11.8.0   API_Gateway    1f88f24b9098   7 months ago
1.74GB
storagegrid-11.7.0   Storage_Node   1655350eff6f   16 months ago
2.51GB
storagegrid-11.7.0   Admin_Node     872258dd0dc8   16 months ago
2.48GB
storagegrid-11.7.0   Archive_Node   121e7c8b6d3b   16 months ago
2.41GB
storagegrid-11.7.0   API_Gateway    5b7a26e382de   16 months ago
1.77GB
storagegrid-11.6.0   Admin_Node     ee39f71a73e1   2 years ago
2.38GB
storagegrid-11.6.0   Storage_Node   f5ef895dcad0   2 years ago
2.08GB
storagegrid-11.6.0   Archive_Node   5782de552db0   2 years ago
1.95GB
storagegrid-11.6.0   API_Gateway    cb480ed37eea   2 years ago
1.35GB
[root@docker-example ~]#
```

2. Entfernen Sie die Container-Images für frühere StorageGRID Versionen: `docker rmi image id`

   Entfernen Sie nicht die Container-Images für die Version von StorageGRID , die Sie derzeit ausführen, oder für die Versionen von StorageGRID , auf die Sie ein Upgrade planen.

Beispiel:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051dd
f02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8ccc
afa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66
bde
[root@docker-example ~]#
```

Podman

1. Erfassen Sie die Liste der installierten Container-Images: `podman images`

   Beispiel:

```
[root@podman-example ~]# podman images
REPOSITORY                    TAG           IMAGE ID      CREATED
SIZE
localhost/storagegrid-11.8.0  Storage_Node  7125480de71b  7 months
ago   2.57 GB
localhost/storagegrid-11.8.0  Admin_Node    404e9f1bd173  7 months
ago   2.67 GB
localhost/storagegrid-11.8.0  Archive_Node  c3294a29697c  7 months
ago   2.42 GB
localhost/storagegrid-11.8.0  API_Gateway   1f88f24b9098  7 months
ago   1.77 GB
localhost/storagegrid-11.7.0  Storage_Node  1655350eff6f  16 months
ago  2.54 GB
localhost/storagegrid-11.7.0  Admin_Node    872258dd0dc8  16 months
ago  2.51 GB
localhost/storagegrid-11.7.0  Archive_Node  121e7c8b6d3b  16 months
ago  2.44 GB
localhost/storagegrid-11.7.0  API_Gateway   5b7a26e382de  16 months
ago  1.8 GB
localhost/storagegrid-11.6.0  Admin_Node    ee39f71a73e1  2 years
ago    2.42 GB
localhost/storagegrid-11.6.0  Storage_Node  f5ef895dcad0  2 years
ago    2.11 GB
localhost/storagegrid-11.6.0  Archive_Node  5782de552db0  2 years
ago    1.98 GB
localhost/storagegrid-11.6.0  API_Gateway   cb480ed37eea  2 years
ago    1.38 GB
[root@podman-example ~]#
```

2. Entfernen Sie die Container-Images für frühere StorageGRID Versionen: `podman rmi image id`

> Entfernen Sie nicht die Container-Images für die Version von StorageGRID , die Sie derzeit ausführen, oder für die Versionen von StorageGRID , auf die Sie ein Upgrade planen.

Beispiel:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

Führen Sie das Upgrade durch

Sie können auf StorageGRID 11.9 aktualisieren und gleichzeitig den neuesten Hotfix für diese Version anwenden. Die StorageGRID Upgradeseite bietet den empfohlenen Upgradepfad und verlinkt direkt zu den richtigen Downloadseiten.

Bevor Sie beginnen

Sie haben alle Überlegungen geprüft und alle Planungs- und Vorbereitungsschritte abgeschlossen.

Greifen Sie auf die StorageGRID -Upgrade-Seite zu

Rufen Sie als ersten Schritt die StorageGRID Upgrade-Seite im Grid Manager auf.

Schritte

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Wählen Sie **WARTUNG** > **System** > **Software-Update**.
3. Wählen Sie auf der StorageGRID -Upgrade-Kachel **Upgrade** aus.

Dateien auswählen

Der Aktualisierungspfad auf der StorageGRID -Upgradeseite gibt an, welche Hauptversionen (z. B. 11.9.0) und Hotfixes (z. B. 11.9.0.1) Sie installieren müssen, um die neueste StorageGRID Version zu erhalten. Sie sollten die empfohlenen Versionen und Hotfixes in der angegebenen Reihenfolge installieren.

> Wenn kein Aktualisierungspfad angezeigt wird, kann Ihr Browser möglicherweise nicht auf die NetApp Support-Site zugreifen oder das Kontrollkästchen **Nach Software-Updates suchen** auf der AutoSupport Seite (**SUPPORT** > **Tools** > * AutoSupport* > **Einstellungen**) ist möglicherweise deaktiviert.

Schritte

1. Überprüfen Sie für den Schritt **Dateien auswählen** den Aktualisierungspfad.
2. Wählen Sie im Abschnitt „Dateien herunterladen“ jeden **Download**-Link aus, um die erforderlichen Dateien von der NetApp -Support-Site herunterzuladen.

   Wenn kein Update-Pfad angezeigt wird, gehen Sie zu "NetApp Downloads: StorageGRID" um festzustellen, ob eine neue Version oder ein Hotfix verfügbar ist, und um die benötigten Dateien herunterzuladen.

   > Wenn Sie ein RPM- oder DEB-Paket auf allen Linux-Hosts herunterladen und installieren mussten, sind die StorageGRID Upgrade- und Hotfix-Dateien möglicherweise bereits im Updatepfad aufgeführt.

3. Wählen Sie **Durchsuchen**, um die Versions-Upgrade-Datei auf StorageGRID hochzuladen: `NetApp_StorageGRID_11.9.0_Software_uniqueID.upgrade`

   Wenn der Upload- und Validierungsprozess abgeschlossen ist, wird neben dem Dateinamen ein grünes Häkchen angezeigt.

4. Wenn Sie eine Hotfix-Datei heruntergeladen haben, wählen Sie **Durchsuchen**, um diese Datei hochzuladen. Der Hotfix wird automatisch als Teil des Versions-Upgrades angewendet.
5. Wählen Sie **Weiter**.

Vorprüfungen durchführen

Durch die Ausführung von Vorprüfungen können Sie etwaige Upgrade-Probleme erkennen und beheben, bevor Sie mit der Aktualisierung Ihres Grids beginnen.

Schritte

1. Geben Sie im Schritt **Vorabprüfungen ausführen** zunächst die Bereitstellungspassphrase für Ihr Grid ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.

   Sie sollten die aktuelle Kopie der Wiederherstellungspaketdatei herunterladen, bevor Sie den primären Admin-Knoten aktualisieren. Mit der Wiederherstellungspaketdatei können Sie das System wiederherstellen, wenn ein Fehler auftritt.

3. Wenn die Datei heruntergeladen ist, bestätigen Sie, dass Sie auf die Inhalte zugreifen können, einschließlich der `Passwords.txt` Datei.
4. Kopieren Sie die heruntergeladene Datei(`.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.

5. Wählen Sie **Vorprüfungen ausführen** und warten Sie, bis die Vorprüfungen abgeschlossen sind.
6. Überprüfen Sie die Details für jede gemeldete Vorprüfung und beheben Sie alle gemeldeten Fehler. Siehe die "Lösungshandbuch für StorageGRID -Software-Upgrades" für die StorageGRID Version 11.9.

   Sie müssen alle Vorprüfungsfehler beheben, bevor Sie Ihr System aktualisieren können. Sie müssen jedoch vor dem Upgrade keine Vorabprüfungswarnungen beachten.

   > Wenn Sie benutzerdefinierte Firewall-Ports geöffnet haben, werden Sie während der Vorabprüfung benachrichtigt. Sie müssen sich an den technischen Support wenden, bevor Sie mit dem Upgrade fortfahren.

7. Wenn Sie Konfigurationsänderungen vorgenommen haben, um die gemeldeten Probleme zu beheben, wählen Sie **Vorabprüfungen ausführen** erneut aus, um aktualisierte Ergebnisse zu erhalten.

   Wenn alle Fehler behoben wurden, werden Sie aufgefordert, das Upgrade zu starten.

Starten Sie das Upgrade und aktualisieren Sie den primären Admin-Knoten

Wenn Sie das Upgrade starten, werden die Upgrade-Vorprüfungen erneut ausgeführt und der primäre Admin-Knoten wird automatisch aktualisiert. Dieser Teil des Upgrades kann bis zu 30 Minuten dauern.

> Während der primäre Admin-Knoten aktualisiert wird, können Sie auf keine anderen Grid Manager-Seiten zugreifen. Auch Audit-Protokolle sind nicht verfügbar.

Schritte

1. Wählen Sie **Upgrade starten**.

   Es wird eine Warnung angezeigt, die Sie daran erinnert, dass Sie vorübergehend den Zugriff auf den Grid Manager verlieren.

2. Wählen Sie **OK**, um die Warnung zu bestätigen und das Upgrade zu starten.
3. Warten Sie, bis die Upgrade-Vorprüfungen durchgeführt und der primäre Admin-Knoten aktualisiert wurde.

   Wenn Vorprüfungsfehler gemeldet werden, beheben Sie diese und wählen Sie erneut **Upgrade starten**.

   Wenn das Grid über einen anderen Admin-Knoten verfügt, der online und bereit ist, können Sie ihn verwenden, um den Status des primären Admin-Knotens zu überwachen. Sobald der primäre Admin-Knoten aktualisiert ist, können Sie die anderen Grid-Knoten genehmigen.

4. Wählen Sie bei Bedarf **Weiter** aus, um auf den Schritt **Andere Knoten aktualisieren** zuzugreifen.

Aktualisieren Sie andere Knoten

Sie müssen alle Grid-Knoten aktualisieren, Sie können jedoch mehrere Aktualisierungssitzungen durchführen und die Aktualisierungsreihenfolge anpassen. Beispielsweise möchten Sie möglicherweise die Knoten an Standort A in einer Sitzung aktualisieren und dann die Knoten an Standort B in einer späteren Sitzung aktualisieren. Wenn Sie das Upgrade in mehreren Sitzungen durchführen möchten, beachten Sie, dass Sie die neuen Funktionen erst verwenden können, wenn alle Knoten aktualisiert wurden.

Wenn die Reihenfolge, in der Knoten aktualisiert werden, wichtig ist, genehmigen Sie Knoten oder Knotengruppen einzeln und warten Sie, bis die Aktualisierung auf jedem Knoten abgeschlossen ist, bevor Sie den nächsten Knoten oder die nächste Knotengruppe genehmigen.

Wenn das Upgrade auf einem Grid-Knoten beginnt, werden die Dienste auf diesem Knoten gestoppt. Später wird der Grid-Knoten neu gestartet. Um Dienstunterbrechungen für Clientanwendungen zu vermeiden, die mit dem Knoten kommunizieren, genehmigen Sie das Upgrade für einen Knoten erst, wenn Sie sicher sind, dass der Knoten zum Anhalten und Neustarten bereit ist. Planen Sie bei Bedarf ein Wartungsfenster ein oder benachrichtigen Sie Kunden.

Schritte

1. Überprüfen Sie für den Schritt **Andere Knoten aktualisieren** die Zusammenfassung, die die Startzeit für die gesamte Aktualisierung und den Status für jede größere Aktualisierungsaufgabe angibt.
   - **Upgrade-Dienst starten** ist die erste Upgrade-Aufgabe. Während dieser Aufgabe wird die Softwaredatei an die Grid-Knoten verteilt und der Upgrade-Dienst auf jedem Knoten gestartet.
   - Wenn die Aufgabe **Upgradedienst starten** abgeschlossen ist, wird die Aufgabe **Andere Grid-Knoten aktualisieren** gestartet und Sie werden aufgefordert, eine neue Kopie des Wiederherstellungspakets herunterzuladen.
2. Geben Sie bei entsprechender Aufforderung Ihre Bereitstellungspassphrase ein und laden Sie eine neue Kopie des Wiederherstellungspakets herunter.

   Sie sollten eine neue Kopie der Wiederherstellungspaketdatei herunterladen, nachdem der primäre Admin-Knoten aktualisiert wurde. Mit der Wiederherstellungspaketdatei können Sie das System wiederherstellen, wenn ein Fehler auftritt.

3. Überprüfen Sie die Statustabellen für jeden Knotentyp. Es gibt Tabellen für nicht primäre Admin-Knoten, Gateway-Knoten und Speicherknoten.

   Ein Rasterknoten kann sich in einer der folgenden Phasen befinden, wenn die Tabellen zum ersten Mal angezeigt werden:

- Auspacken des Upgrades
- Herunterladen
- Warten auf die Genehmigung

4. Wenn Sie bereit sind, Grid-Knoten für das Upgrade auszuwählen (oder wenn Sie die Genehmigung ausgewählter Knoten aufheben müssen), befolgen Sie diese Anweisungen:

Aufgabe	Anweisung
Suchen Sie nach bestimmten Knoten, die Sie genehmigen möchten, z. B. alle Knoten an einem bestimmten Standort.	Geben Sie den Suchbegriff in das Feld **Suchen** ein
Alle Knoten für das Upgrade auswählen	Wählen Sie **Alle Knoten genehmigen**
Wählen Sie alle Knoten desselben Typs für das Upgrade aus (z. B. alle Speicherknoten).	Wählen Sie die Schaltfläche **Alle genehmigen** für den Knotentyp Wenn Sie mehr als einen Knoten desselben Typs genehmigen, werden die Knoten einzeln aktualisiert.
Wählen Sie einen einzelnen Knoten für das Upgrade aus	Wählen Sie die Schaltfläche **Genehmigen** für den Knoten
Verschieben Sie das Upgrade auf allen ausgewählten Knoten	Wählen Sie **Alle Knoten nicht genehmigen**
Verschieben Sie das Upgrade auf allen ausgewählten Knoten desselben Typs	Wählen Sie die Schaltfläche **Alle nicht genehmigen** für den Knotentyp
Verschieben des Upgrades auf einem einzelnen Knoten	Wählen Sie die Schaltfläche **Nicht genehmigen** für den Knoten

5. Warten Sie, bis die genehmigten Knoten diese Upgradephasen durchlaufen haben:
   - Genehmigt und wartet auf ein Upgrade
   - Dienste beenden

     Sie können einen Knoten nicht entfernen, wenn sein Stadium den Status **Dienste werden beendet** erreicht. Die Schaltfläche **Nicht genehmigen** ist deaktiviert.

   - Container stoppen
   - Docker-Images bereinigen
   - Upgrade der Basis-Betriebssystempakete

Wenn ein Appliance-Knoten dieses Stadium erreicht, wird die StorageGRID Appliance Installer-Software auf der Appliance aktualisiert. Dieser automatisierte Prozess stellt sicher, dass die Version des StorageGRID Appliance Installer mit der StorageGRID -Softwareversion synchronisiert bleibt.

- Neustart

Einige Gerätemodelle werden möglicherweise mehrmals neu gestartet, um die Firmware und das BIOS zu aktualisieren.

- Ausführen von Schritten nach dem Neustart
- Starten von Diensten
- Erledigt

6. Wiederholen Sie dieGenehmigungsschritt so oft wie nötig, bis alle Grid-Knoten aktualisiert wurden.

Komplettes Upgrade

Wenn alle Grid-Knoten die Upgrade-Phasen abgeschlossen haben, wird die Aufgabe **Andere Grid-Knoten aktualisieren** als Abgeschlossen angezeigt. Die restlichen Upgrade-Aufgaben werden automatisch im Hintergrund ausgeführt.

Schritte

1. Sobald die Aufgabe **Funktionen aktivieren** abgeschlossen ist (was schnell geht), können Sie mit der Verwendung der"neue Funktionen" in der aktualisierten StorageGRID -Version.
2. Während der Aufgabe **Datenbank aktualisieren** überprüft der Aktualisierungsprozess jeden Knoten, um sicherzustellen, dass die Cassandra-Datenbank nicht aktualisiert werden muss.

Das Upgrade von StorageGRID 11.8 auf 11.9 erfordert kein Upgrade der Cassandra-Datenbank. Der Cassandra-Dienst wird jedoch auf jedem Speicherknoten gestoppt und neu gestartet. Bei zukünftigen StorageGRID Funktionsversionen kann die Aktualisierung der Cassandra-Datenbank mehrere Tage dauern.

3. Wenn die Aufgabe **Datenbank-Upgrade** abgeschlossen ist, warten Sie einige Minuten, bis die **Letzten Upgrade-Schritte** abgeschlossen sind.
4. Wenn die **letzten Upgrade-Schritte** abgeschlossen sind, ist das Upgrade abgeschlossen. Der erste Schritt „Dateien auswählen“ wird erneut mit einem grünen Erfolgsbanner angezeigt.
5. Überprüfen Sie, ob der Netzbetrieb wieder normal läuft:
   a. Überprüfen Sie, ob die Dienste normal funktionieren und keine unerwarteten Warnungen auftreten.
   b. Bestätigen Sie, dass die Clientverbindungen zum StorageGRID -System wie erwartet funktionieren.

Beheben von Upgradeproblemen

Wenn bei der Durchführung eines Upgrades etwas schief geht, können Sie das Problem möglicherweise selbst beheben. Wenn Sie ein Problem nicht lösen können, sammeln Sie so viele Informationen wie möglich und wenden Sie sich dann an den technischen Support.

Das Upgrade wird nicht abgeschlossen

In den folgenden Abschnitten wird beschrieben, wie Sie Situationen wiederherstellen, in denen das Upgrade teilweise fehlgeschlagen ist.

Upgrade-Vorabprüfungsfehler

Um Probleme zu erkennen und zu beheben, können Sie die Upgrade-Vorprüfungen manuell ausführen, bevor Sie mit dem eigentlichen Upgrade beginnen. Die meisten Vorprüfungsfehler enthalten Informationen zur Lösung des Problems.

Bereitstellungsfehler

Wenn der automatische Bereitstellungsprozess fehlschlägt, wenden Sie sich an den technischen Support.

Grid-Knoten stürzt ab oder kann nicht gestartet werden

Wenn ein Grid-Knoten während des Upgrade-Vorgangs abstürzt oder nach Abschluss des Upgrades nicht erfolgreich gestartet werden kann, wenden Sie sich an den technischen Support, um die zugrunde liegenden Probleme zu untersuchen und zu beheben.

Die Aufnahme oder der Datenabruf wird unterbrochen

Wenn die Datenaufnahme oder der Datenabruf unerwartet unterbrochen wird, während Sie keinen Grid-Knoten aktualisieren, wenden Sie sich an den technischen Support.

Datenbank-Upgradefehler

Wenn das Datenbank-Upgrade mit einem Fehler fehlschlägt, versuchen Sie es erneut. Wenn es erneut fehlschlägt, wenden Sie sich an den technischen Support.

Ähnliche Informationen

"Überprüfen des Systemzustands vor dem Upgrade der Software"

Probleme mit der Benutzeroberfläche

Während oder nach dem Upgrade können Probleme mit dem Grid Manager oder dem Tenant Manager auftreten.

Grid Manager zeigt während des Upgrades mehrere Fehlermeldungen an

Wenn Sie Ihren Browser aktualisieren oder zu einer anderen Grid Manager-Seite navigieren, während der primäre Admin-Knoten aktualisiert wird, werden möglicherweise mehrere Meldungen „503: Dienst nicht verfügbar“ und „Problem beim Verbinden mit dem Server“ angezeigt. Sie können diese Meldungen getrost ignorieren. Sie werden nicht mehr angezeigt, sobald der Knoten aktualisiert ist.

Wenn diese Meldungen nach dem Start des Upgrades länger als eine Stunde angezeigt werden, ist möglicherweise etwas passiert, das das Upgrade des primären Admin-Knotens verhindert hat. Wenn Sie das Problem nicht selbst lösen können, wenden Sie sich an den technischen Support.

Die Weboberfläche reagiert nicht wie erwartet

Der Grid Manager oder der Tenant Manager reagiert nach der Aktualisierung der StorageGRID -Software möglicherweise nicht wie erwartet.

Wenn Sie Probleme mit der Weboberfläche haben:

- Stellen Sie sicher, dass Sie ein"unterstützter Webbrowser" .

  Die Browserunterstützung ändert sich normalerweise für jede StorageGRID Version.

- Leeren Sie den Cache Ihres Webbrowsers.

  Durch das Leeren des Caches werden veraltete Ressourcen entfernt, die von der vorherigen Version der StorageGRID -Software verwendet wurden, und die Benutzeroberfläche kann wieder ordnungsgemäß funktionieren. Anweisungen finden Sie in der Dokumentation Ihres Webbrowsers.

Fehlermeldungen zur Überprüfung der Verfügbarkeit von Docker-Images

Beim Versuch, den Upgrade-Vorgang zu starten, erhalten Sie möglicherweise die Fehlermeldung „Die folgenden Probleme wurden von der Validierungssuite zur Überprüfung der Verfügbarkeit von Docker-Images festgestellt.“ Alle Probleme müssen gelöst werden, bevor Sie das Upgrade abschließen können.

Wenden Sie sich an den technischen Support, wenn Sie sich nicht sicher sind, welche Änderungen zur Lösung der festgestellten Probleme erforderlich sind.

Nachricht	Ursache	Lösung
Die Upgrade-Version konnte nicht ermittelt werden. Upgrade-Versionsinformationsdatei `{file_path}` entsprach nicht dem erwarteten Format.	Das Upgrade-Paket ist beschädigt.	Laden Sie das Upgrade-Paket erneut hoch und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
Upgrade-Versionsinformationsdatei `{file_path}` wurde nicht gefunden. Die Upgrade-Version konnte nicht ermittelt werden.	Das Upgrade-Paket ist beschädigt.	Laden Sie das Upgrade-Paket erneut hoch und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
Die aktuell installierte Release-Version kann nicht ermittelt werden auf `{node_name}` .	Eine wichtige Datei auf dem Knoten ist beschädigt.	Wenden Sie sich an den technischen Support.
Verbindungsfehler beim Versuch, Versionen aufzulisten auf `{node_name}`	Der Knoten ist offline oder die Verbindung wurde unterbrochen.	Stellen Sie sicher, dass alle Knoten online und vom primären Admin-Knoten aus erreichbar sind, und versuchen Sie es erneut.

Nachricht	Ursache	Lösung
Der Host für den Knoten `{node_name}` hat kein StorageGRID `{upgrade_version}` Bild geladen. Bilder und Dienste müssen auf dem Host installiert werden, bevor das Upgrade fortgesetzt werden kann.	Die RPM- oder DEB-Pakete für das Upgrade wurden nicht auf dem Host installiert, auf dem der Knoten ausgeführt wird, oder die Images werden noch importiert. **Hinweis:** Dieser Fehler betrifft nur Knoten, die als Container unter Linux ausgeführt werden.	Stellen Sie sicher, dass die RPM- oder DEB-Pakete auf allen Linux-Hosts installiert wurden, auf denen Knoten ausgeführt werden. Stellen Sie sicher, dass die Version sowohl für den Dienst als auch für die Bilddatei korrekt ist. Warten Sie einige Minuten und versuchen Sie es erneut. Sehen "Linux: Installieren Sie das RPM- oder DEB-Paket auf allen Hosts" .
Fehler beim Überprüfen des Knotens `{node_name}`	Ein unerwarteter Fehler ist aufgetreten.	Warten Sie einige Minuten und versuchen Sie es erneut.
Beim Ausführen der Vorprüfungen ist ein nicht abgefangener Fehler aufgetreten. `{error_string}`	Ein unerwarteter Fehler ist aufgetreten.	Warten Sie einige Minuten und versuchen Sie es erneut.

StorageGRID Hotfix anwenden

StorageGRID Hotfix-Verfahren

Möglicherweise müssen Sie einen Hotfix auf Ihr StorageGRID -System anwenden, wenn zwischen den Funktionsversionen Probleme mit der Software erkannt und behoben werden.

StorageGRID -Hotfixes enthalten Softwareänderungen, die außerhalb einer Funktions- oder Patch-Version verfügbar gemacht werden. Dieselben Änderungen sind in einer zukünftigen Version enthalten. Darüber hinaus enthält jede Hotfix-Version eine Zusammenfassung aller vorherigen Hotfixes innerhalb der Funktions- oder Patch-Version.

Überlegungen zum Anwenden eines Hotfixes

Sie können keinen StorageGRID Hotfix anwenden, wenn ein anderer Wartungsvorgang ausgeführt wird. Beispielsweise können Sie keinen Hotfix anwenden, während ein Außerbetriebnahme-, Erweiterungs- oder Wiederherstellungsverfahren ausgeführt wird.

> Wenn die Außerbetriebnahme eines Knotens oder einer Site angehalten wird, können Sie problemlos einen Hotfix anwenden. Darüber hinaus können Sie möglicherweise in den letzten Phasen eines StorageGRID Upgradevorgangs einen Hotfix anwenden. Weitere Informationen finden Sie in den Anweisungen zum Upgrade der StorageGRID -Software.

Nachdem Sie den Hotfix im Grid Manager hochgeladen haben, wird der Hotfix automatisch auf den primären Admin-Knoten angewendet. Anschließend können Sie die Anwendung des Hotfixes auf die restlichen Knoten in Ihrem StorageGRID -System genehmigen.

Wenn die Anwendung eines Hotfixes auf einen oder mehrere Knoten fehlschlägt, wird der Grund für den Fehler in der Spalte „Details“ der Hotfix-Fortschrittstabelle angezeigt. Sie müssen alle Probleme beheben, die die Fehler verursacht haben, und dann den gesamten Vorgang wiederholen. Knoten, bei denen der Hotfix zuvor erfolgreich angewendet wurde, werden bei nachfolgenden Anwendungen übersprungen. Sie können den Hotfix-Vorgang beliebig oft wiederholen, bis alle Knoten aktualisiert wurden. Damit die Anwendung vollständig ist, muss der Hotfix auf allen Grid-Knoten erfolgreich installiert werden.

Während Grid-Knoten mit der neuen Hotfix-Version aktualisiert werden, wirken sich die tatsächlichen Änderungen in einem Hotfix möglicherweise nur auf bestimmte Dienste auf bestimmten Knotentypen aus. Beispielsweise könnte ein Hotfix nur den LDR-Dienst auf Speicherknoten betreffen.

So werden Hotfixes zur Wiederherstellung und Erweiterung angewendet

Nachdem ein Hotfix auf Ihr Grid angewendet wurde, installiert der primäre Admin-Knoten automatisch dieselbe Hotfix-Version auf allen Knoten, die durch Wiederherstellungsvorgänge wiederhergestellt oder in einer Erweiterung hinzugefügt wurden.

Wenn Sie jedoch den primären Admin-Knoten wiederherstellen müssen, müssen Sie die richtige StorageGRID Version manuell installieren und dann den Hotfix anwenden. Die endgültige StorageGRID -Version des primären Admin-Knotens muss mit der Version der anderen Knoten im Grid übereinstimmen.

Das folgende Beispiel veranschaulicht, wie beim Wiederherstellen des primären Admin-Knotens ein Hotfix angewendet wird:

1. Angenommen, das Grid führt eine StorageGRID 11.*A.B*-Version mit dem neuesten Hotfix aus. Die „Gitterversion“ ist 11.*A.B.y*.
2. Der primäre Admin-Knoten fällt aus.
3. Sie stellen den primären Admin-Knoten mit StorageGRID 11.*A.B* erneut bereit und führen das Wiederherstellungsverfahren durch.

   > Um die Übereinstimmung mit der Grid-Version zu gewährleisten, können Sie beim Bereitstellen des Knotens eine Nebenversion verwenden. Sie müssen nicht zuerst die Hauptversion bereitstellen.

4. Anschließend wenden Sie Hotfix 11.*A.B.y* auf den primären Admin-Knoten an.

Weitere Informationen finden Sie unter "Konfigurieren Sie den Ersatz-Primäradministratorknoten" .

Auswirkungen auf Ihr System bei der Anwendung eines Hotfixes

Sie müssen verstehen, welche Auswirkungen die Anwendung eines Hotfixes auf Ihr StorageGRID -System hat.

StorageGRID -Hotfixes sind unterbrechungsfrei

Das StorageGRID -System kann während des gesamten Hotfix-Prozesses Daten von Client-Anwendungen aufnehmen und abrufen. Wenn Sie für alle Knoten desselben Typs (z. B. Speicherknoten) ein Hotfix genehmigen, werden die Knoten einzeln heruntergefahren, sodass es nicht vorkommt, dass alle Grid-Knoten oder alle Grid-Knoten eines bestimmten Typs nicht verfügbar sind.

Um eine kontinuierliche Verfügbarkeit zu gewährleisten, stellen Sie sicher, dass Ihre ILM-Richtlinie Regeln enthält, die das Speichern mehrerer Kopien jedes Objekts vorschreiben. Sie müssen außerdem sicherstellen, dass alle externen S3-Clients so konfiguriert sind, dass sie Anfragen an eines der folgenden Elemente senden:

- Eine virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe (HA)
- Ein hochverfügbarer Load Balancer eines Drittanbieters
- Mehrere Gateway-Knoten für jeden Client
- Mehrere Speicherknoten für jeden Client

Bei Clientanwendungen kann es zu kurzfristigen Störungen kommen

Das StorageGRID -System kann während des gesamten Hotfix-Prozesses Daten von Client-Anwendungen aufnehmen und abrufen. Allerdings können Client-Verbindungen zu einzelnen Gateway-Knoten oder Speicherknoten vorübergehend unterbrochen werden, wenn der Hotfix einen Neustart der Dienste auf diesen Knoten erfordert. Die Konnektivität wird wiederhergestellt, nachdem der Hotfix-Prozess abgeschlossen ist und die Dienste auf den einzelnen Knoten wieder aufgenommen werden.

Wenn ein kurzzeitiger Verbindungsverlust nicht akzeptabel ist, müssen Sie möglicherweise eine Ausfallzeit einplanen, um einen Hotfix anzuwenden. Mithilfe der selektiven Genehmigung können Sie planen, wann bestimmte Knoten aktualisiert werden.

> Sie können mehrere Gateways und Hochverfügbarkeitsgruppen (HA) verwenden, um während des Hotfix-Prozesses ein automatisches Failover bereitzustellen. Siehe die Anweisungen für"Konfigurieren von Hochverfügbarkeitsgruppen" .

Es können Warnungen und SNMP-Benachrichtigungen ausgelöst werden

Warnungen und SNMP-Benachrichtigungen können ausgelöst werden, wenn Dienste neu gestartet werden und wenn das StorageGRID -System als Umgebung mit gemischten Versionen betrieben wird (einige Grid-Knoten führen eine frühere Version aus, während andere auf eine neuere Version aktualisiert wurden). Im Allgemeinen werden diese Warnungen und Benachrichtigungen gelöscht, wenn der Hotfix abgeschlossen ist.

Konfigurationsänderungen sind eingeschränkt

Beim Anwenden eines Hotfixes auf StorageGRID:

- Nehmen Sie keine Änderungen an der Grid-Konfiguration vor (z. B. Festlegen von Grid-Netzwerk-Subnetzen oder Genehmigen ausstehender Grid-Knoten), bis der Hotfix auf alle Knoten angewendet wurde.
- Aktualisieren Sie die ILM-Konfiguration erst, wenn der Hotfix auf allen Knoten angewendet wurde.

Besorgen Sie sich die erforderlichen Materialien für den Hotfix

Bevor Sie einen Hotfix anwenden, müssen Sie alle erforderlichen Materialien besorgen.

Artikel	Hinweise
StorageGRID -Hotfixdatei	Sie müssen die StorageGRID Hotfixdatei herunterladen.
• Netzwerkanschluss • "Unterstützte Webbrowser" • SSH-Client (z. B. PuTTY)	

Artikel	Hinweise
Wiederherstellungspaket(`.zip`) Datei	Bevor Sie einen Hotfix anwenden,"Laden Sie die neueste Wiederherstellungspaketdatei herunter" falls während des Hotfixes Probleme auftreten. Laden Sie anschließend nach der Anwendung des Hotfixes eine neue Kopie der Wiederherstellungspaketdatei herunter und speichern Sie sie an einem sicheren Ort. Mit der aktualisierten Wiederherstellungspaketdatei können Sie das System wiederherstellen, wenn ein Fehler auftritt.
Passwords.txt-Datei	Optional und nur verwendet, wenn Sie einen Hotfix manuell mithilfe des SSH-Clients anwenden. Der `Passwords.txt` Datei ist Teil des Wiederherstellungspakets `.zip` Datei.
Bereitstellungspassphrase	Die Passphrase wird bei der Erstinstallation des StorageGRID -Systems erstellt und dokumentiert. Die Bereitstellungspassphrase ist nicht aufgeführt in der `Passwords.txt` Datei.
Zugehörige Dokumentation	`readme.txt`Datei für den Hotfix. Diese Datei ist auf der Hotfix-Downloadseite enthalten. Lesen Sie unbedingt die `readme` Überprüfen Sie die Datei sorgfältig, bevor Sie den Hotfix anwenden.

Hotfix-Datei herunterladen

Sie müssen die Hotfixdatei herunterladen, bevor Sie den Hotfix anwenden können.

Schritte

1. Gehe zu "NetApp Downloads: StorageGRID" .
2. Wählen Sie den Abwärtspfeil unter **Verfügbare Software** aus, um eine Liste der zum Download verfügbaren Hotfixes anzuzeigen.

   Hotfix-Dateiversionen haben die Form: 11.4.*x.y*.

3. Überprüfen Sie die im Update enthaltenen Änderungen.

   Wenn Sie gerade"den primären Admin-Knoten wiederhergestellt" und Sie einen Hotfix anwenden müssen, wählen Sie dieselbe Hotfixversion aus, die auf den anderen Grid-Knoten installiert ist.

   a. Wählen Sie die Hotfix-Version aus, die Sie herunterladen möchten, und wählen Sie **Los**.
   b. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Ihr NetApp -Konto an .
   c. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.

      Die Downloadseite für die von Ihnen ausgewählte Version wird angezeigt.

   d. Herunterladen des Hotfixes `readme.txt` Datei, um eine Zusammenfassung der im Hotfix enthaltenen Änderungen anzuzeigen.

4. Wählen Sie die Download-Schaltfläche für den Hotfix und speichern Sie die Datei.

   Ändern Sie den Namen dieser Datei nicht.

   Wenn Sie ein macOS-Gerät verwenden, wird die Hotfix-Datei möglicherweise automatisch als `.txt` Datei. Wenn dies der Fall ist, müssen Sie die Datei umbenennen, ohne `.txt` Verlängerung.

5. Wählen Sie einen Speicherort für den Download und wählen Sie **Speichern**.

Überprüfen Sie den Systemzustand, bevor Sie den Hotfix anwenden

Sie müssen überprüfen, ob das System für die Aufnahme des Hotfixes bereit ist.

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Stellen Sie nach Möglichkeit sicher, dass das System normal läuft und alle Netzknoten mit dem Netz verbunden sind.

   Verbundene Knoten haben grüne Häkchen auf der Seite „Knoten“.

3. Suchen Sie nach aktuellen Warnungen und beheben Sie diese, wenn möglich.
4. Stellen Sie sicher, dass keine anderen Wartungsvorgänge ausgeführt werden, beispielsweise ein Upgrade, eine Wiederherstellung, eine Erweiterung oder eine Außerbetriebnahme.

   Sie sollten warten, bis alle aktiven Wartungsvorgänge abgeschlossen sind, bevor Sie einen Hotfix anwenden.

   Sie können keinen StorageGRID Hotfix anwenden, wenn ein anderer Wartungsvorgang ausgeführt wird. Beispielsweise können Sie keinen Hotfix anwenden, während ein Außerbetriebnahme-, Erweiterungs- oder Wiederherstellungsverfahren ausgeführt wird.

   Wenn ein Knoten oder eine Site"Stilllegungsverfahren ist ausgesetzt" , können Sie bedenkenlos einen Hotfix anwenden. Darüber hinaus können Sie möglicherweise in den letzten Phasen eines StorageGRID Upgradevorgangs einen Hotfix anwenden. Siehe die Anweisungen für"Aktualisierung der StorageGRID -Software" .

Hotfix anwenden

Der Hotfix wird zunächst automatisch auf den primären Admin-Knoten angewendet. Anschließend müssen Sie die Anwendung des Hotfixes auf andere Grid-Knoten genehmigen, bis auf allen Knoten dieselbe Softwareversion ausgeführt wird. Sie können die Genehmigungssequenz anpassen, indem Sie einzelne Rasterknoten, Gruppen von Rasterknoten oder alle Rasterknoten genehmigen.

Bevor Sie beginnen

- Sie haben die"Überlegungen zur Anwendung eines Hotfixes" .
- Sie haben die Bereitstellungspassphrase.
- Sie verfügen über Root-Zugriff oder die Berechtigung zur Wartung.

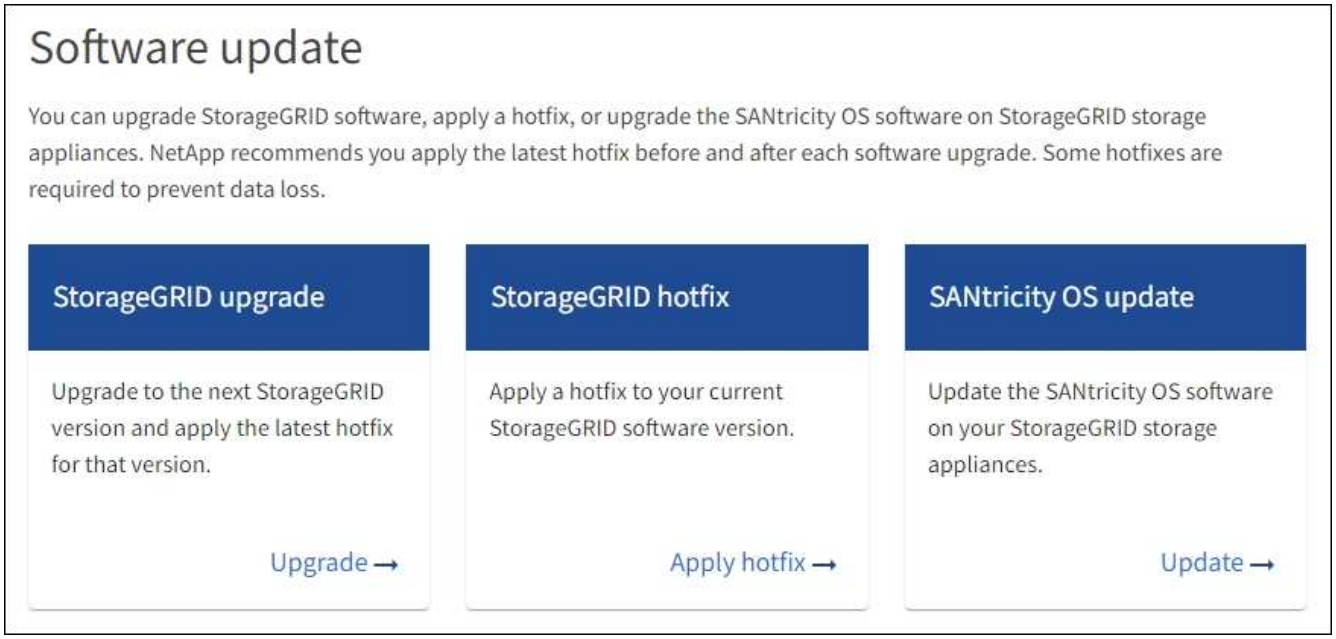
Informationen zu diesem Vorgang

- Sie können die Anwendung eines Hotfixes auf einen Knoten verzögern, der Hotfix-Prozess ist jedoch erst abgeschlossen, wenn Sie den Hotfix auf allen Knoten angewendet haben.
- Sie können kein StorageGRID -Software-Upgrade oder SANtricity OS-Update durchführen, bis Sie den Hotfix-Prozess abgeschlossen haben.

Schritte

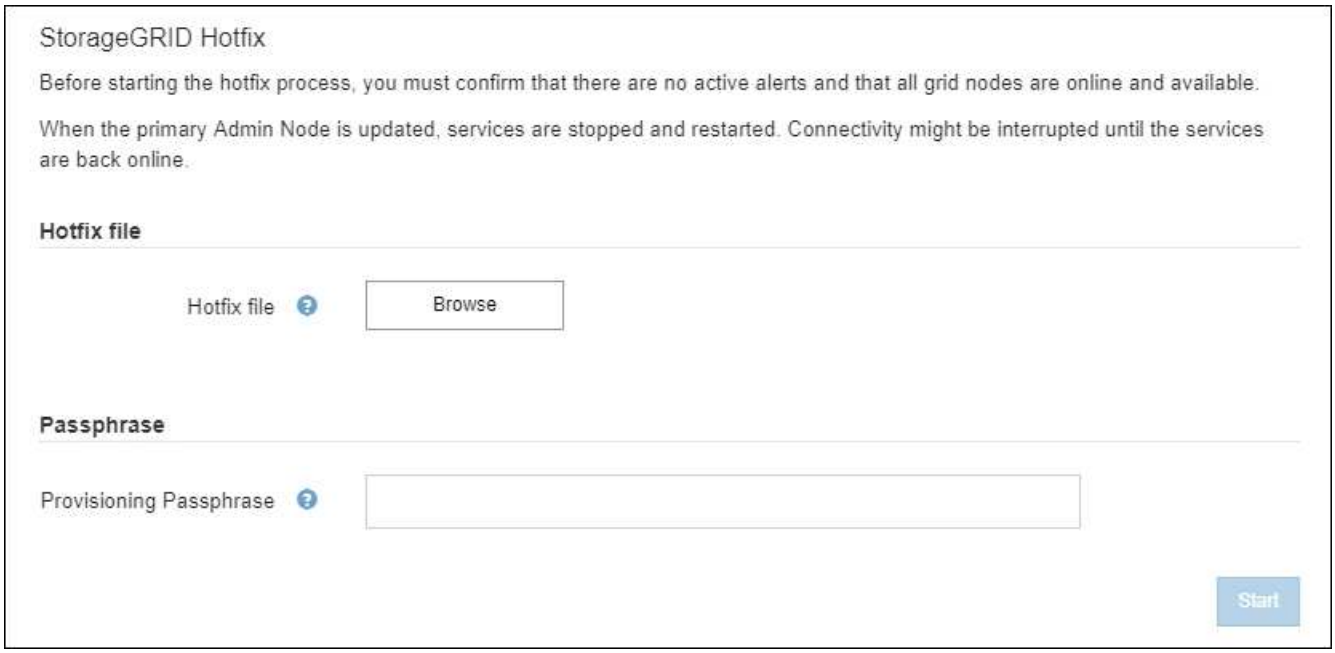
1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Wählen Sie **WARTUNG** > **System** > **Software-Update**.

   Die Seite „Softwareaktualisierung“ wird angezeigt.



3. Wählen Sie **Hotfix anwenden**.

   Die StorageGRID Hotfix-Seite wird angezeigt.



4. Wählen Sie die Hotfix-Datei aus, die Sie von der NetApp Support-Site heruntergeladen haben.

   a. Wählen Sie **Durchsuchen**.

   b. Suchen und wählen Sie die Datei aus.

      `hotfix-install-version`

   c. Wählen Sie **Öffnen**.

      Die Datei wird hochgeladen. Wenn der Upload abgeschlossen ist, wird der Dateiname im Feld „Details“ angezeigt.

      Ändern Sie den Dateinamen nicht, da dies Teil des Überprüfungsprozesses ist.

5. Geben Sie die Bereitstellungspassphrase in das Textfeld ein.

   Die Schaltfläche **Start** wird aktiviert.

6. Wählen Sie **Start**.

   Es wird eine Warnung angezeigt, dass die Verbindung Ihres Browsers möglicherweise vorübergehend verloren geht, da die Dienste auf dem primären Admin-Knoten neu gestartet werden.

7. Wählen Sie **OK**, um mit der Anwendung des Hotfixes auf den primären Admin-Knoten zu beginnen.

   Wenn der Hotfix startet:

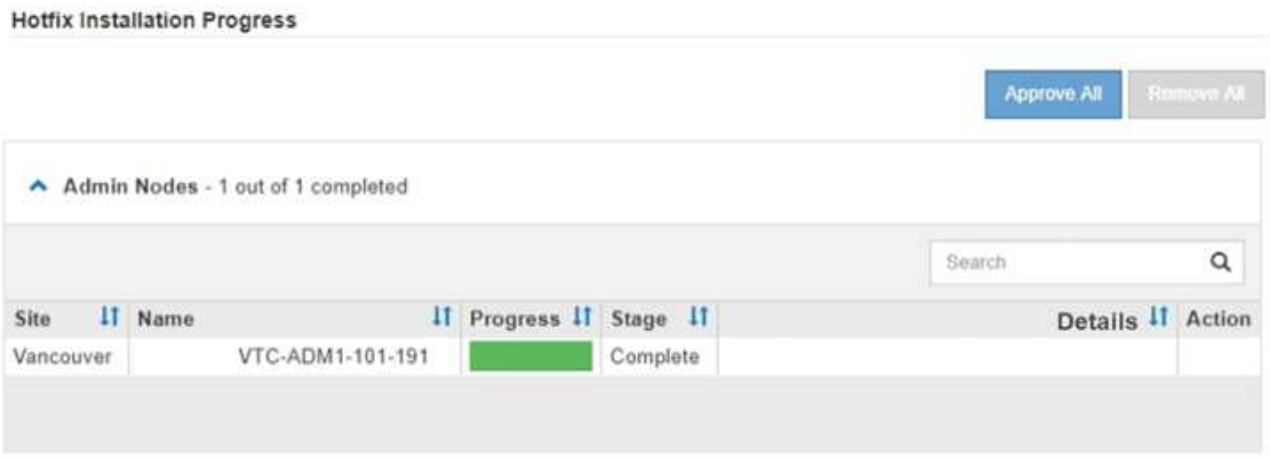
   a. Die Hotfix-Validierungen werden ausgeführt.

      Wenn Fehler gemeldet werden, beheben Sie diese, laden Sie die Hotfix-Datei erneut hoch und wählen Sie erneut **Start**.

   b. Die Fortschrittstabelle für die Hotfix-Installation wird angezeigt.

Diese Tabelle zeigt alle Knoten in Ihrem Raster und den aktuellen Status der Hotfix-Installation für jeden Knoten. Die Knoten in der Tabelle sind nach Typ gruppiert (Admin-Knoten, Gateway-Knoten und Speicherknoten).

c. Der Fortschrittsbalken zeigt den Abschluss an und dann wird für den primären Admin-Knoten „Abgeschlossen“ angezeigt.



8. Sortieren Sie die Knotenlisten in jeder Gruppierung optional in aufsteigender oder absteigender Reihenfolge nach **Site**, **Name**, **Fortschritt**, **Phase** oder **Details**. Oder geben Sie einen Begriff in das Feld **Suchen** ein, um nach bestimmten Knoten zu suchen.
9. Genehmigen Sie die Rasterknoten, die zur Aktualisierung bereit sind. Genehmigte Knoten desselben Typs werden einzeln aktualisiert.

> Genehmigen Sie den Hotfix für einen Knoten nicht, es sei denn, Sie sind sicher, dass der Knoten zur Aktualisierung bereit ist. Wenn der Hotfix auf einen Grid-Knoten angewendet wird, werden einige Dienste auf diesem Knoten möglicherweise neu gestartet. Diese Vorgänge können zu Dienstunterbrechungen für Clients führen, die mit dem Knoten kommunizieren.

- Wählen Sie eine oder mehrere Schaltflächen „Genehmigen“ aus, um einen oder mehrere einzelne Knoten zur Hotfix-Warteschlange hinzuzufügen.
- Wählen Sie innerhalb jeder Gruppierung die Schaltfläche **Alle genehmigen** aus, um alle Knoten desselben Typs zur Hotfix-Warteschlange hinzuzufügen. Wenn Sie Suchkriterien in das Feld **Suchen** eingegeben haben, gilt die Schaltfläche **Alle genehmigen** für alle Knoten, die durch die Suchkriterien ausgewählt wurden.

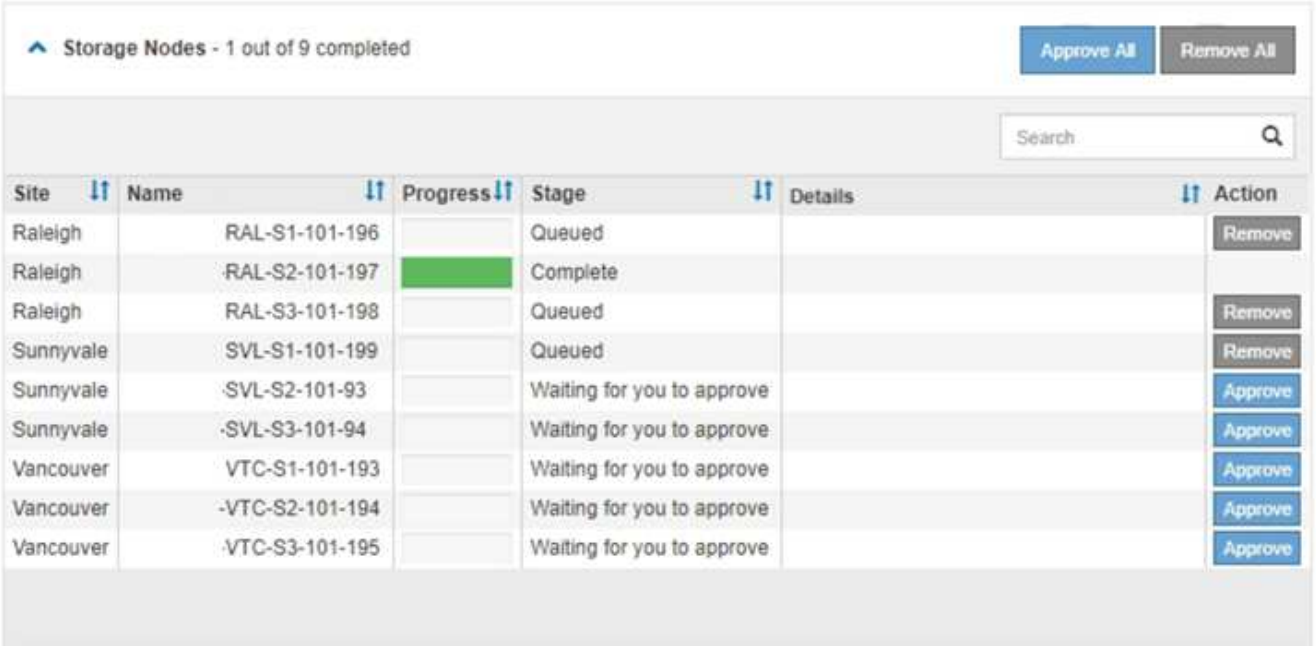
> Mit der Schaltfläche **Alle genehmigen** oben auf der Seite werden alle auf der Seite aufgelisteten Knoten genehmigt, während mit der Schaltfläche **Alle genehmigen** oben in einer Tabellengruppierung nur alle Knoten in dieser Gruppe genehmigt werden. Wenn die Reihenfolge, in der Knoten aktualisiert werden, wichtig ist, genehmigen Sie Knoten oder Knotengruppen einzeln und warten Sie, bis die Aktualisierung auf jedem Knoten abgeschlossen ist, bevor Sie den/die nächsten Knoten genehmigen.

- Wählen Sie oben auf der Seite die Schaltfläche **Alle genehmigen** auf oberster Ebene aus, um alle Knoten im Raster zur Hotfix-Warteschlange hinzuzufügen.

Sie müssen den StorageGRID Hotfix abschließen, bevor Sie ein anderes Softwareupdate starten können. Wenn Sie den Hotfix nicht abschließen können, wenden Sie sich an den technischen Support.

- Wählen Sie **Entfernen** oder **Alle entfernen**, um einen oder alle Knoten aus der Hotfix-Warteschlange zu entfernen.

  Wenn die Phase über „In der Warteschlange“ hinaus fortschreitet, wird die Schaltfläche **Entfernen** ausgeblendet und Sie können den Knoten nicht mehr aus dem Hotfix-Prozess entfernen.



10. Warten Sie, während der Hotfix auf jeden genehmigten Grid-Knoten angewendet wird.

    Wenn der Hotfix erfolgreich auf allen Knoten installiert wurde, wird die Tabelle „Hotfix-Installationsfortschritt“ geschlossen. Ein grünes Banner zeigt das Datum und die Uhrzeit der Fertigstellung des Hotfixes an.

11. Wenn der Hotfix auf keinem Knoten angewendet werden konnte, überprüfen Sie den Fehler für jeden Knoten, beheben Sie das Problem und wiederholen Sie diese Schritte.

    Der Vorgang ist erst abgeschlossen, wenn der Hotfix erfolgreich auf allen Knoten angewendet wurde. Sie können den Hotfix-Vorgang beliebig oft wiederholen, bis er abgeschlossen ist.

Konfigurieren und Verwalten eines StorageGRID -Systems

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

Browserbreite	Pixel
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.

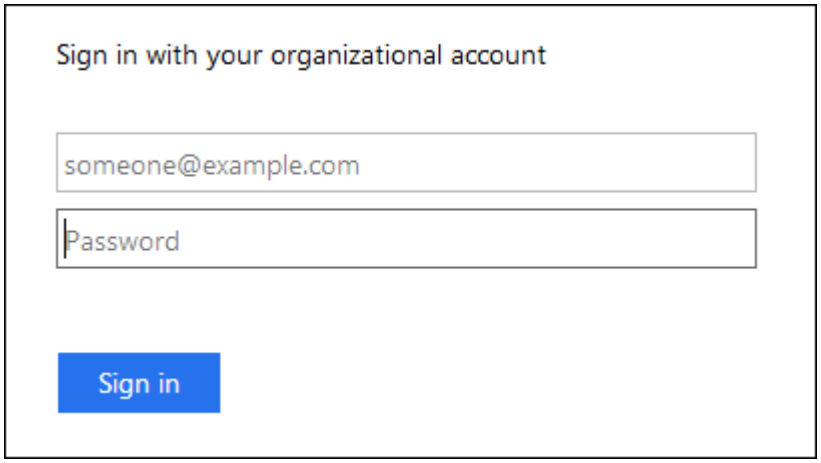
b. Wählen Sie **Anmelden**.

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:



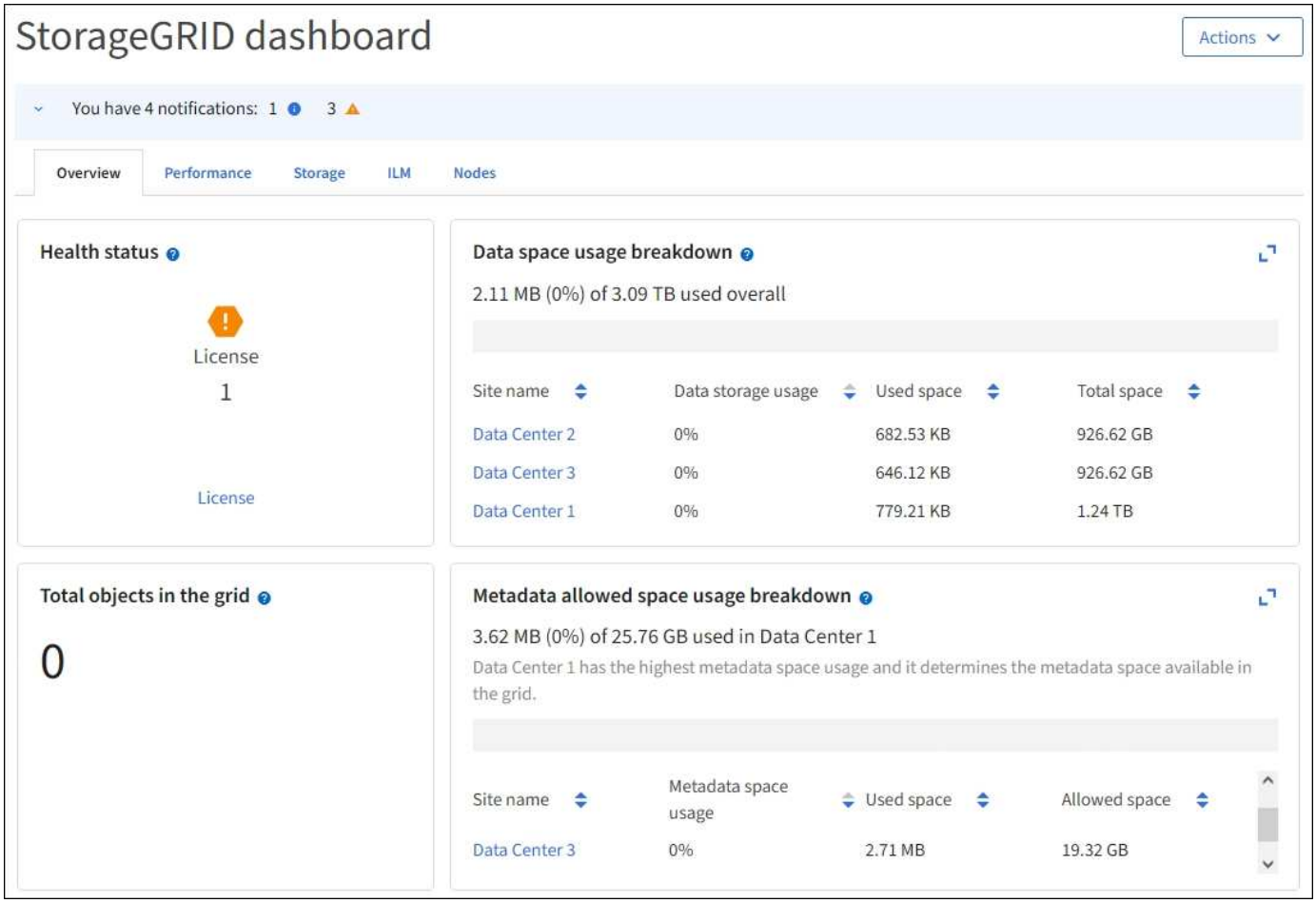
- Wenn StorageGRID SSO verwendet und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:

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

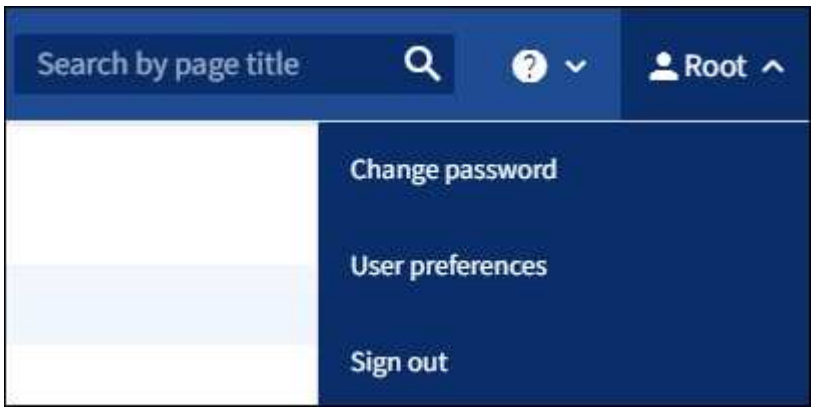
1. Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers ein.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldeinformationen erneut ein.

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

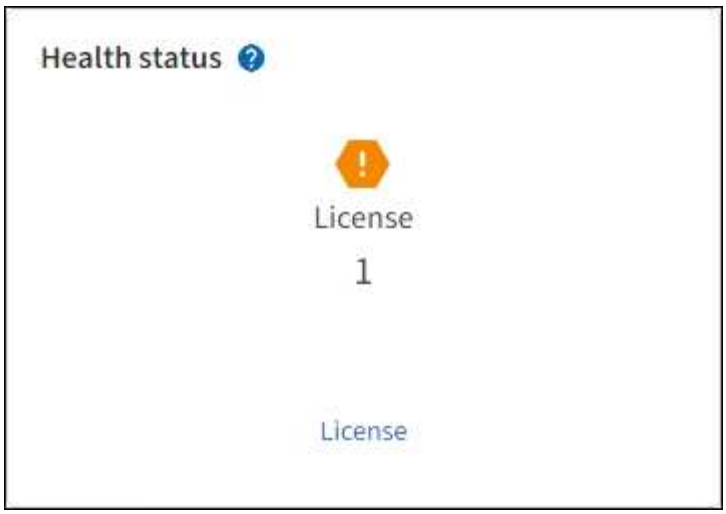
Sie können die Lizenzinformationen für Ihr StorageGRID -System, beispielsweise die maximale Speicherkapazität Ihres Grids, bei Bedarf einsehen.

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.

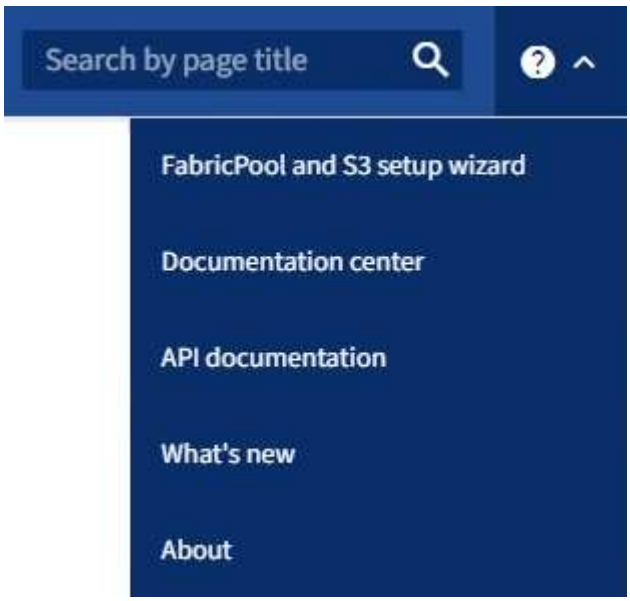
Bevor Sie beginnen

- 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.



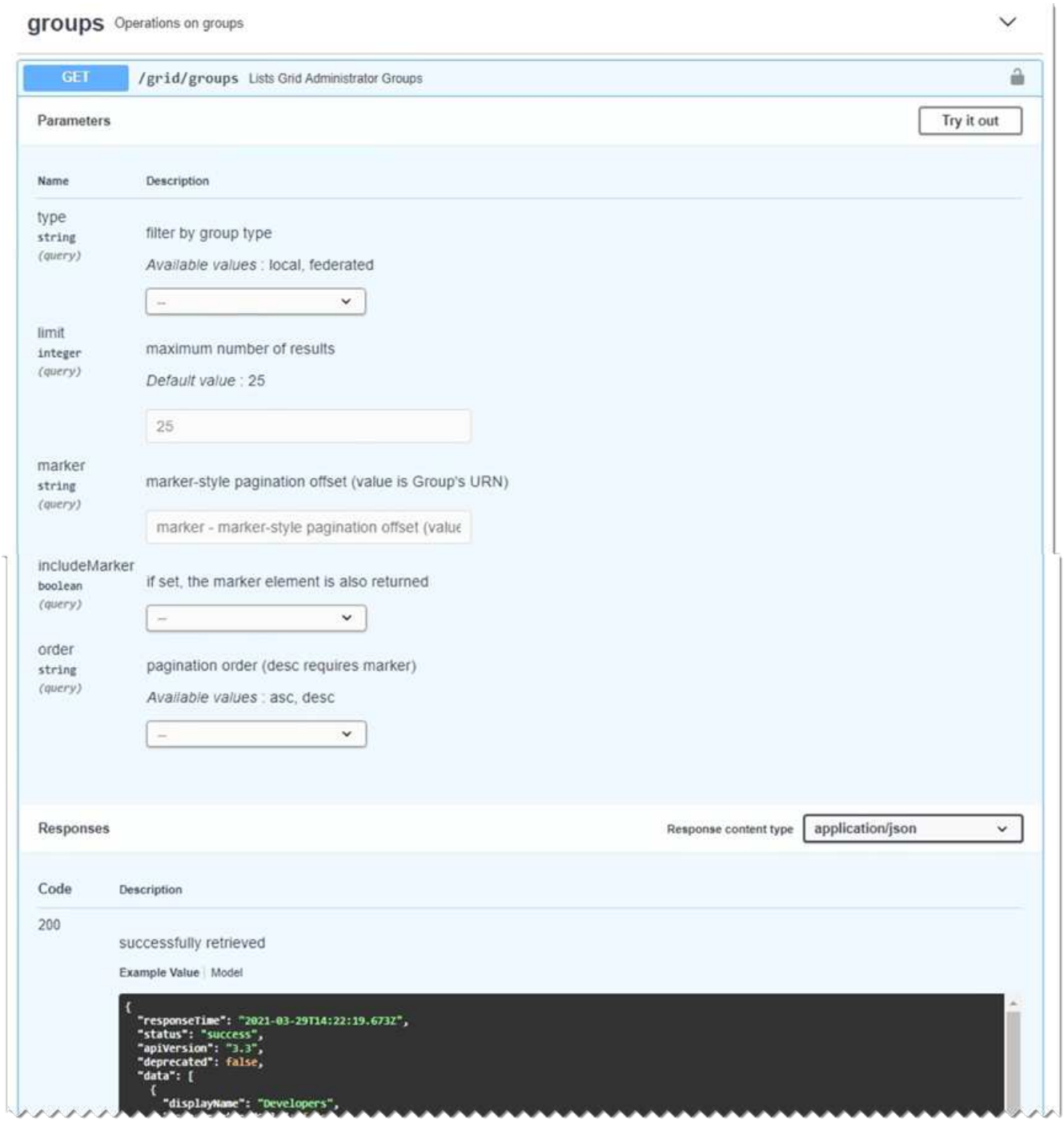
2. Um einen Vorgang mit der privaten API durchzuführen, wählen Sie auf der StorageGRID Management-API-Seite **Zur privaten API-Dokumentation gehen**.

   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.

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

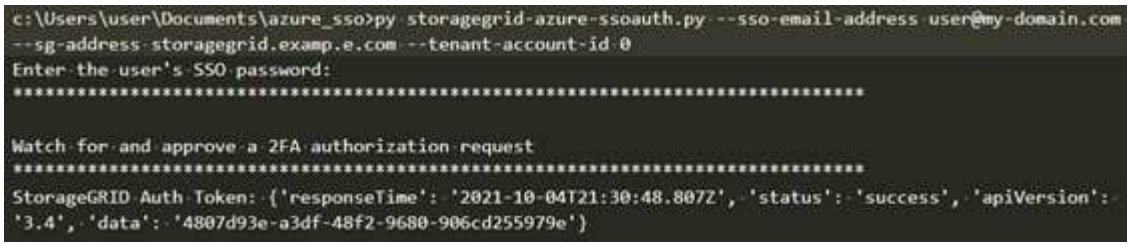
1. Installieren Sie die erforderlichen Abhängigkeiten wie folgt:
   a. Installieren Sie Node.js (siehe "https://nodejs.org/en/download/").
   b. Installieren Sie die erforderlichen Node.js-Module (Puppeteer und jsdom):

      ```
      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

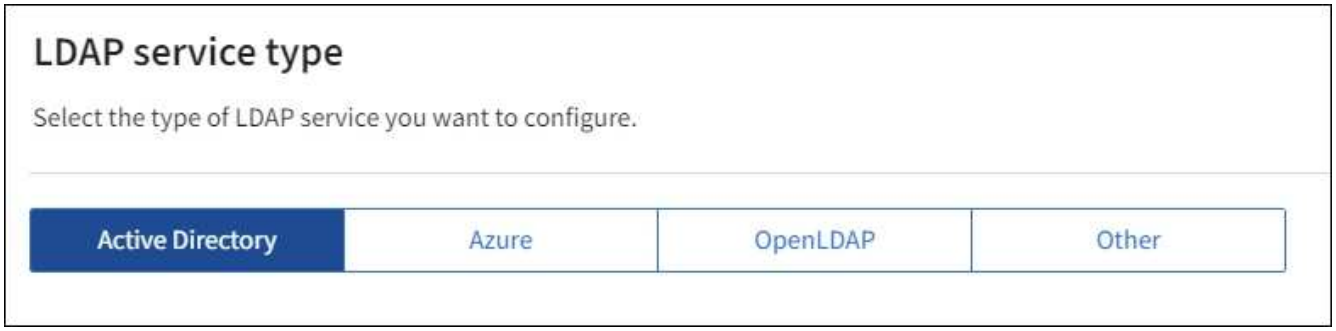
Sie können eine Identitätsquelle für den Grid Manager konfigurieren, wenn Sie Gruppen aus einem anderen System wie Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server importieren möchten. Sie können die folgenden Gruppentypen importieren:

- 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.

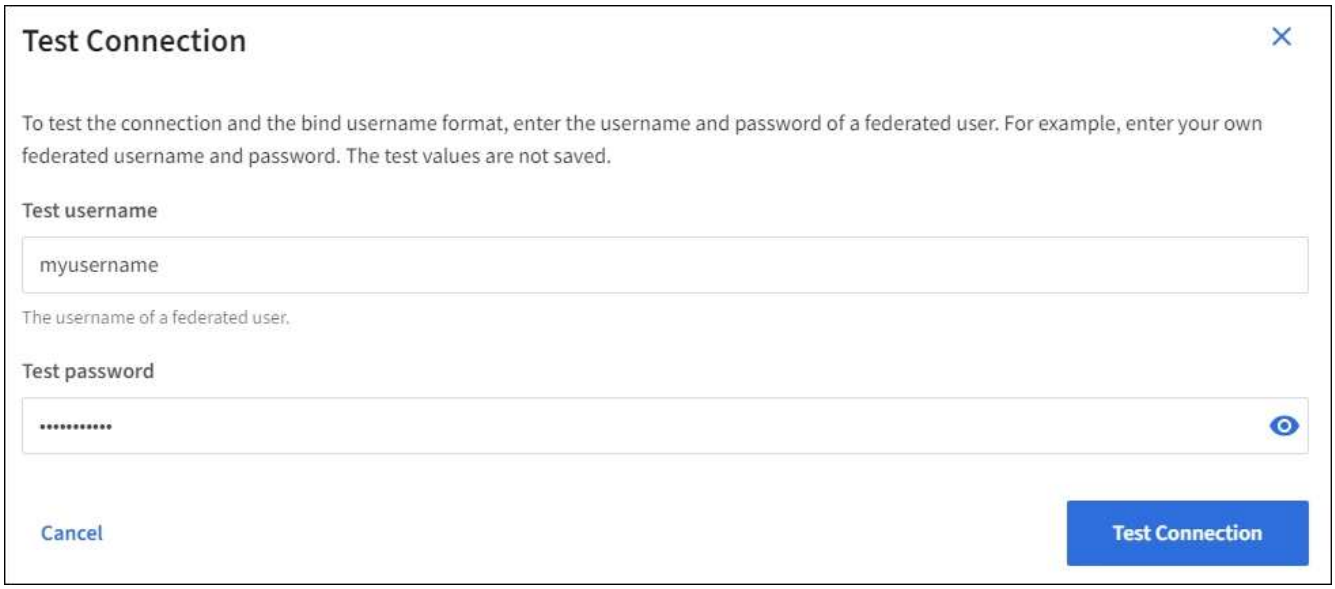
Testen Sie die Verbindung und speichern Sie die Konfiguration

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

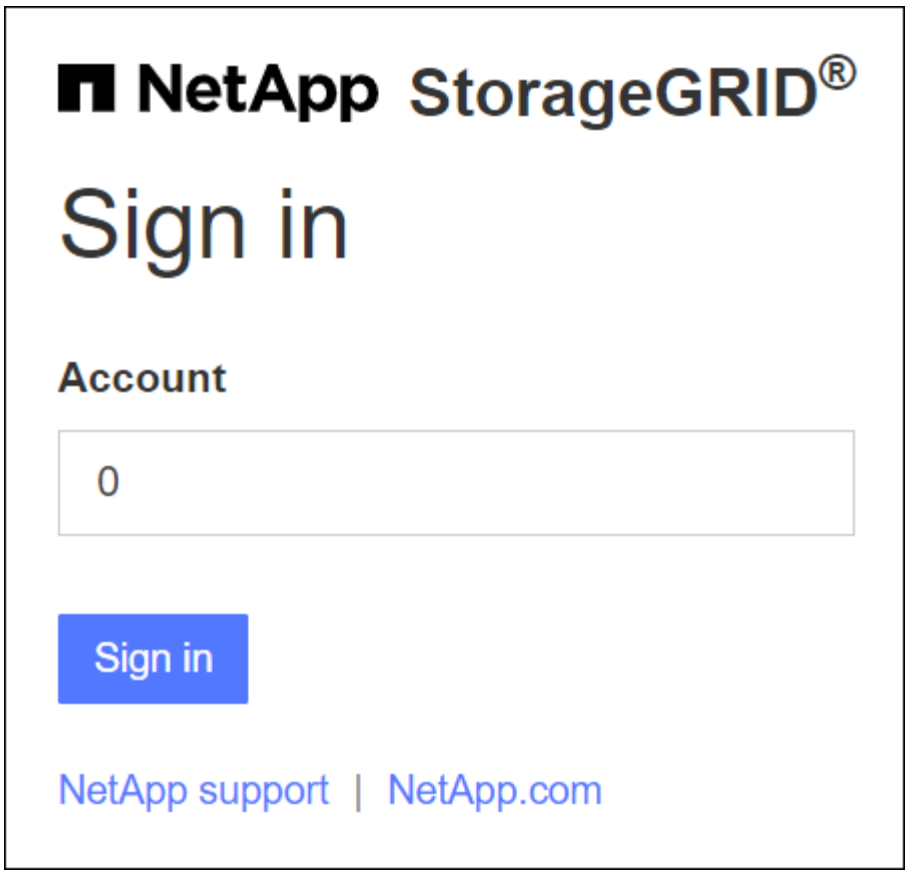
Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur Validierung Ihrer Anmeldeinformationen auf die SSO-Seite Ihrer Organisation weitergeleitet.

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:

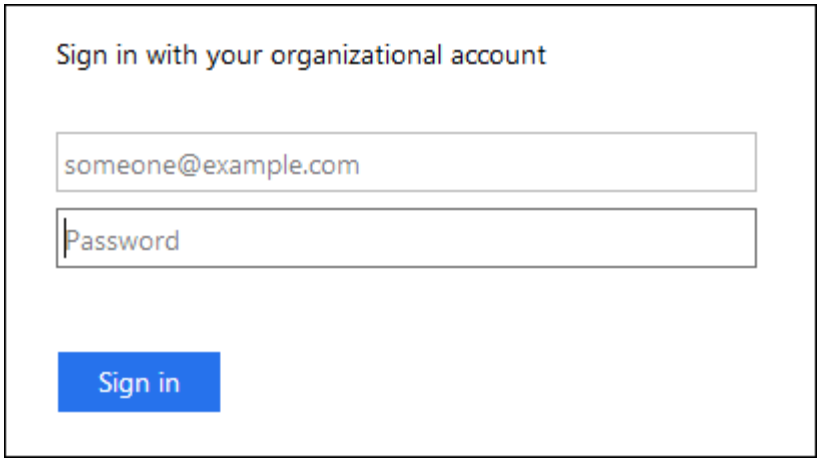


- Wenn Sie zuvor entweder auf den Grid Manager oder den Tenant Manager zugegriffen haben, werden Sie aufgefordert, ein aktuelles Konto auszuwählen oder eine Konto-ID einzugeben:

> 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

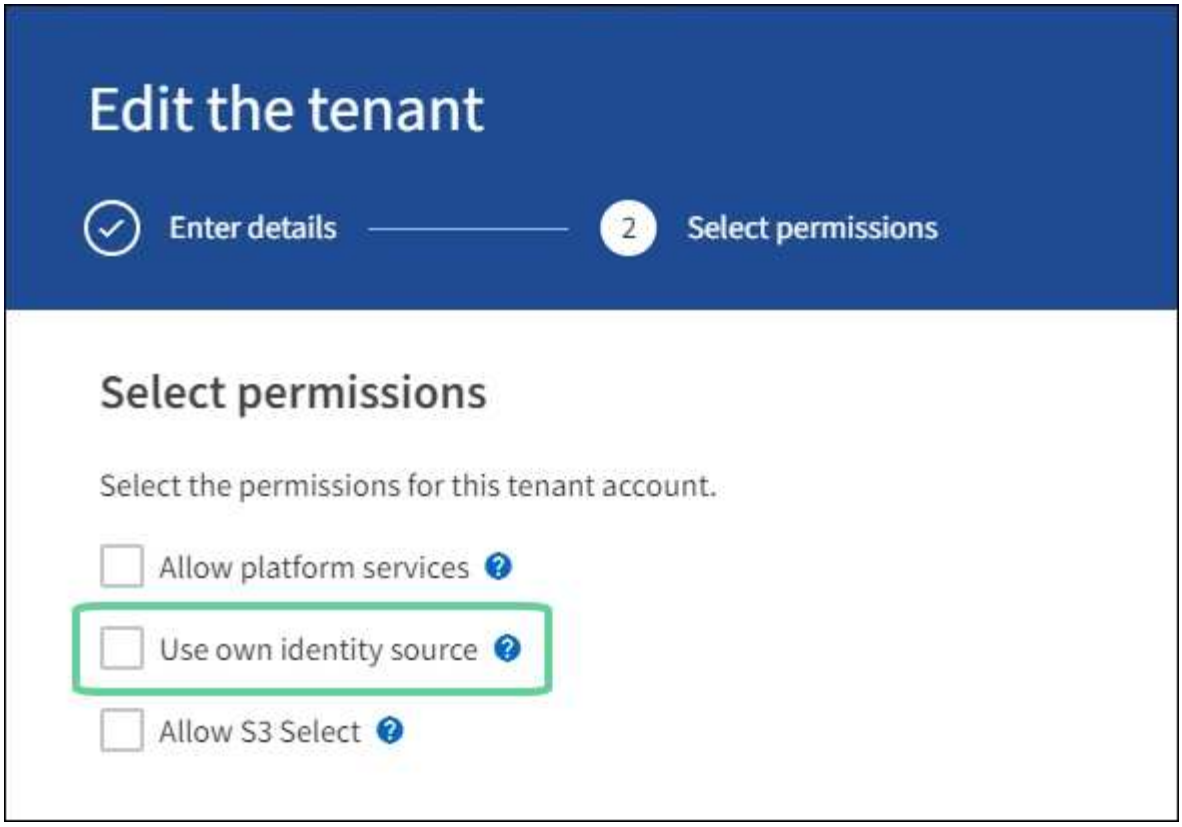
1. Wenn bereits Mandantenkonten vorhanden sind, vergewissern Sie sich, dass keiner der Mandanten eine eigene Identitätsquelle verwendet.

   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.

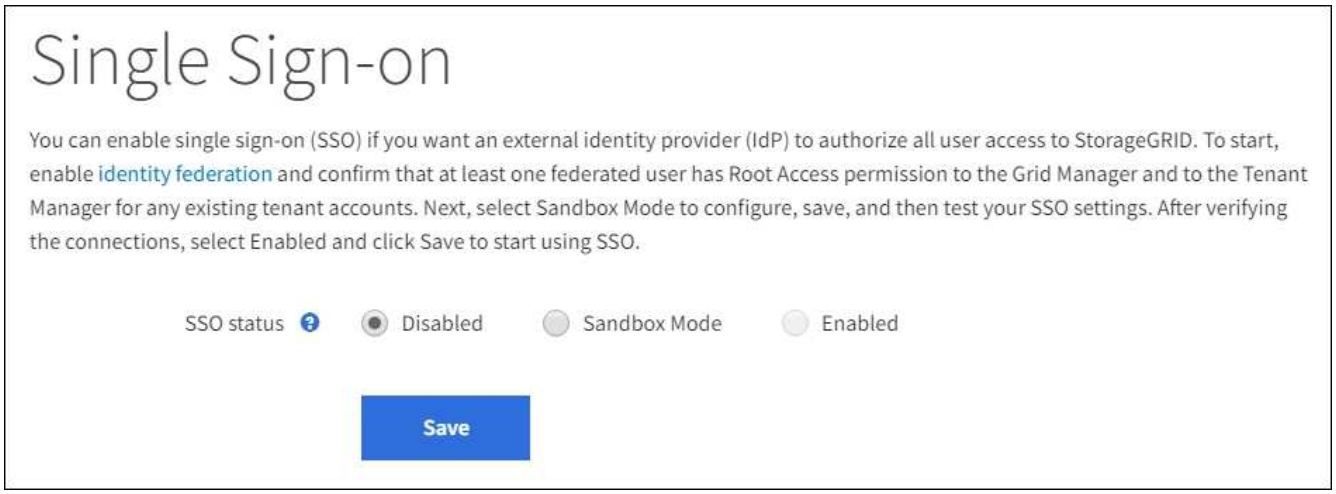
Der Sandbox-Modus erleichtert die Durchführung dieser Hin- und Her-Konfiguration und das Testen aller Ihrer Einstellungen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht per SSO anmelden.

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.

Konfigurieren von Vertrauensstellungen der vertrauenden Seite, Unternehmensanwendungen oder SP Verbindungen

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

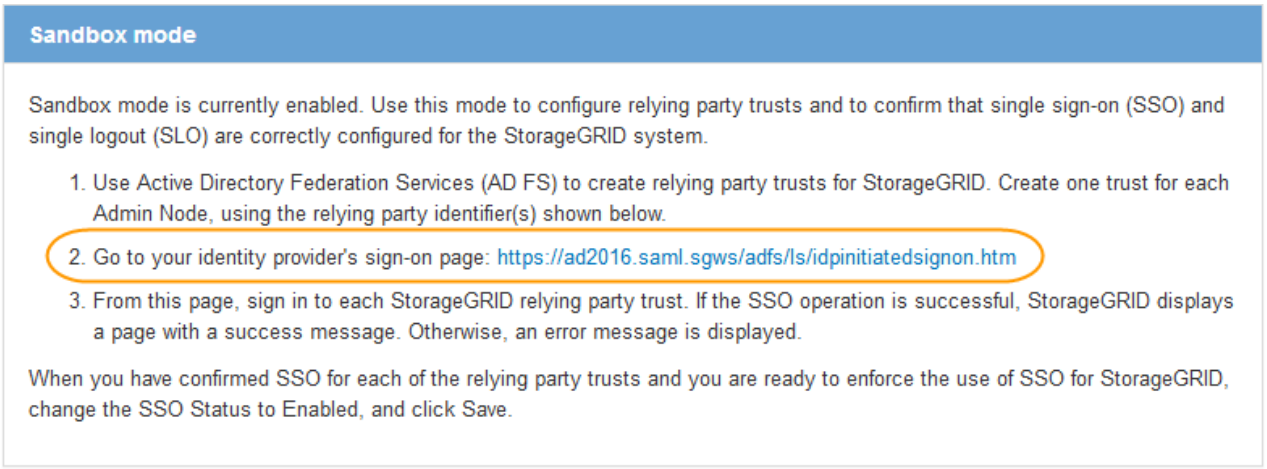
Bevor Sie die Verwendung von Single Sign-On für Ihr gesamtes StorageGRID System erzwingen, sollten Sie bestätigen, dass Single Sign-On und Single Logout für jeden Admin-Knoten richtig konfiguriert sind.

Active Directory

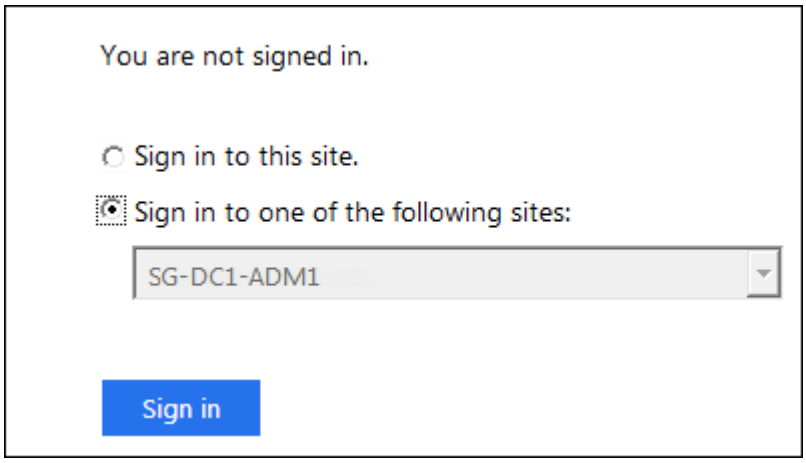
Schritte

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

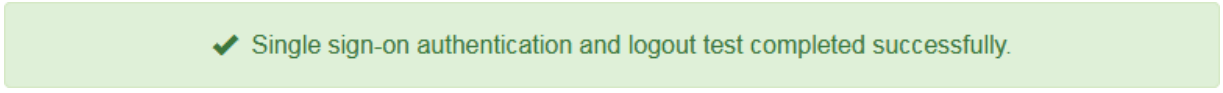
   Die URL wird aus dem Wert abgeleitet, den Sie in das Feld **Name des Verbunddienstes** eingegeben haben.

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.

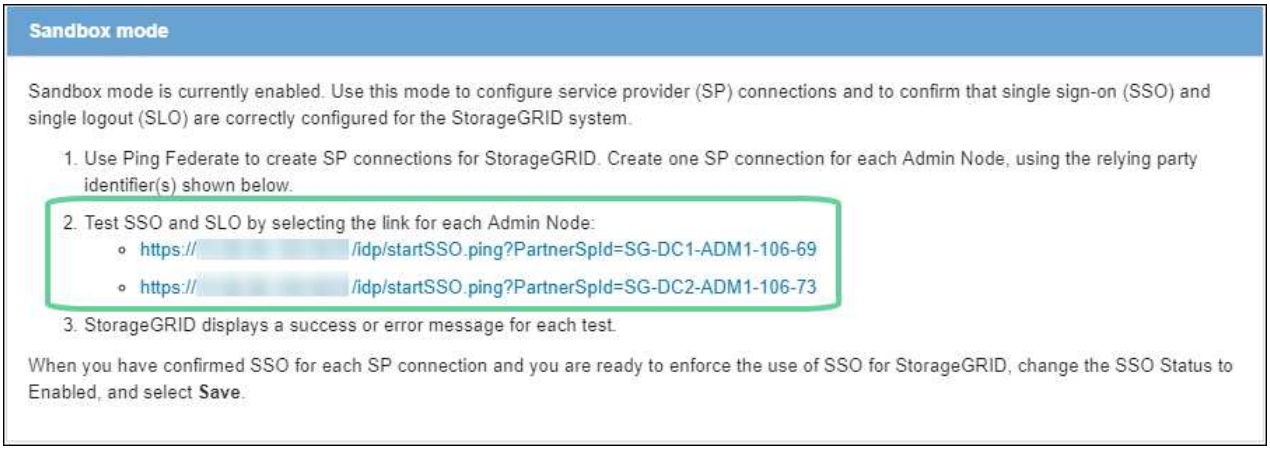
   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers und versuchen Sie es erneut.
4. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Knoten in Ihrem Raster zu überprüfen.

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?

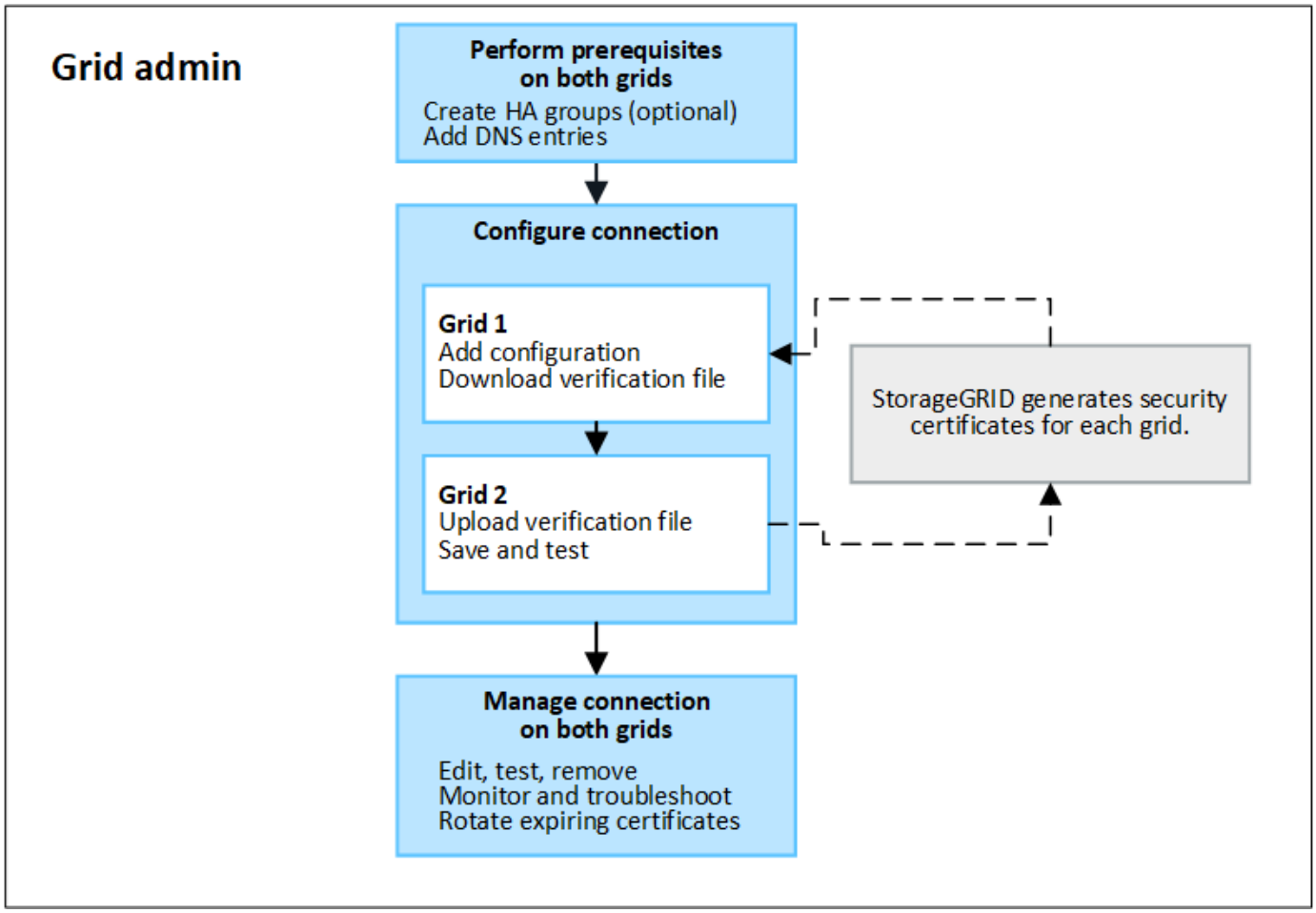
Sie können die Grid-Föderation verwenden, um Mandanten zu klonen und ihre Objekte zwischen zwei StorageGRID -Systemen zur Notfallwiederherstellung zu replizieren.

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

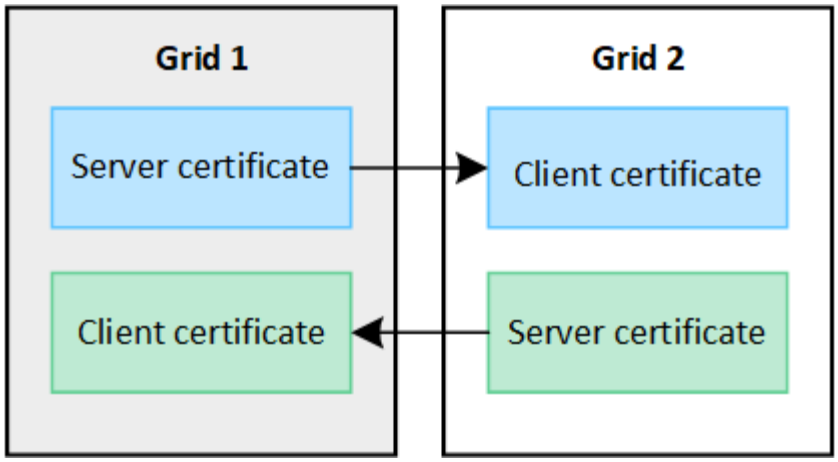
Beim Erstellen einer Grid-Föderation-Verbindung können Sie jede nicht verwendete Portnummer zwischen 23000 und 23999 angeben. Beide Grids in dieser Verbindung verwenden denselben Port.

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"

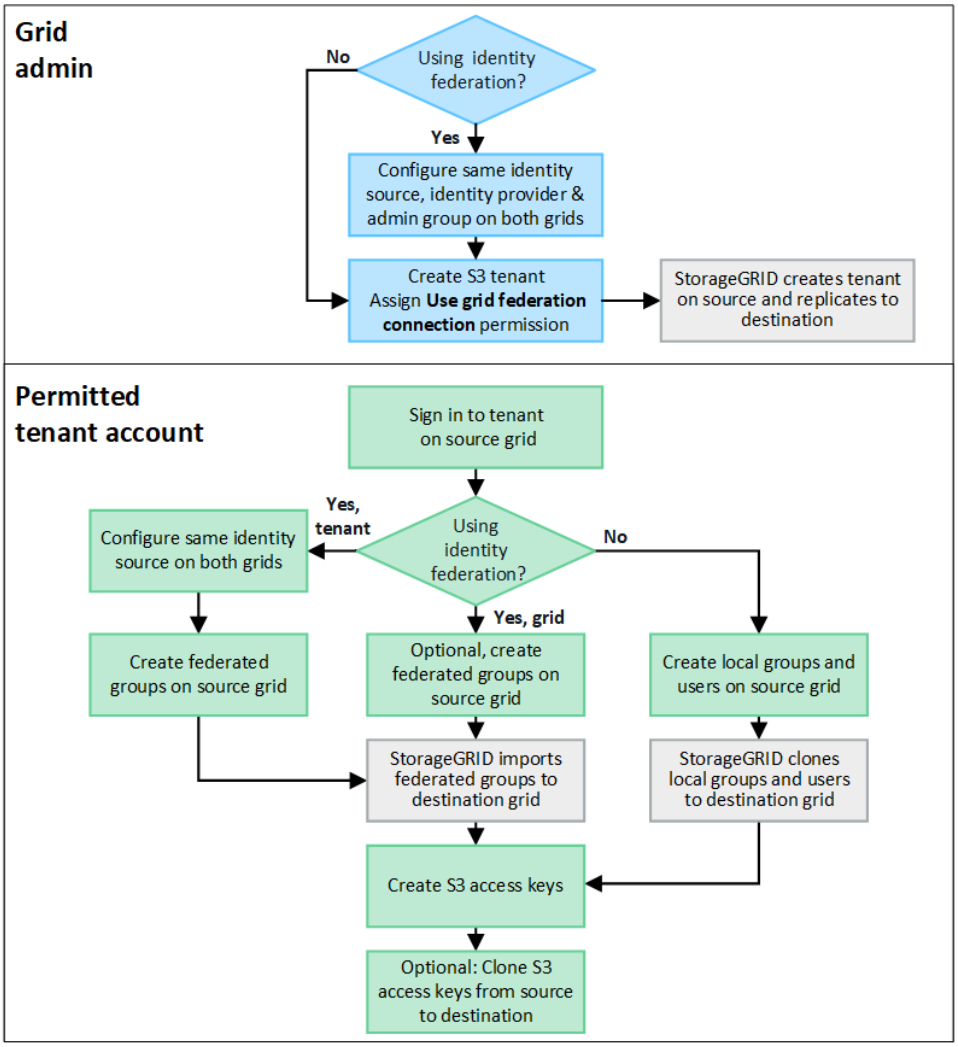
Was ist ein Kontoklon?

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.

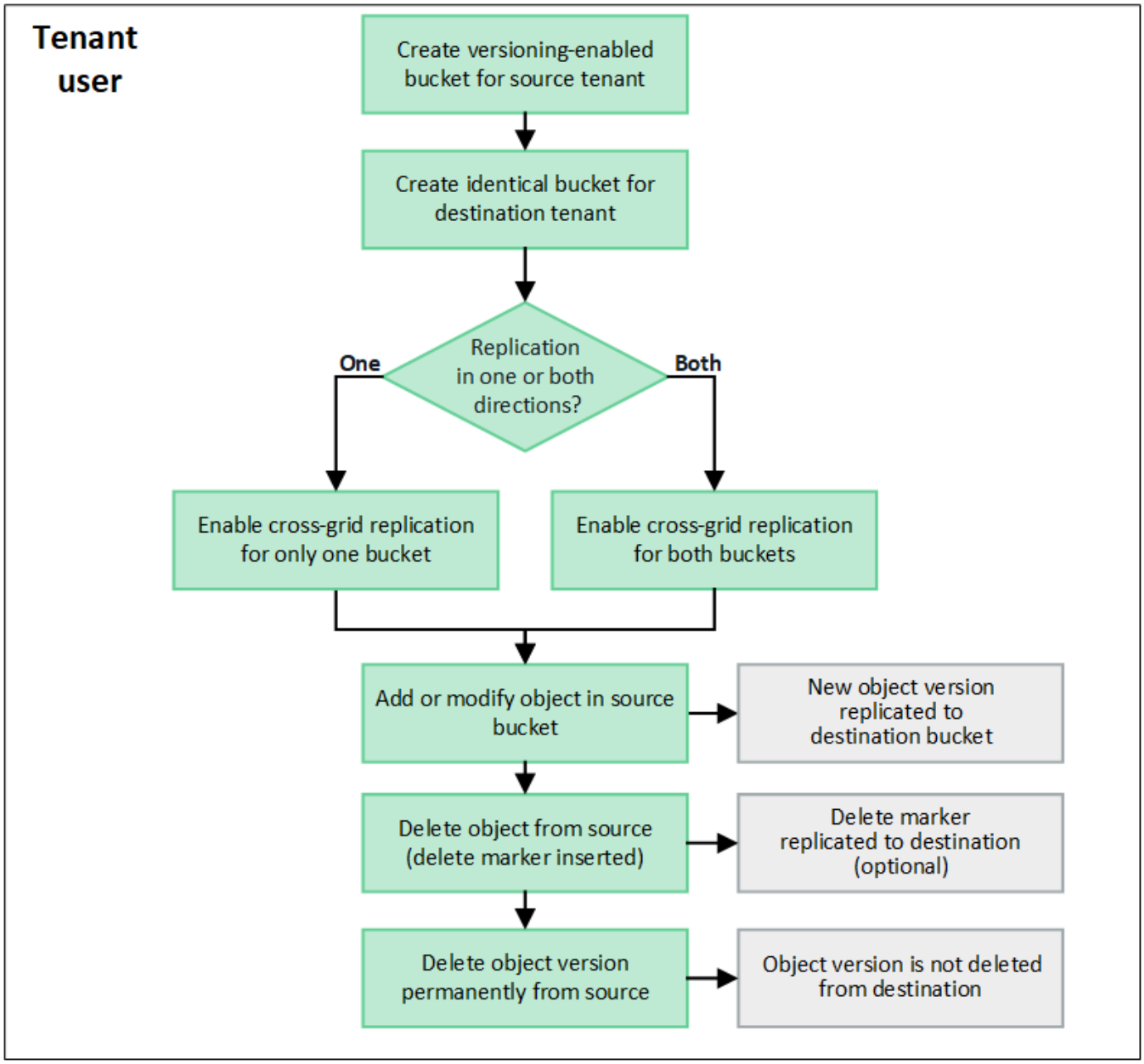
Weitere Informationen zum Workflow für zulässige Mandantenkonten und zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln finden Sie unter"Mandantengruppen und Benutzer klonen" Und"Klonen Sie S3-Zugriffsschlüssel mithilfe der API" .

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.

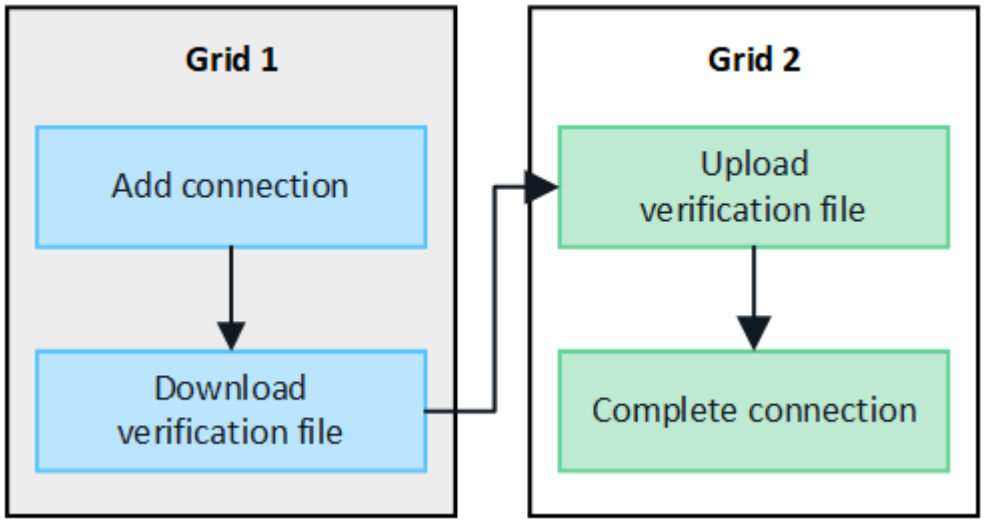
	Cross-Grid-Replikation	CloudMirror-Replikationsdienst
Wie ist es eingerichtet?	1. Konfigurieren Sie eine Grid-Föderationsverbindung zwischen zwei Grids. 2. Fügen Sie neue Mandantenkonten hinzu, die automatisch in das andere Raster geklont werden. 3. Fügen Sie neue Mandantengruppen und Benutzer hinzu, 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.

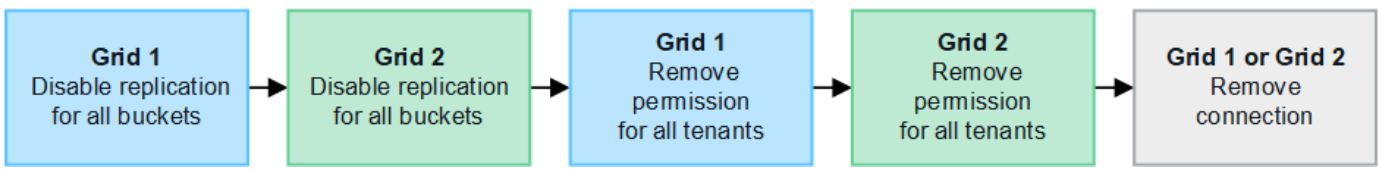
Schritte

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" .

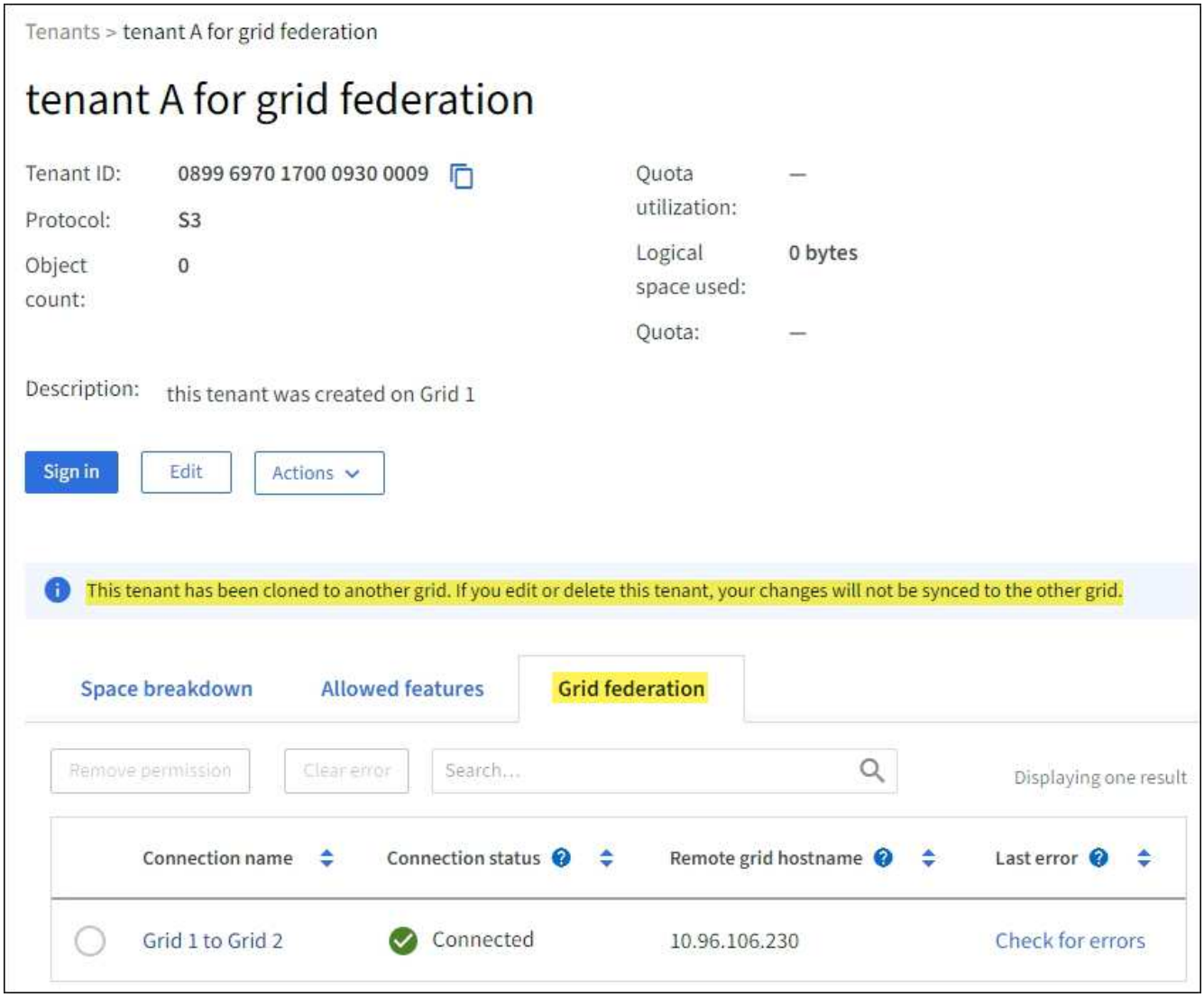
Anzeigen eines zulässigen Mandanten

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

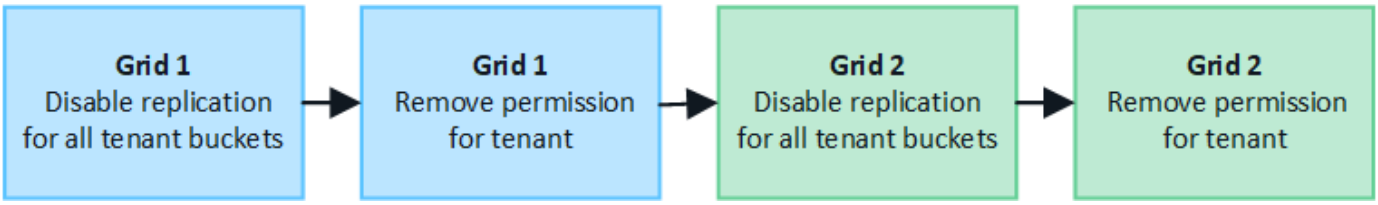
Sie Folgendes:

- 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.

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.

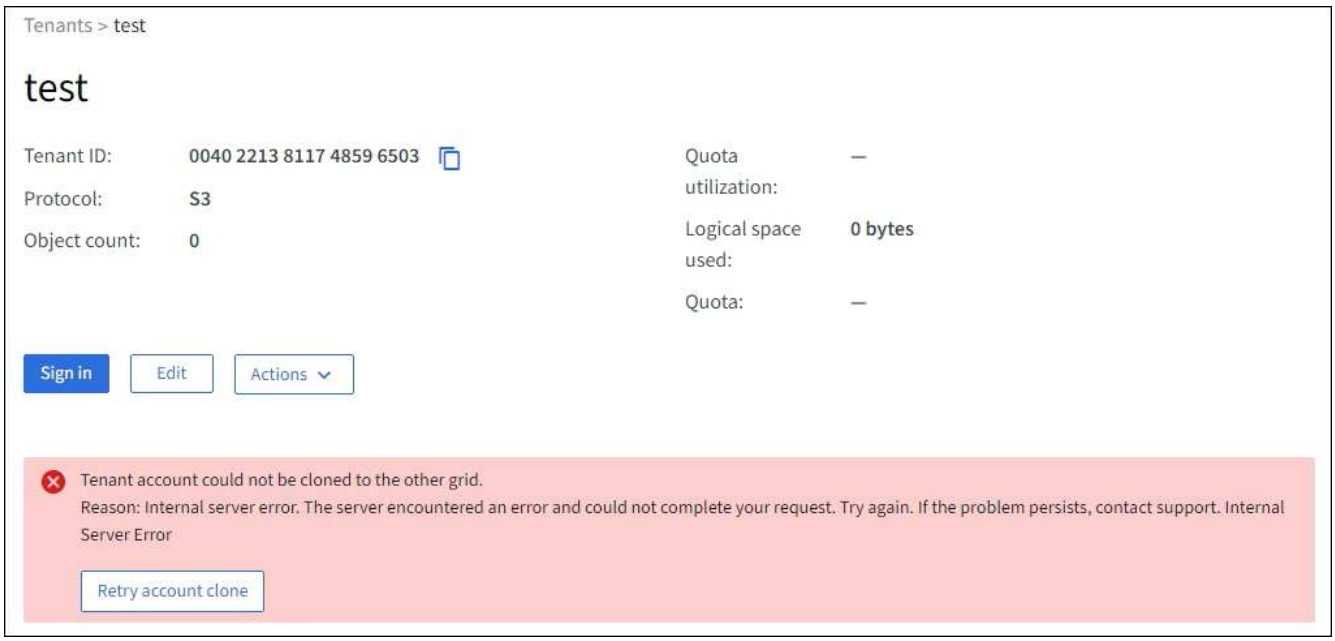
Details

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**.



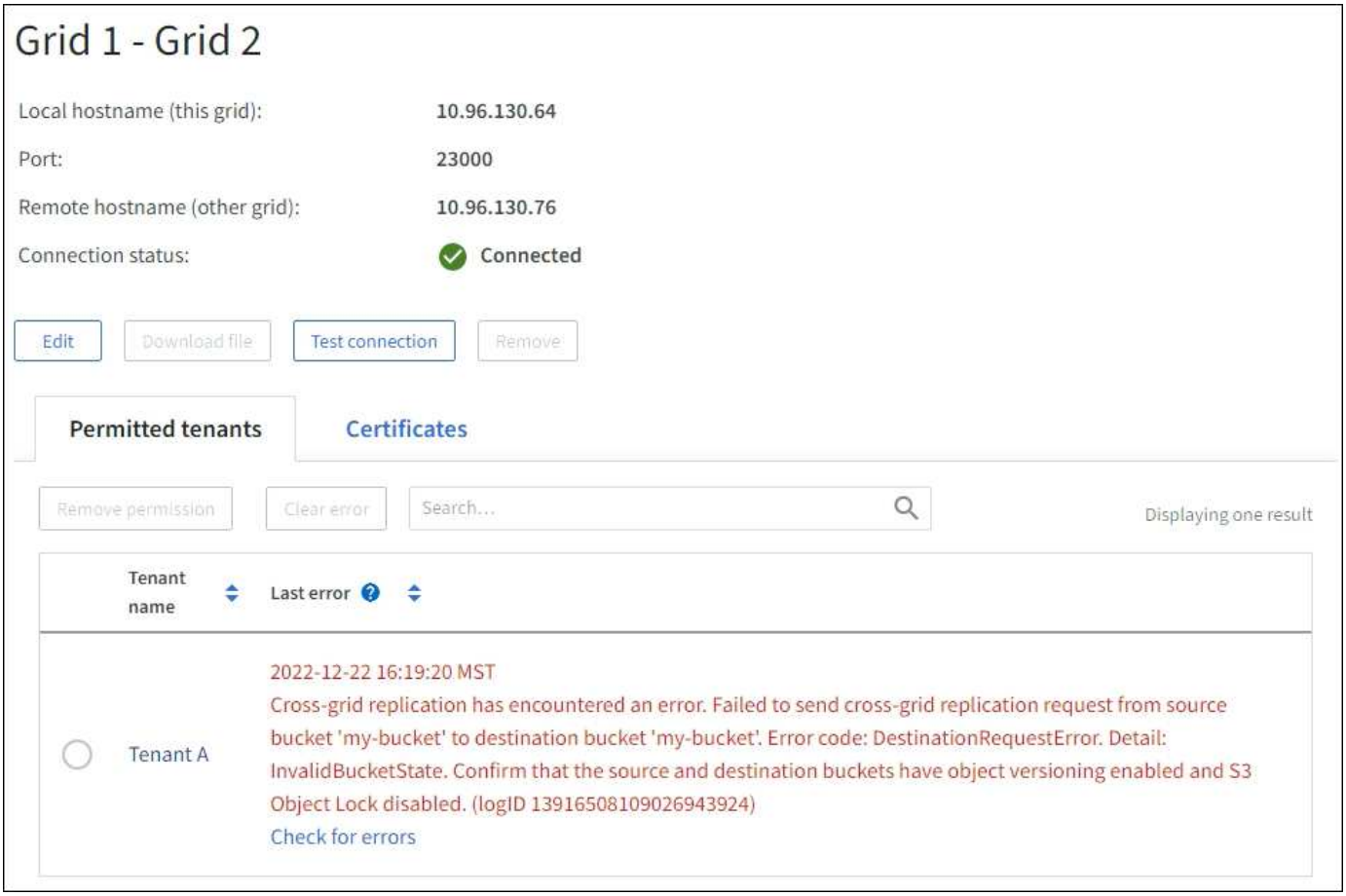
Wenn der Fehler behoben wurde, wird das Mandantenkonto nun in das andere Grid geklont.

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.

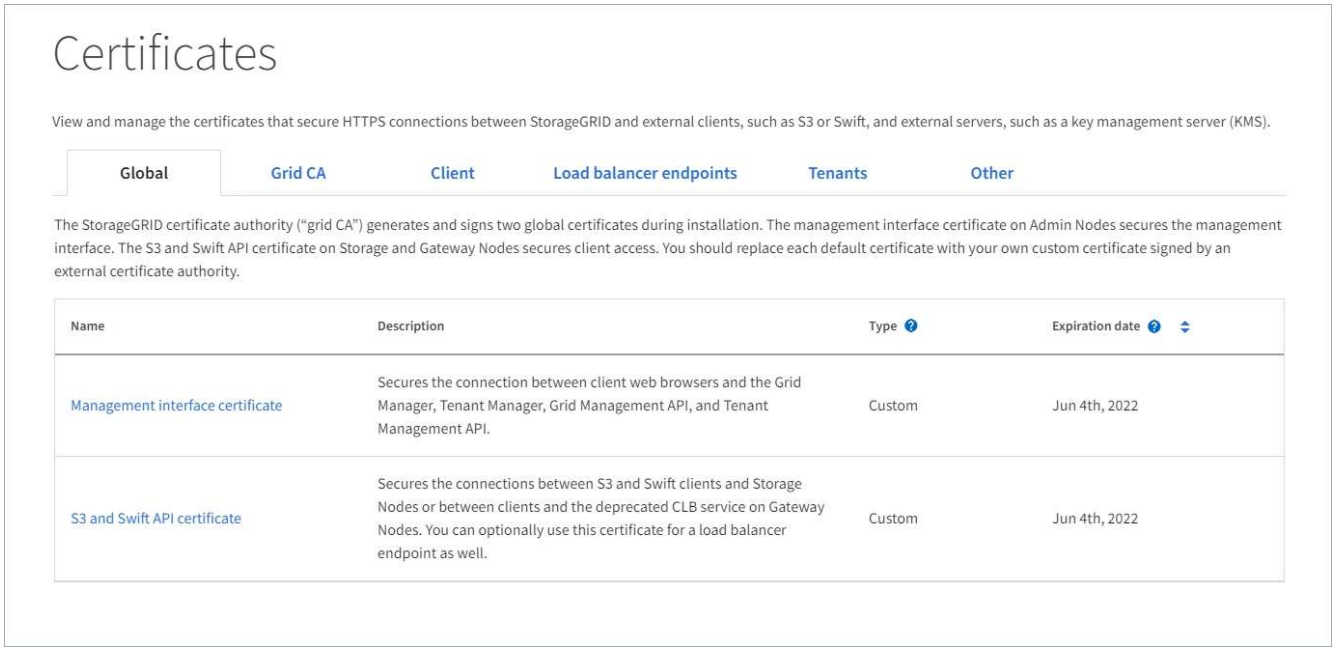
Varianten der Server- und Client-Zertifikattypen werden auf verschiedene Weise implementiert. Sie sollten alle für Ihre spezifische StorageGRID Konfiguration erforderlichen Zertifikate bereithalten, bevor Sie das System konfigurieren.

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.

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.

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.

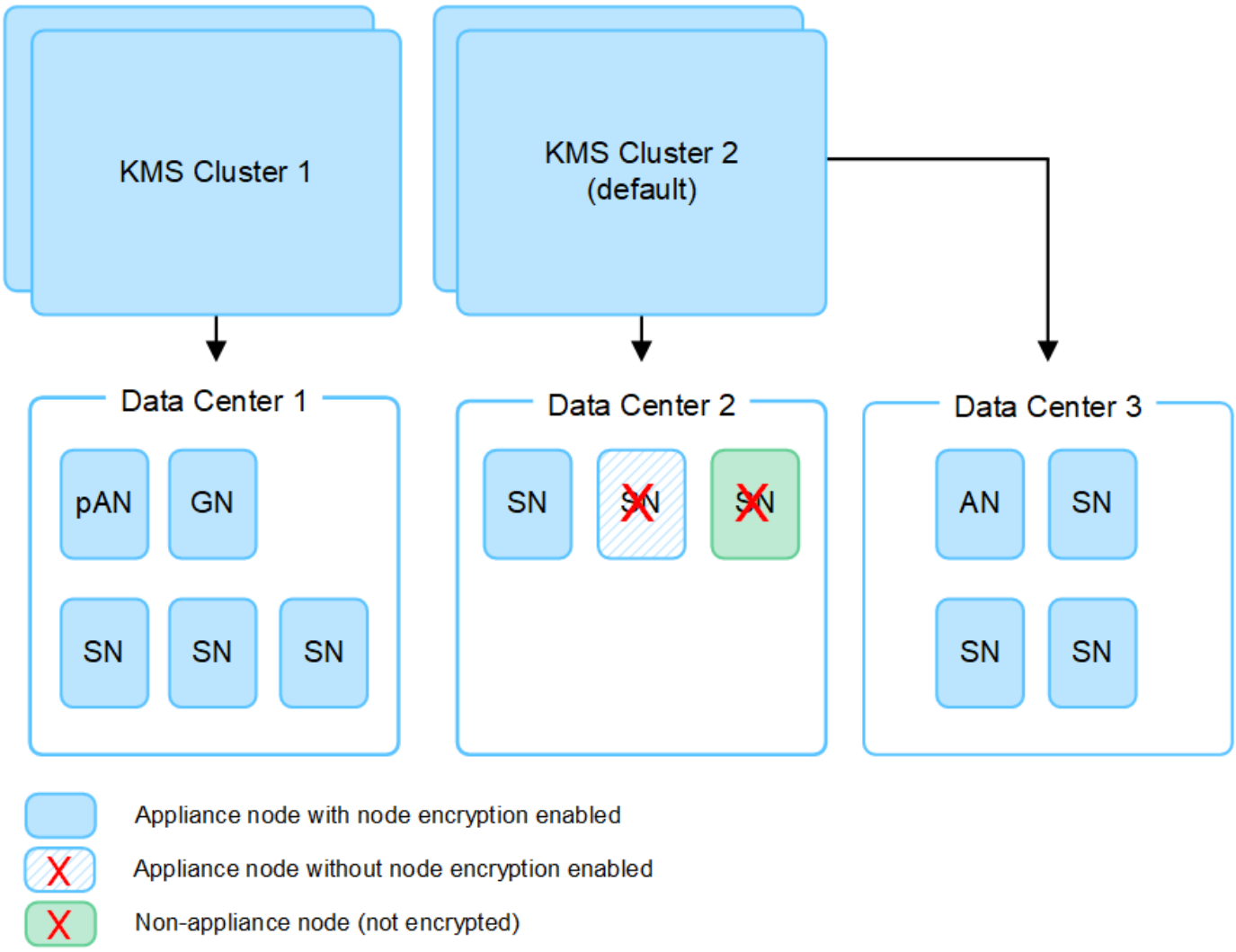
Wie viele Schlüsselverwaltungsserver benötige ich?

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.

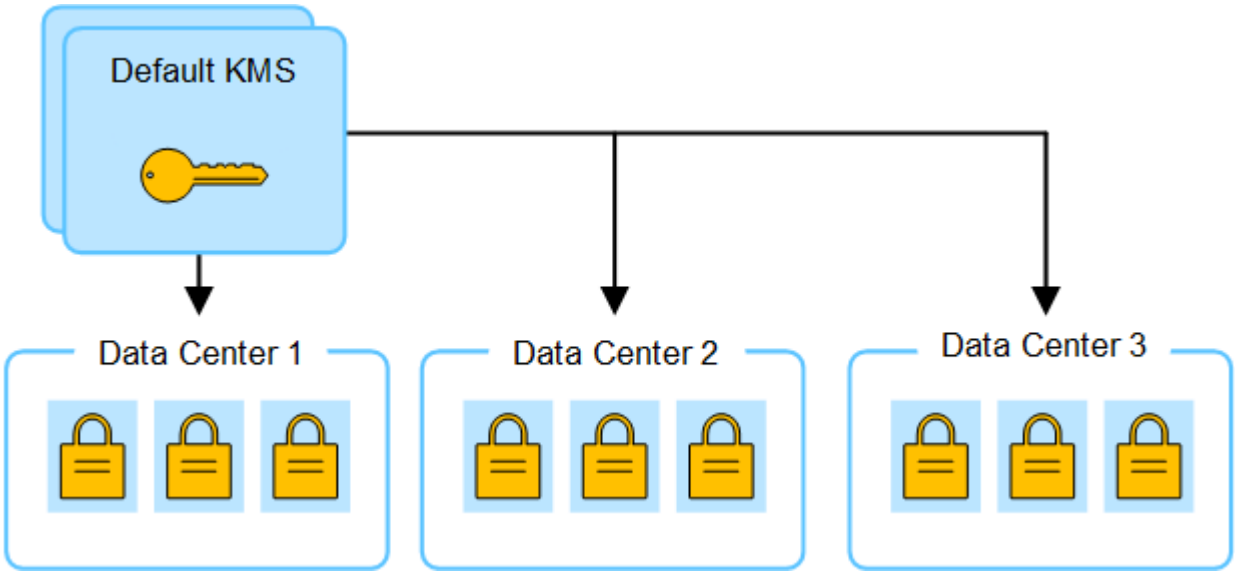
Überlegungen zum Ändern des KMS für eine Site

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.

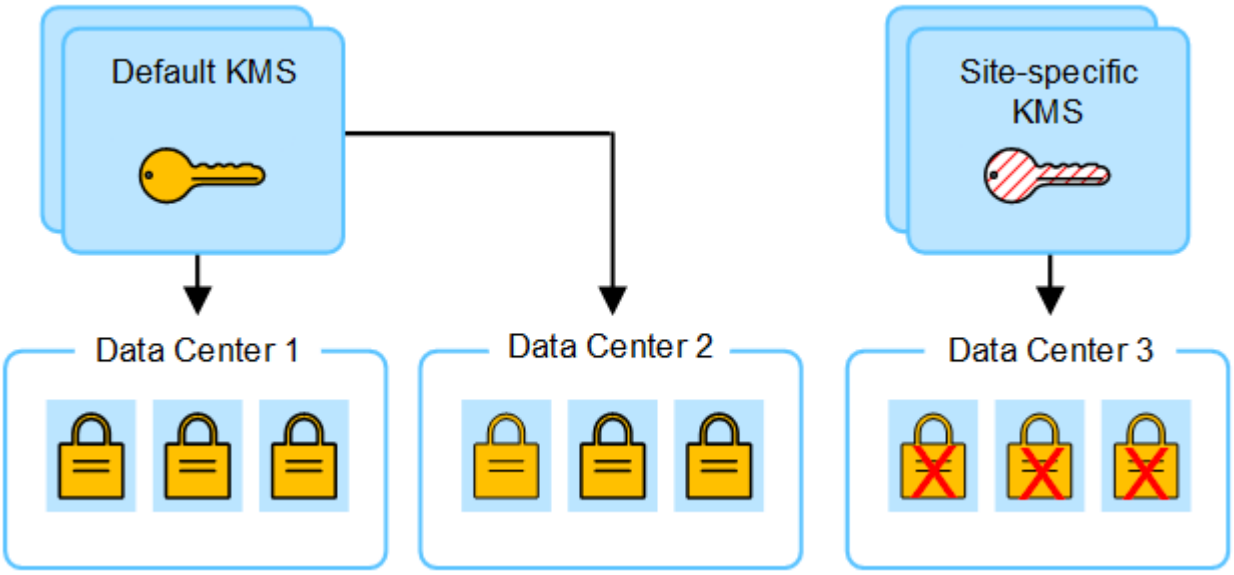
Beispiel:

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.

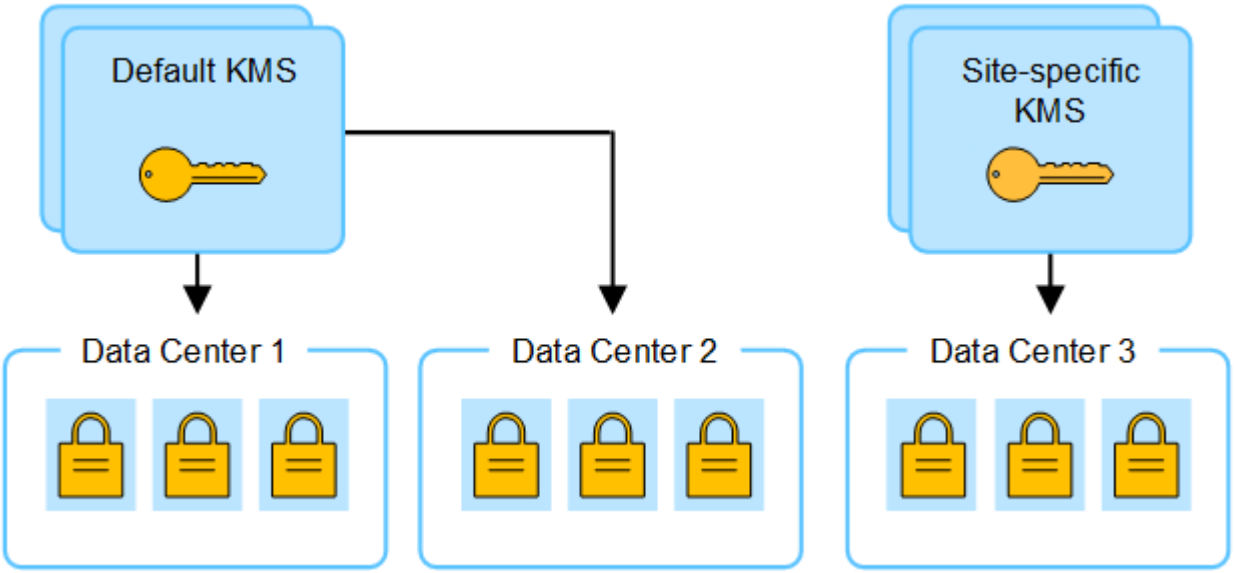


3. Sie entscheiden sich, für einen Standort (Rechenzentrum 3 in der Abbildung) ein standortspezifisches KMS hinzuzufügen. Da die Appliance-Knoten jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für das standortspezifische KMS zu speichern. Der 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" .

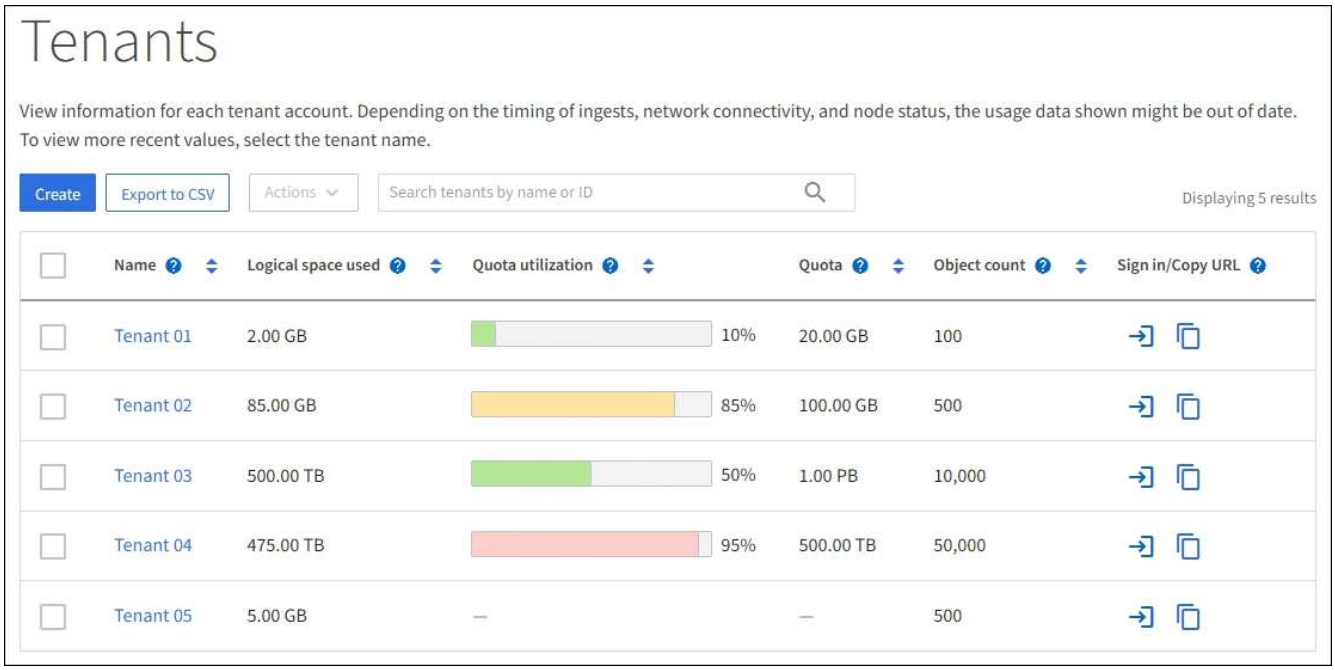
Bevor Sie beginnen

- 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

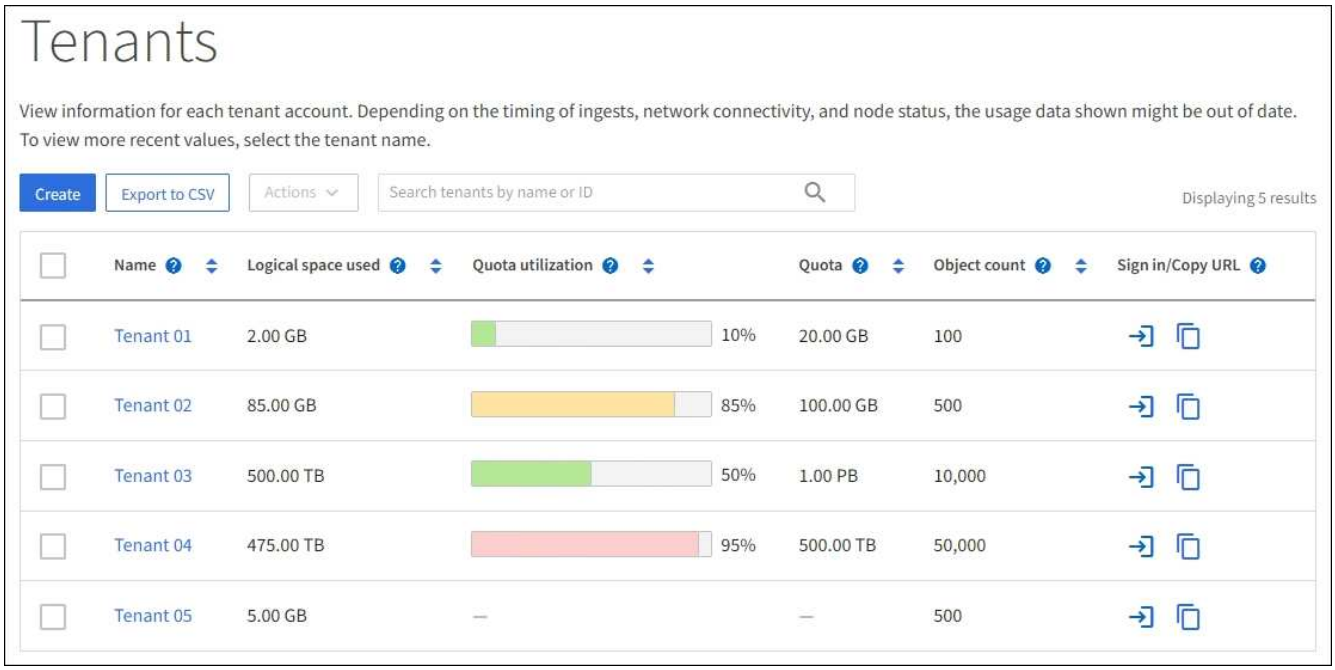
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .

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.

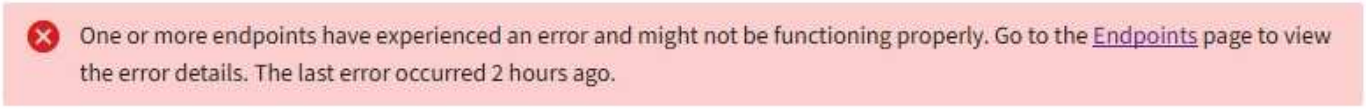
Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID -System, ob der Endpunkt vorhanden ist und mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

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.

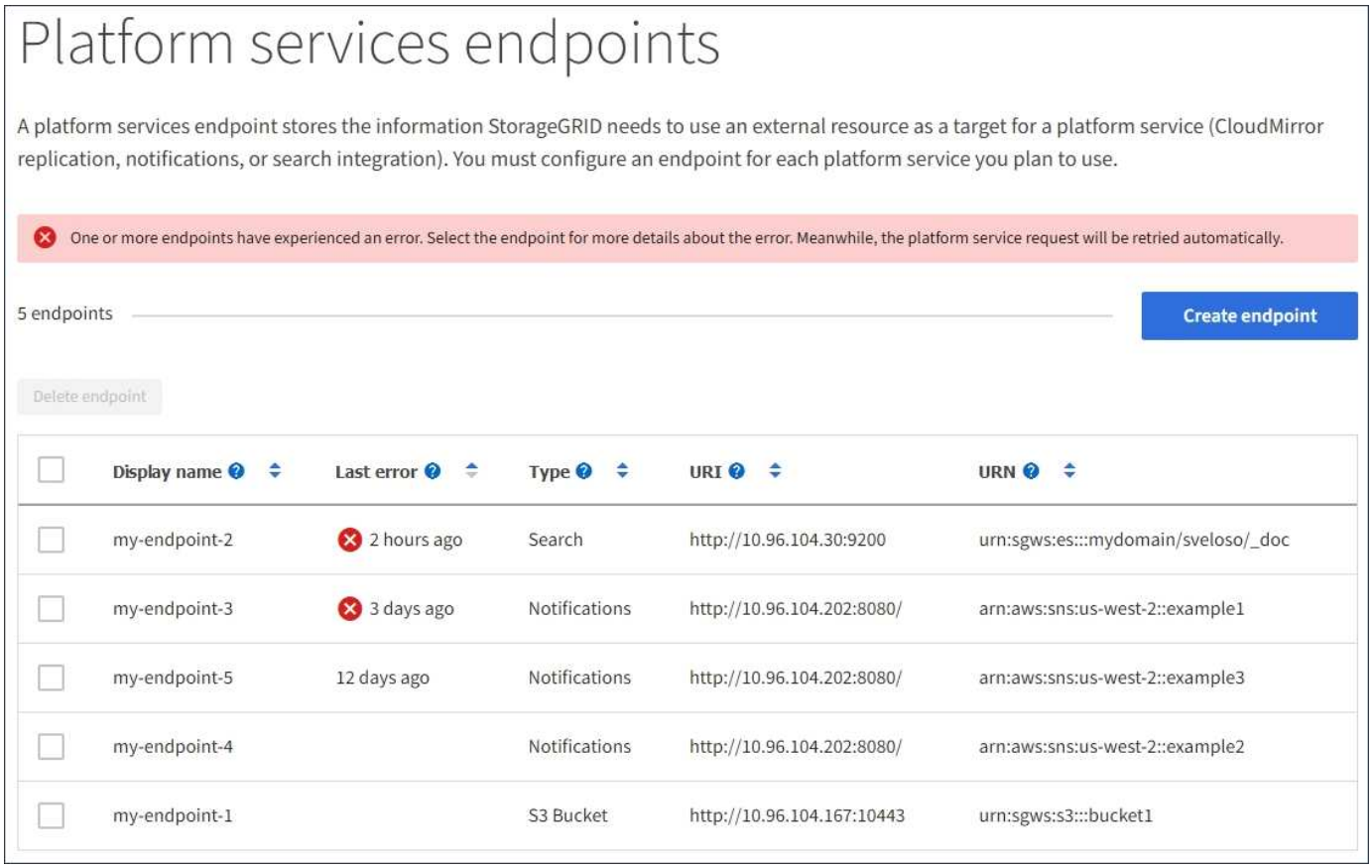
> Die Endpunkterstellung schlägt fehl, wenn die Plattformdienste für das Mandantenkonto nicht aktiviert sind.

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.

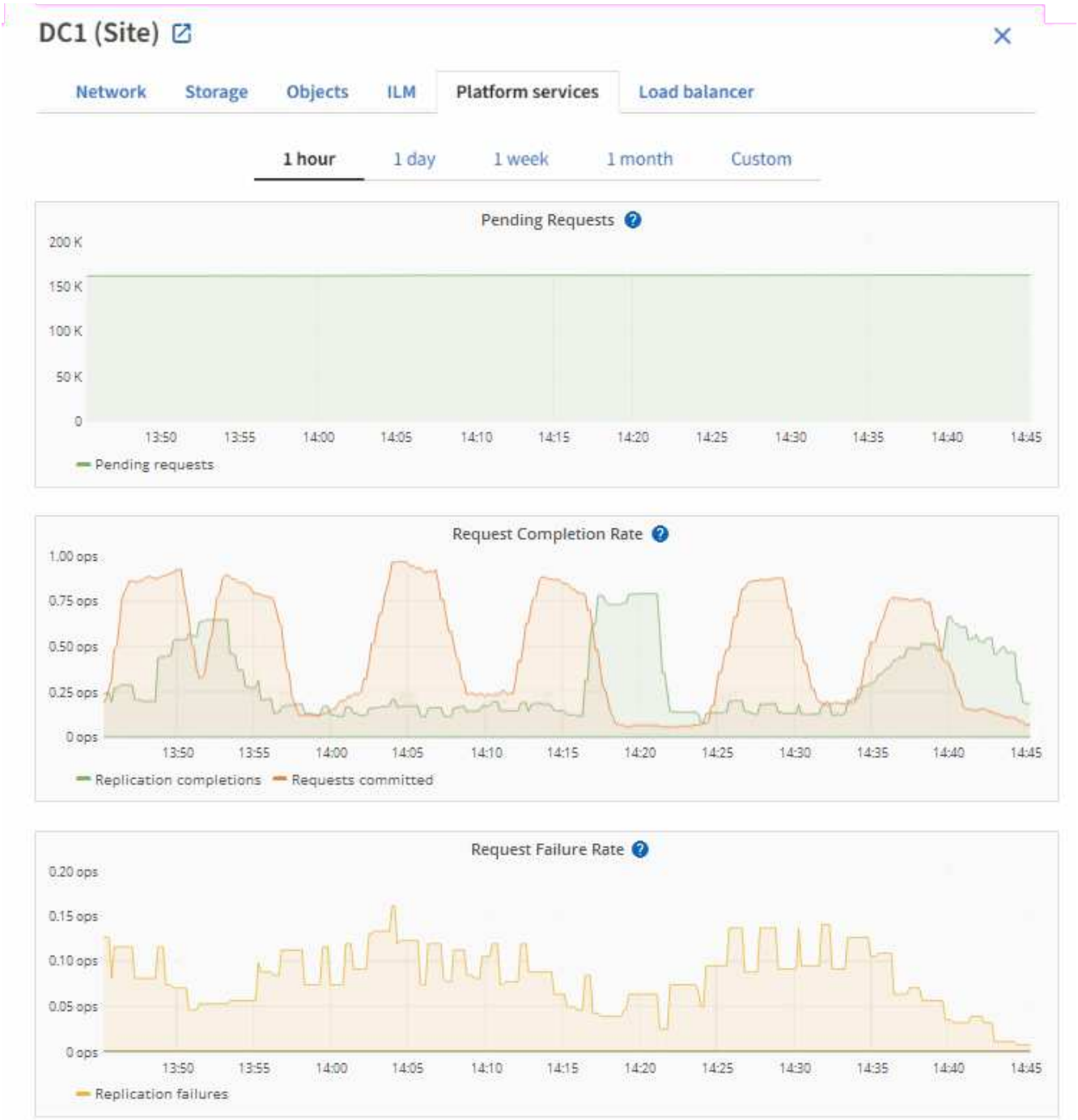
Der einzige sichtbare Effekt besteht darin, dass die Ausführung eingehender S3-Anfragen länger dauert. Wenn Sie eine deutlich langsamere Leistung feststellen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Wenn der Rückstand an Anfragen weiter wächst, schlagen 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.

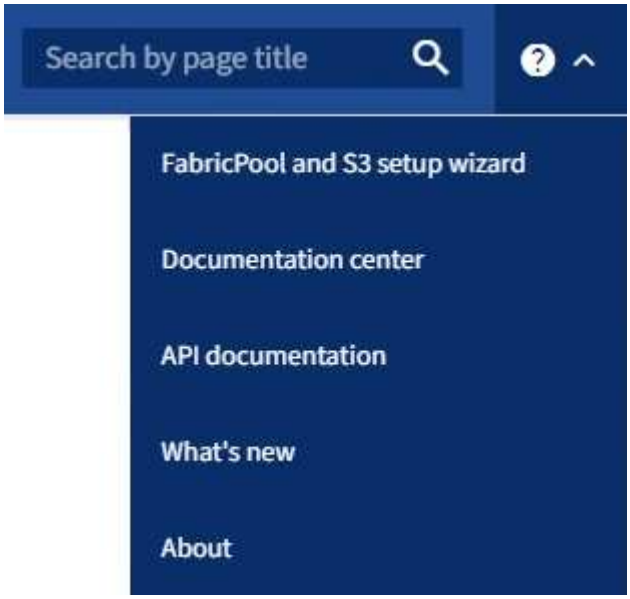
Bevor Sie beginnen

- 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

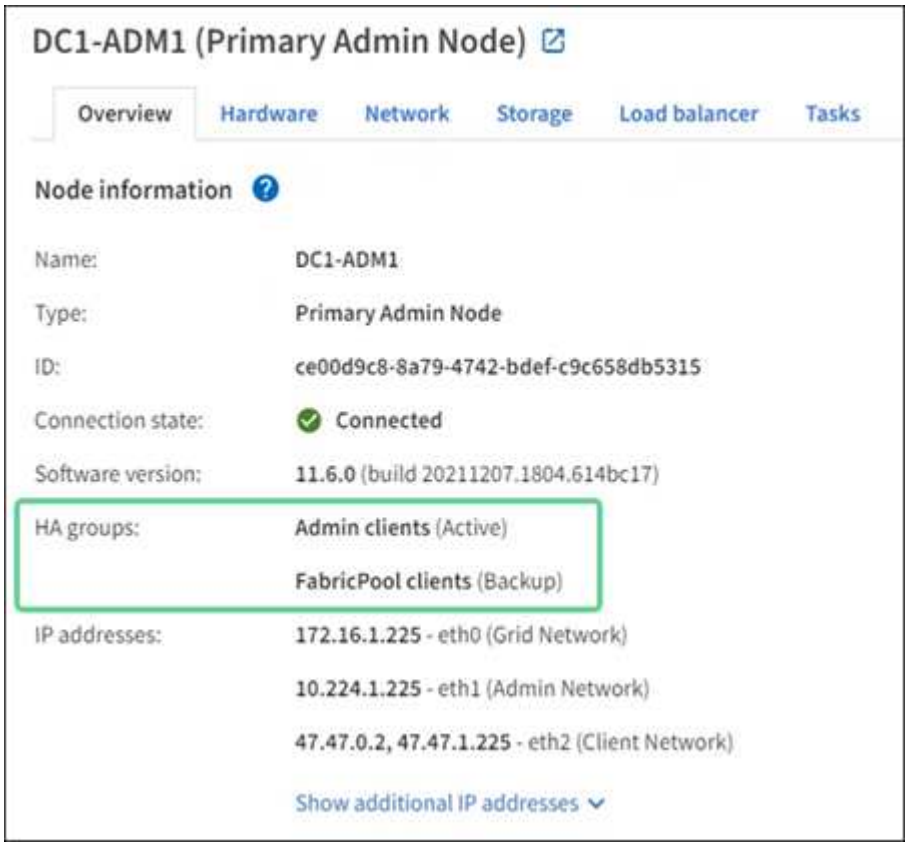
Um zu sehen, ob ein Knoten einer HA-Gruppe zugewiesen ist, und um seinen aktuellen Status zu bestimmen, wählen Sie **NODES** > ***node***.

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.

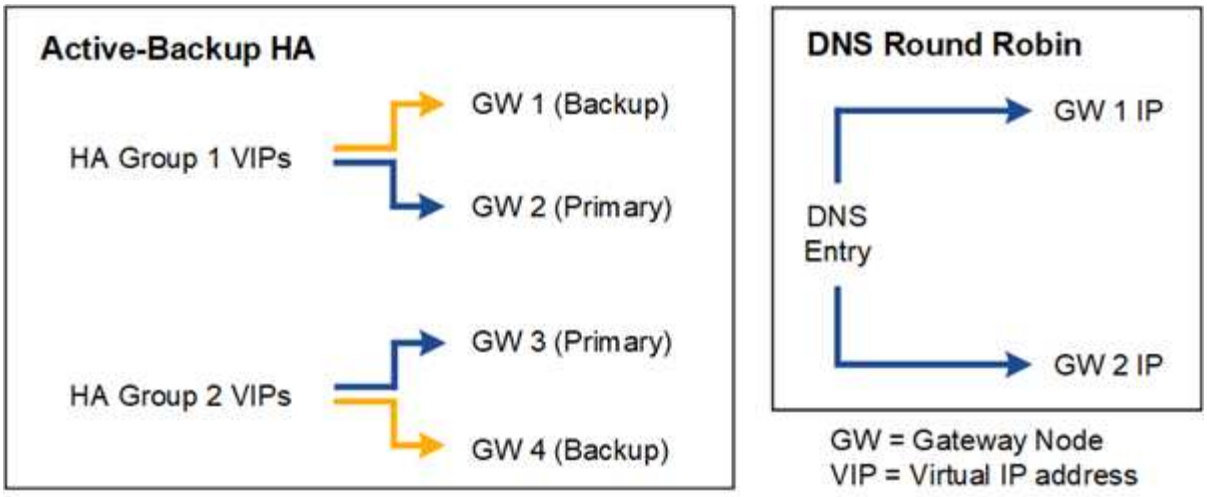
Wenn Sie beim Failover beim Grid Manager oder Tenant Manager angemeldet sind, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

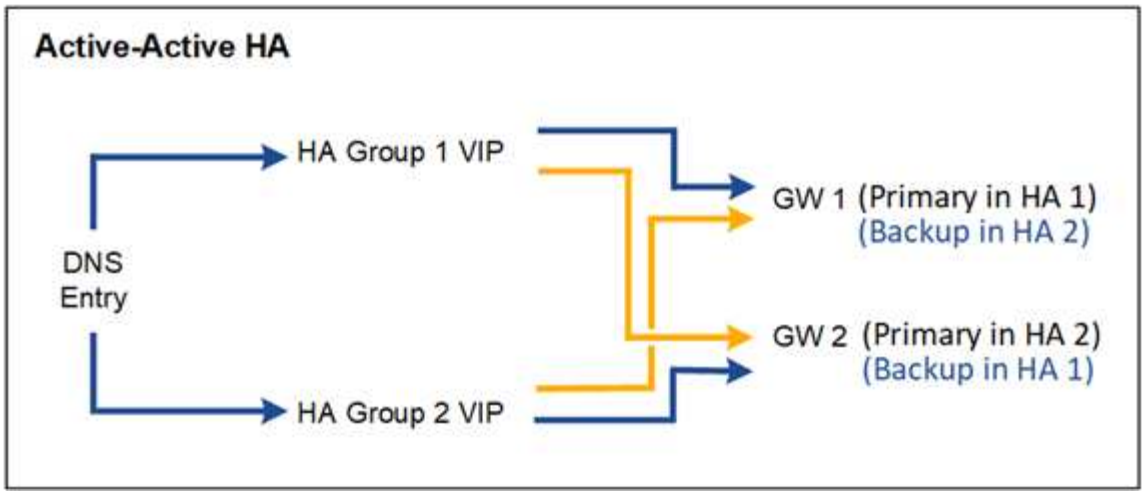
Einige Wartungsverfahren können nicht durchgeführt werden, wenn der primäre Admin-Knoten nicht verfügbar ist. Während des Failovers können Sie den Grid Manager verwenden, um Ihr StorageGRID System zu überwachen.

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

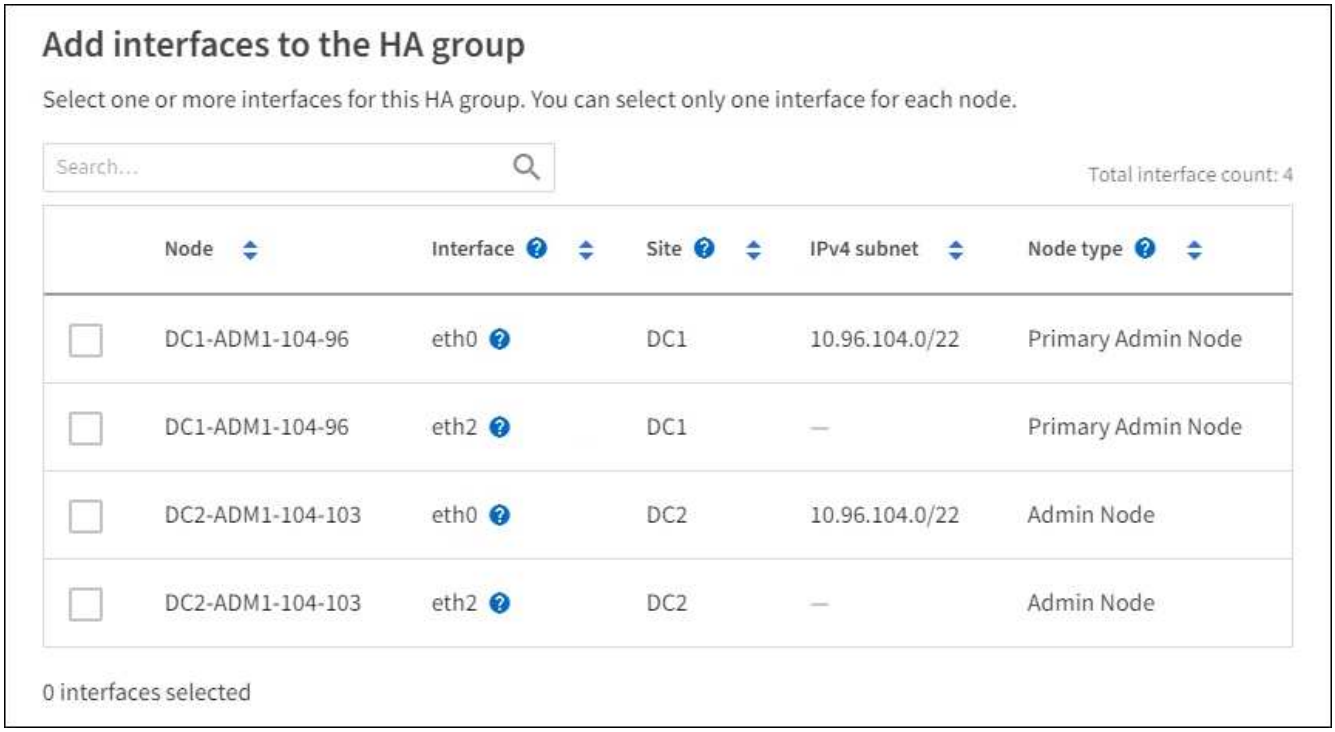
1. Geben Sie einen eindeutigen Namen für die HA-Gruppe an.
2. Geben Sie optional eine Beschreibung für die HA-Gruppe ein.
3. Wählen Sie **Weiter**.

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.

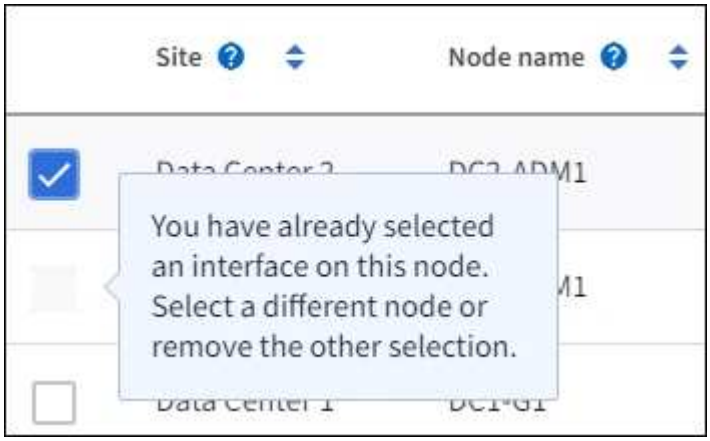


> Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

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**.

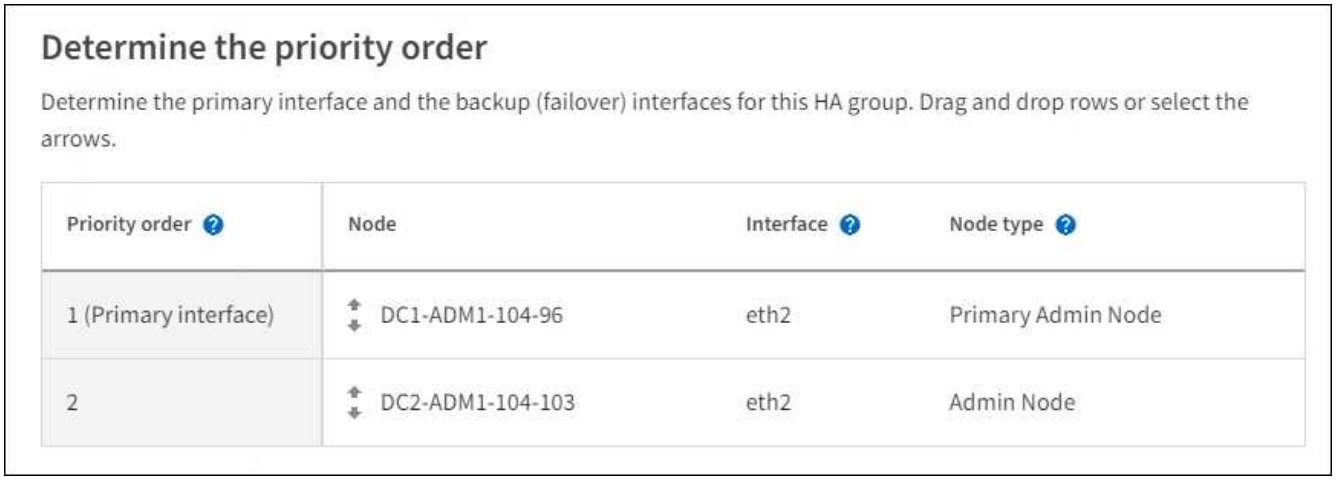
Bestimmen Sie die Prioritätsreihenfolge

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**.

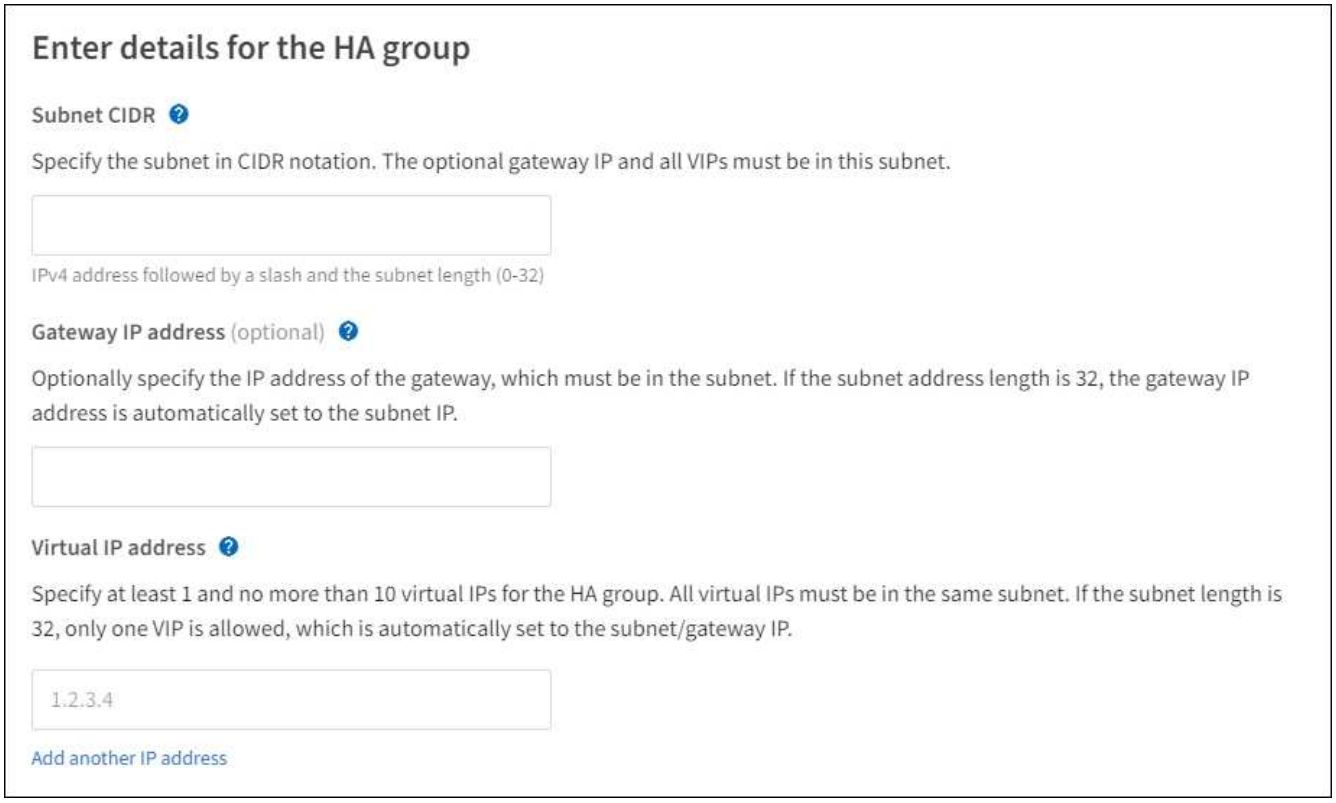
IP-Adressen eingeben

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.

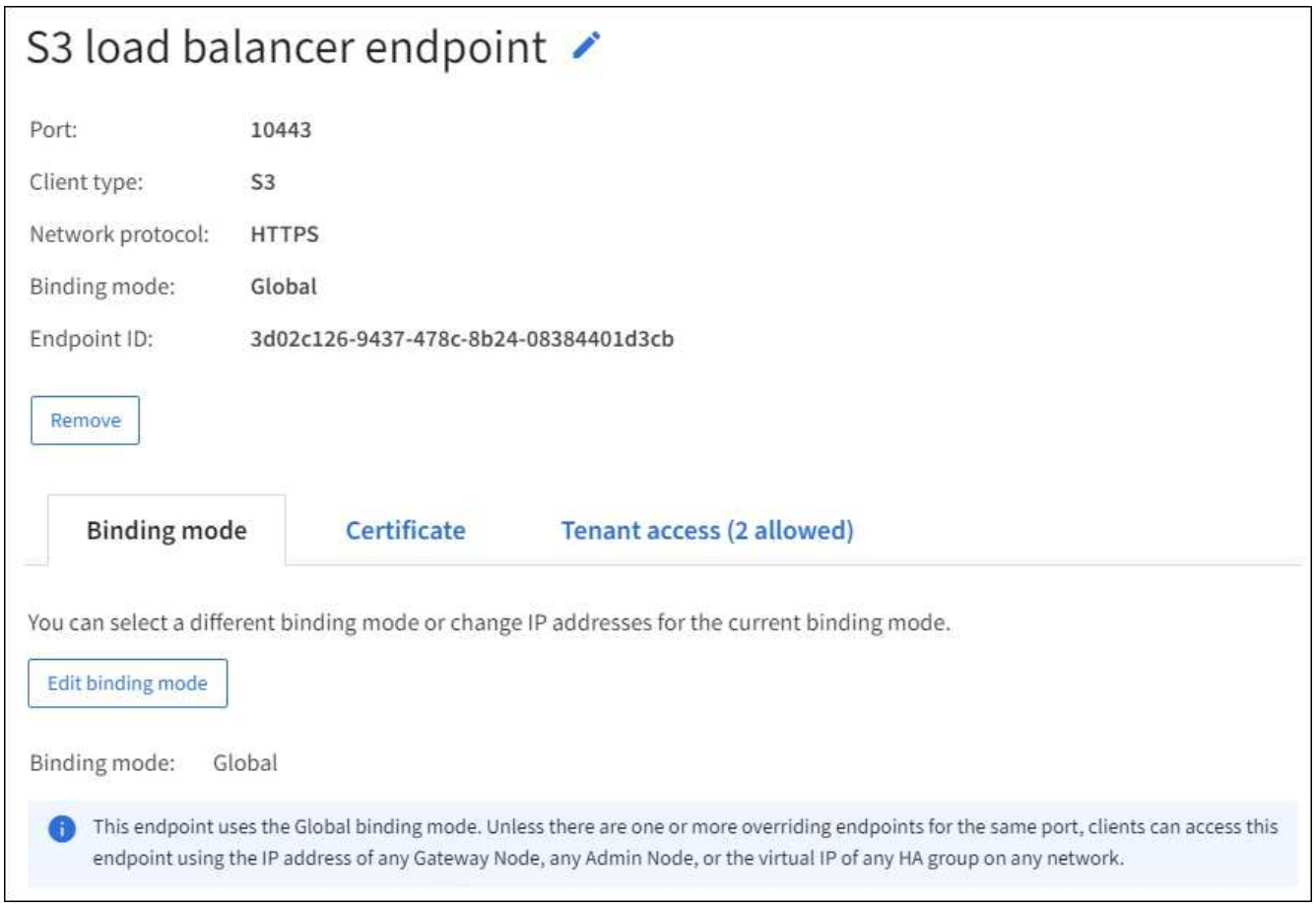
  Sie müssen außerdem sicherstellen, dass der DNS-Eintrag auf alle erforderlichen Endpunktdomänennamen verweist, einschließlich aller Platzhalternamen.

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" .

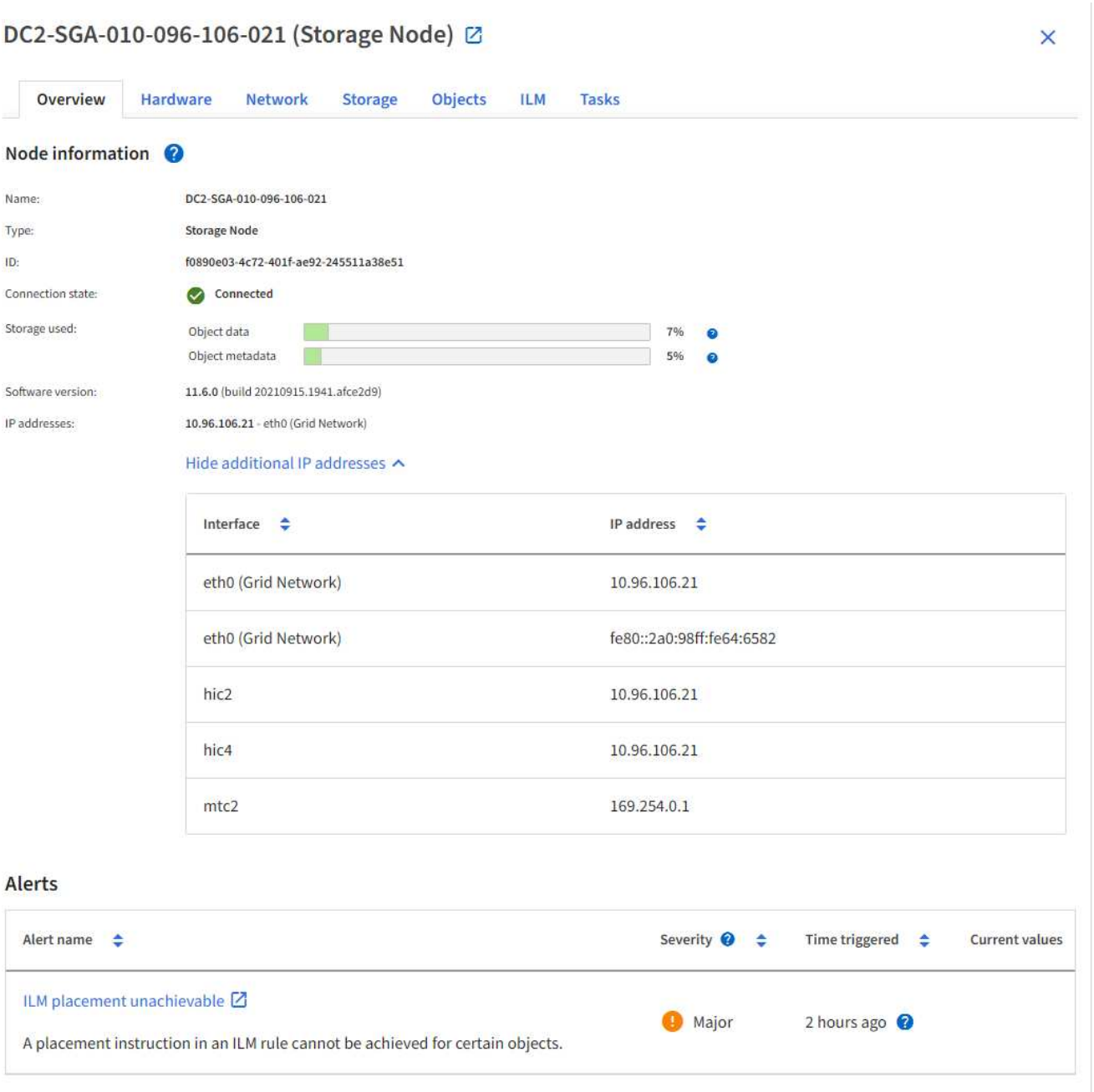
Informationen zu diesem Vorgang

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.

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**.

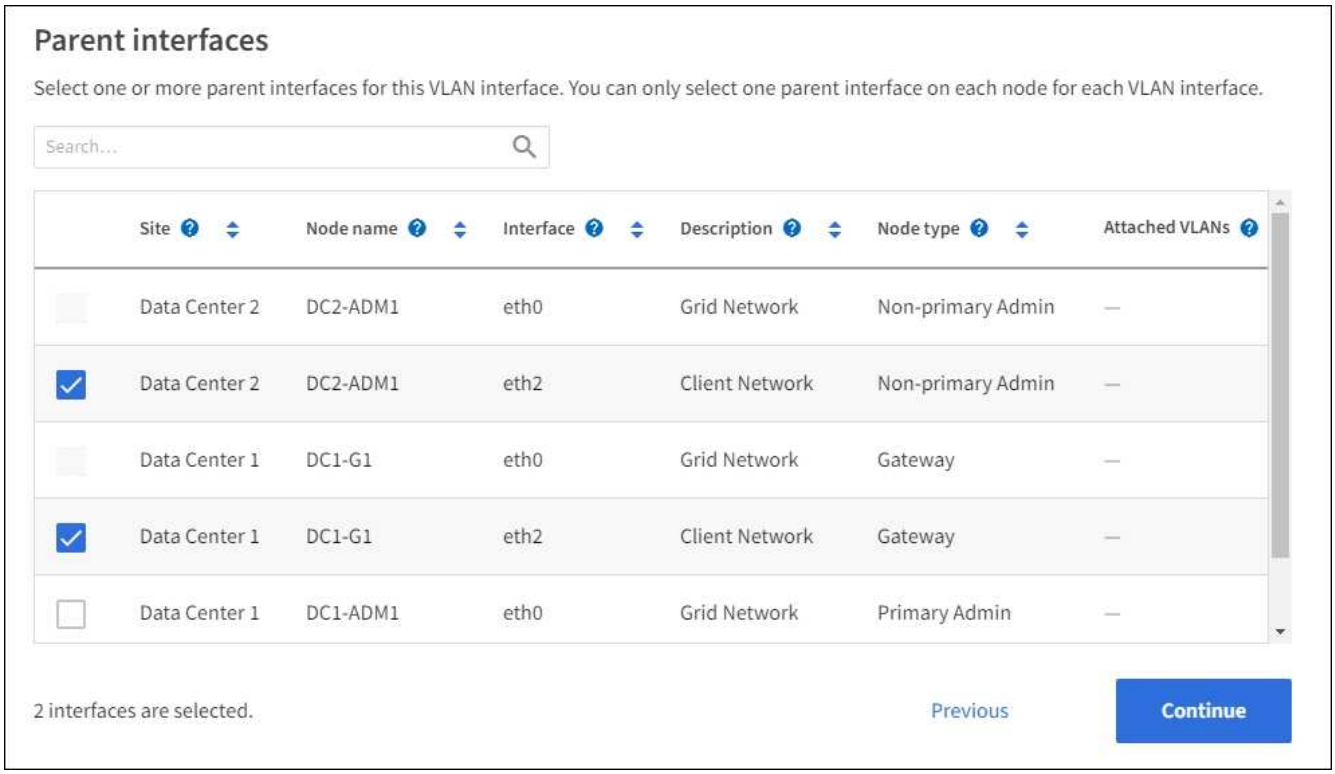
Übergeordnete Schnittstellen auswählen

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	$$$ pro Monat
Silber	250 TB Speicher erlaubt	2 ILM-Kopienregel	10.000 Anfragen/Sek. 1,25 GB/s (10 Gbit/s) Bandbreite	$$ 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.
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**.

Feld	Beschreibung
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.

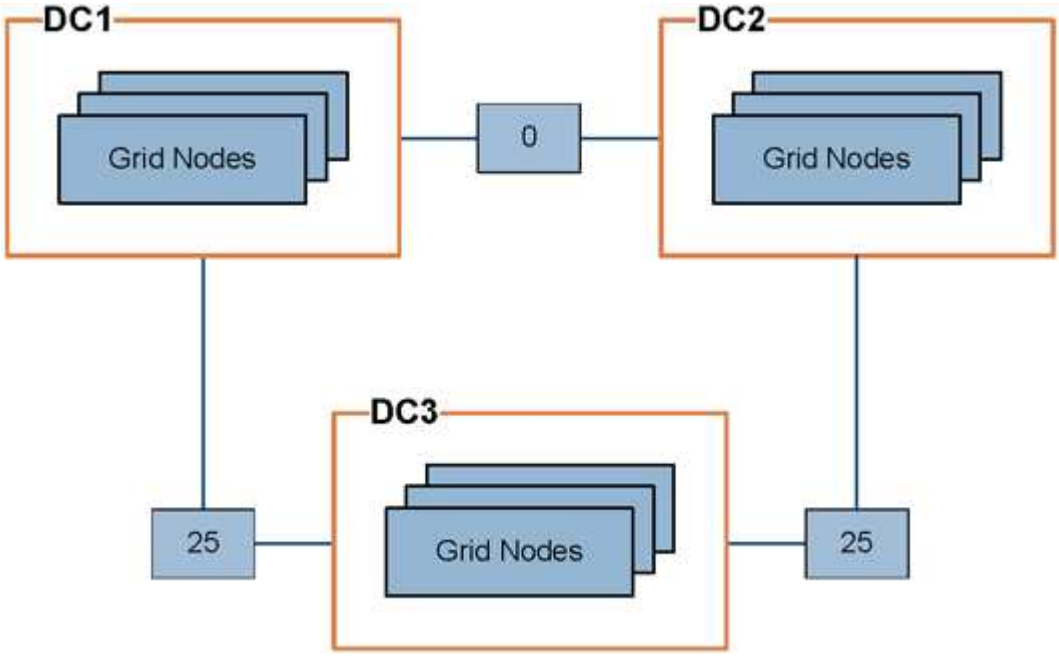
Linkkosten verwalten

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

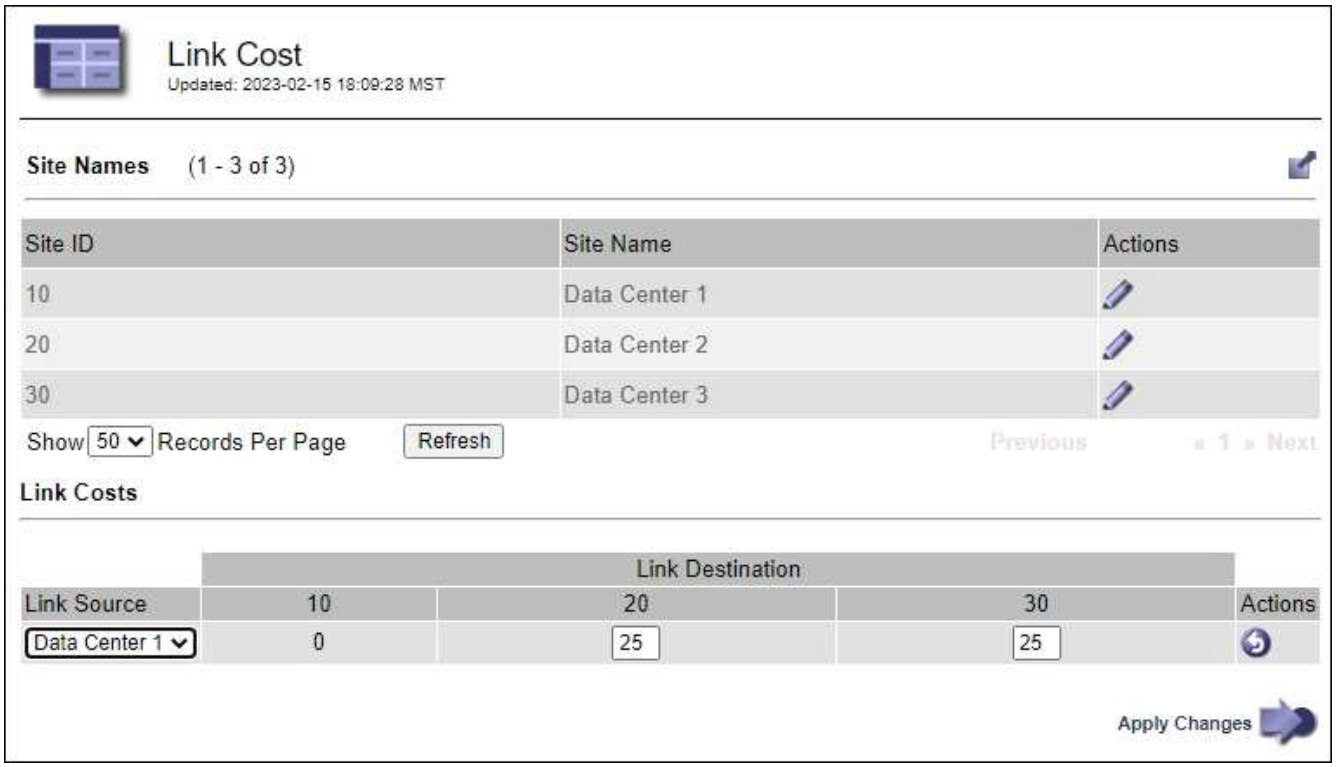
Sie können die Verbindungskosten zwischen Rechenzentrumsstandorten aktualisieren, um die Latenz zwischen den Standorten widerzuspiegeln.

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.

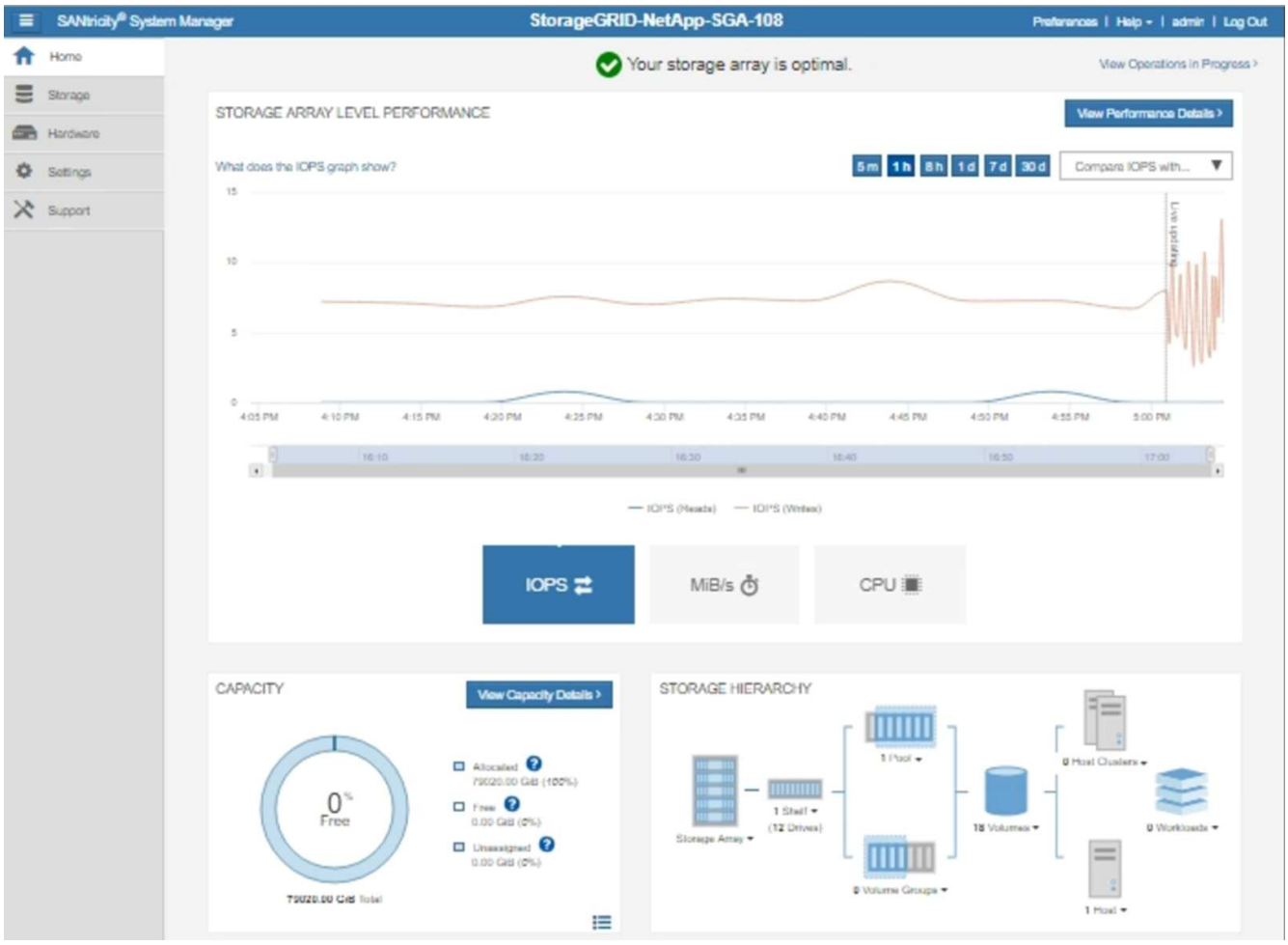
Sie können im SANtricity System Manager eine spezielle Proxyserveradresse konfigurieren, um AutoSupport Pakete über einen StorageGRID Admin-Knoten zu übertragen, ohne den Verwaltungsport des Geräts zu verwenden. Die so übermittelten AutoSupport -Pakete werden von der"bevorzugter Absender-Admin-Knoten" 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

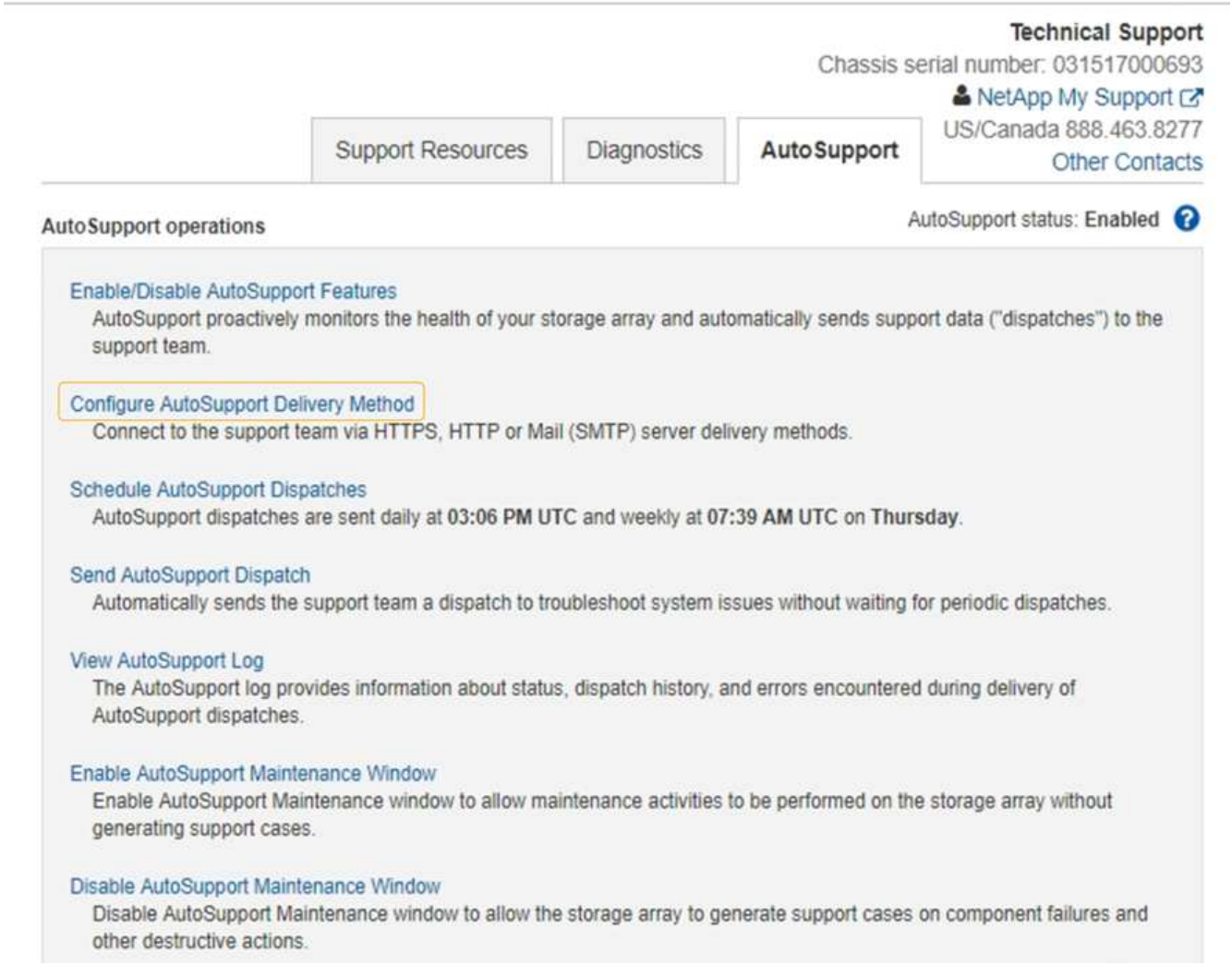
1. Wählen Sie im Grid Manager **NODES** aus.
2. Wählen Sie aus der Knotenliste auf der linken Seite den Speichergeräteknoten aus, den Sie konfigurieren möchten.
3. Wählen Sie * SANtricity System Manager*.

   Die Homepage des SANtricity System Managers wird angezeigt.



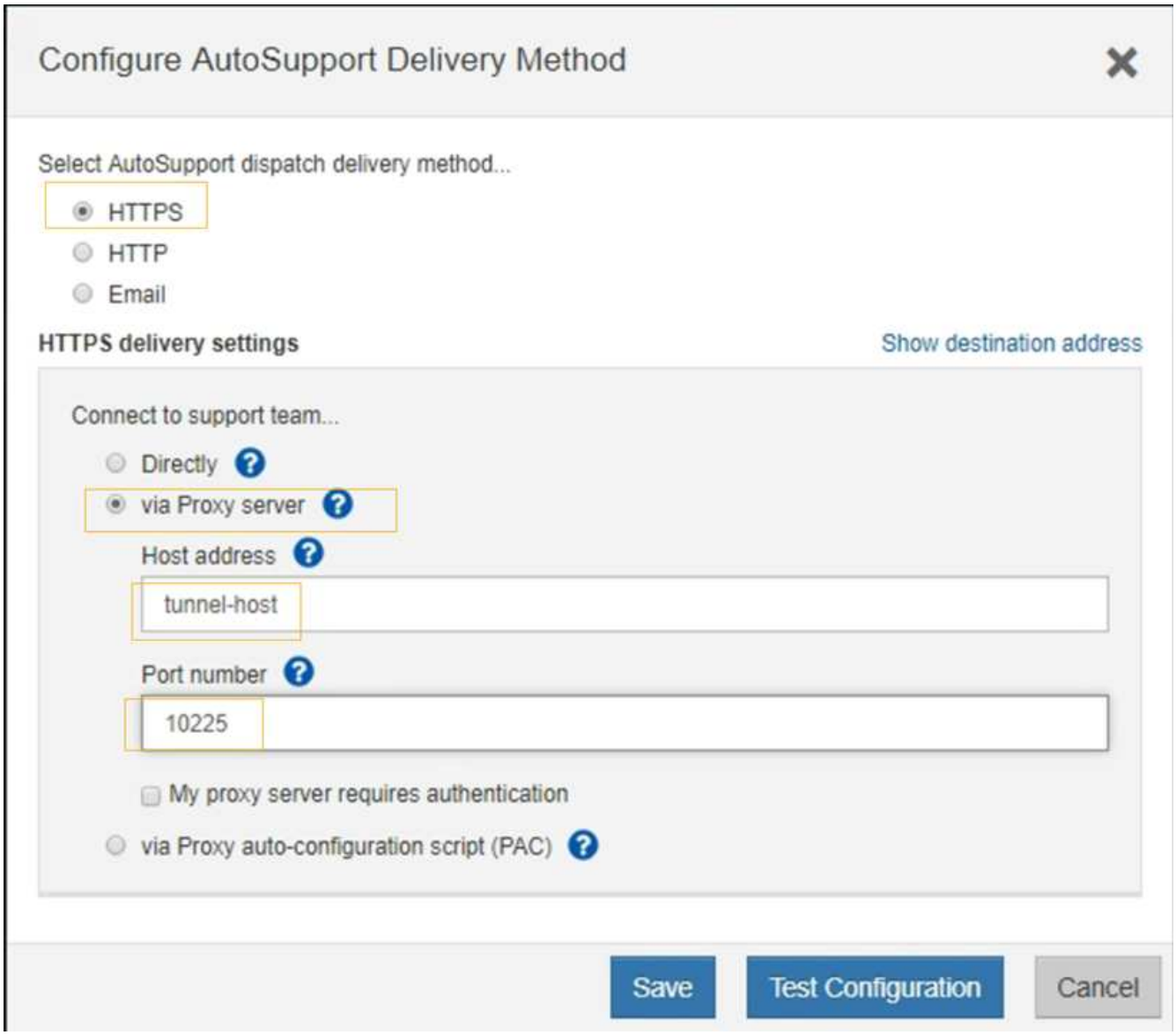
4. Wählen Sie **SUPPORT** > **Supportcenter** > * AutoSupport*.

   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:

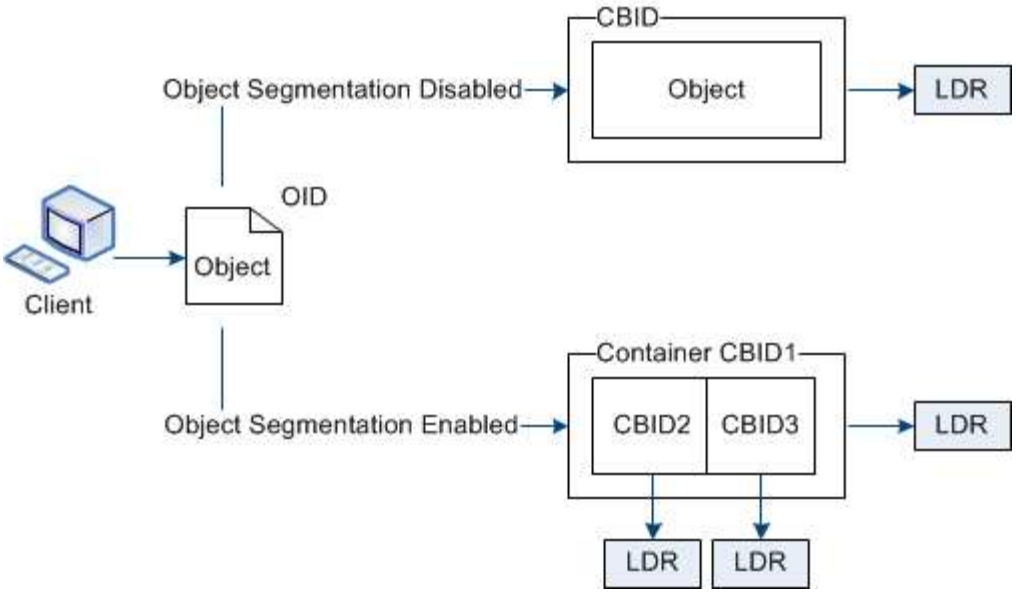
- Verwalten von Speicheroptionen
- Verstehen, was Speichervolumen-Wasserzeichen sind und wie Sie mithilfe von Wasserzeichen-Überschreibungen steuern können, wann Speicherknoten schreibgeschützt werden.
- Überwachung und Verwaltung des für Objektmetadaten verwendeten Speicherplatzes
- Konfigurieren globaler 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.

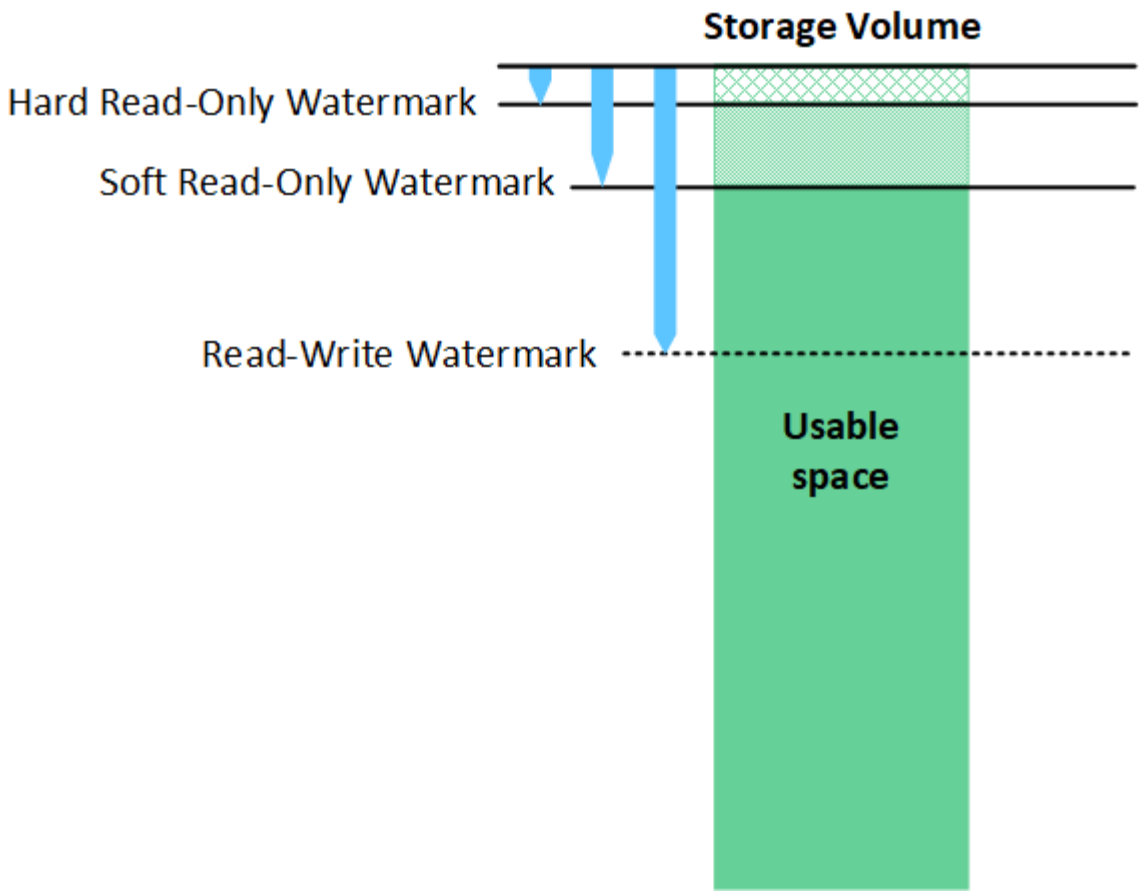
Der Container und die Segmente werden nicht unbedingt auf demselben Speicherknoten gespeichert. Container und Segmente können auf jedem Speicherknoten innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

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:

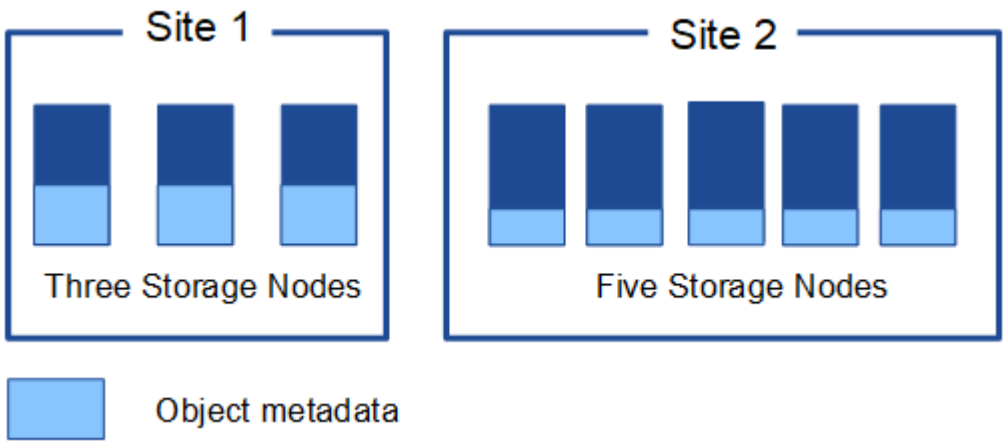
- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), des Objektnamens, des Namens des S3-Buckets, des Mandantenkontonamens oder der ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Objekterstellung sowie des Datums und der Uhrzeit der letzten Objektänderung.

- 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?

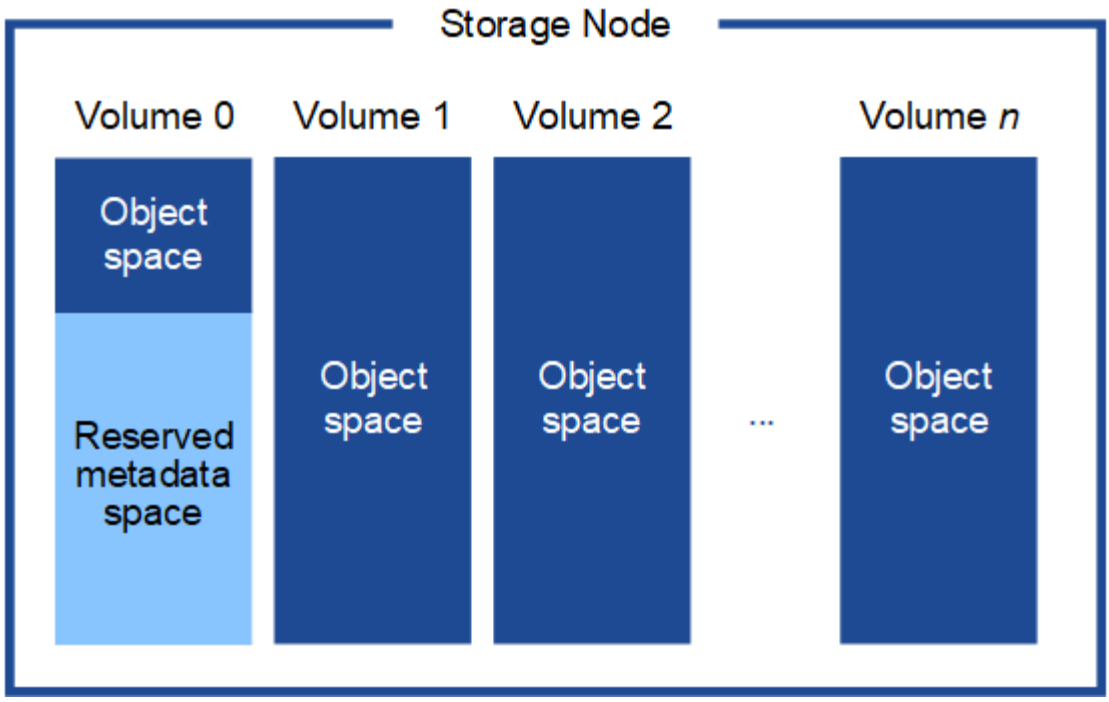
StorageGRID verwaltet Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert wird. Um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen, speichert StorageGRID an jedem Standort drei Kopien der Metadaten für alle Objekte im System.

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.

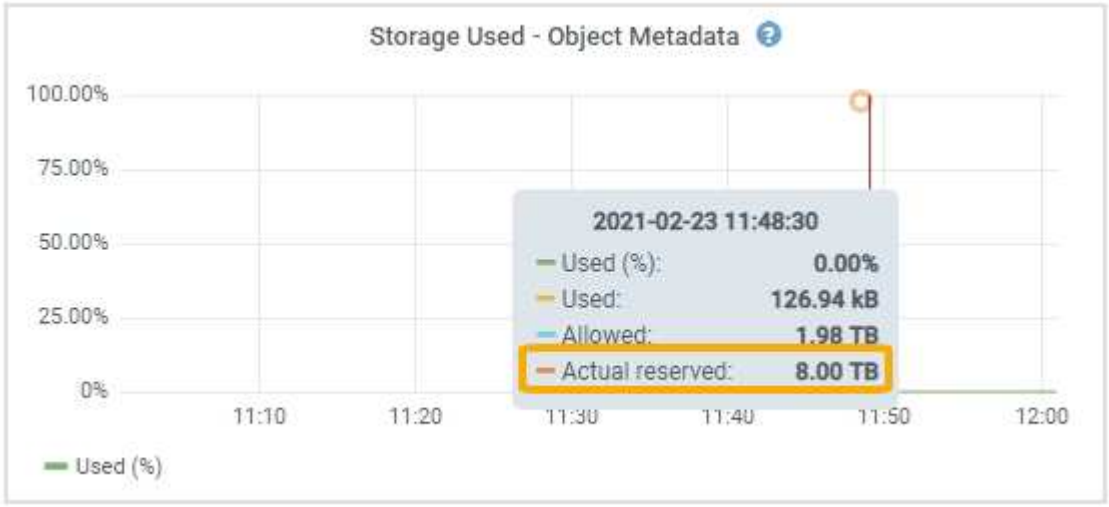
Größe des Datenträgers 0 für den Knoten	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht produktive Nutzung)	10% des Volumens 0
500 GB oder mehr + oder + Nur-Metadaten-Speicherknoten	Der kleinere dieser Werte: • Band 0 • Einstellung für reservierten Speicherplatz für Metadaten **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.

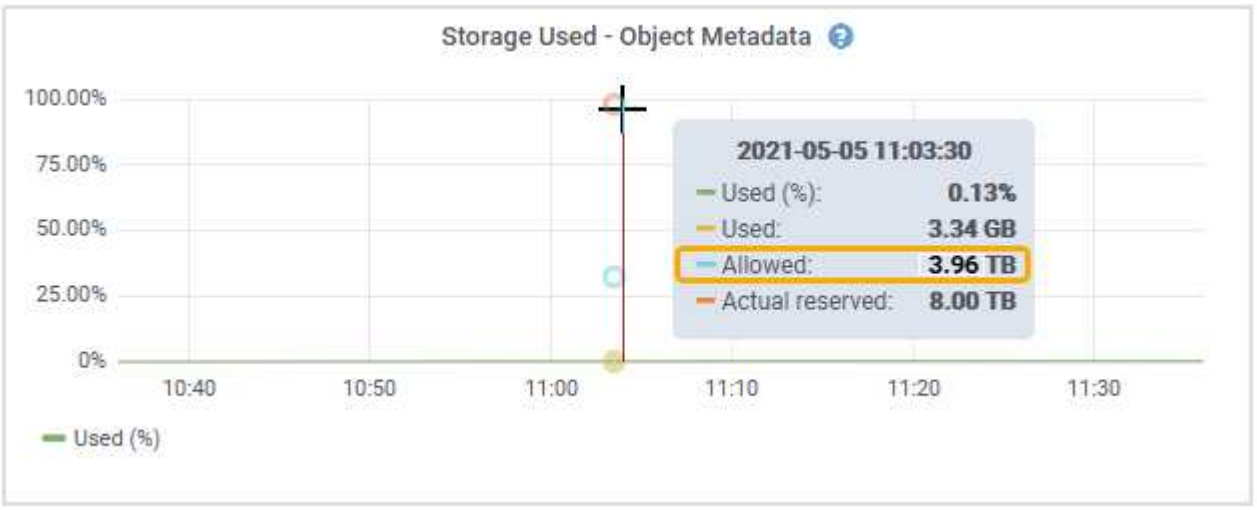
		Speichermenge auf dem Speicherknoten	
	< 128 GB	>= 128 GB	**Tatsächlich reservierter Speicherplatz für Metadaten**
⇐ 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten, bis zu einem Maximum von 1,32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten, bis zu einem Maximum 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

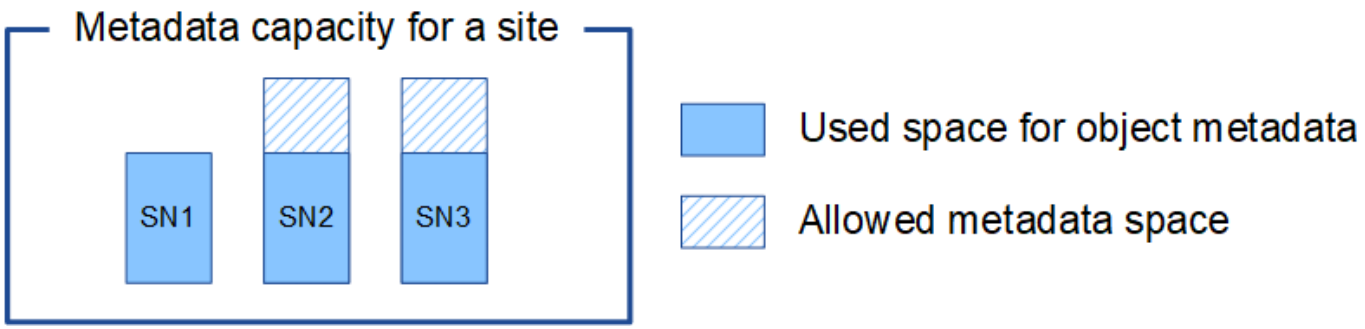
Wie oben beschrieben, verteilt StorageGRID die Objektmetadaten gleichmäßig auf die Speicherknoten an jedem Standort. Wenn eine Site Speicherknoten unterschiedlicher Größe enthält, bestimmt daher der kleinste Knoten an der Site die Metadatenkapazität der Site.

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

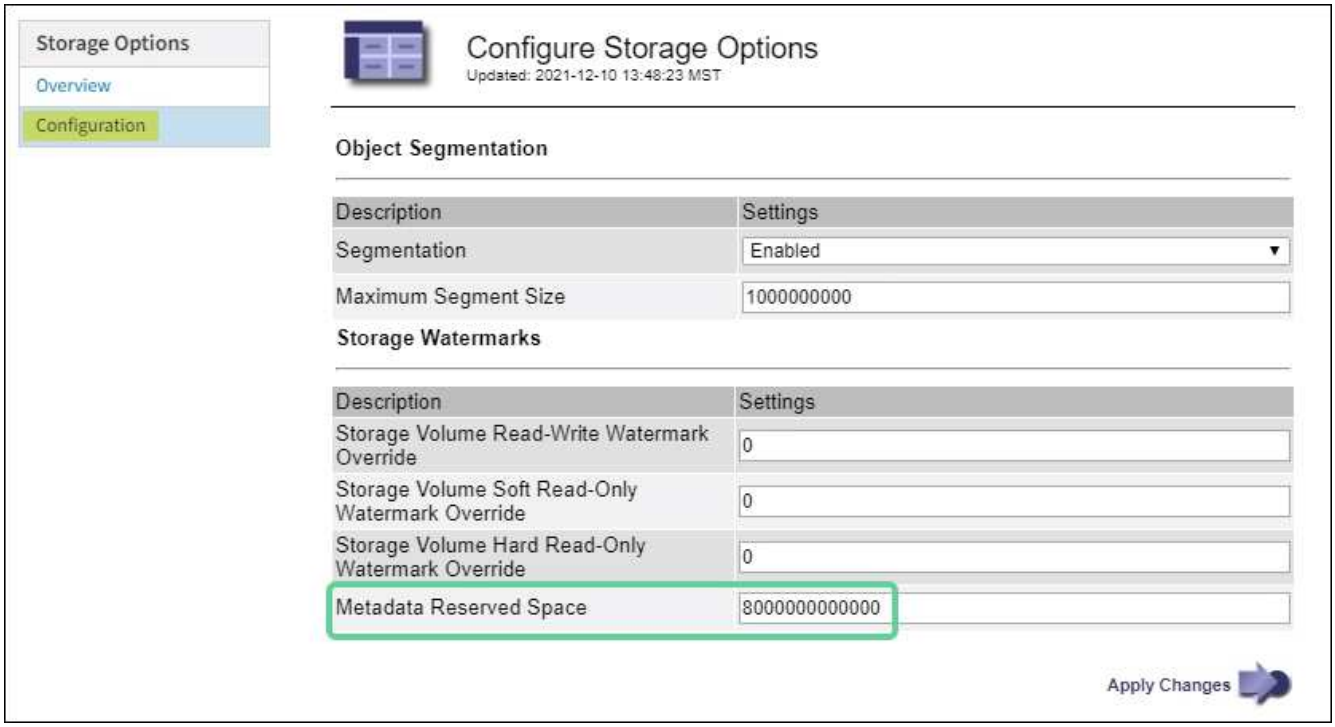
1. Ermitteln Sie die aktuelle Einstellung für den reservierten Speicherplatz für Metadaten.
   a. Wählen Sie **KONFIGURATION** > **System** > **Speicheroptionen**.
   b. Beachten Sie im Abschnitt „Speicherwasserzeichen“ den Wert von „**Reservierter Speicherplatz für Metadaten**“.
2. Stellen Sie sicher, 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" .

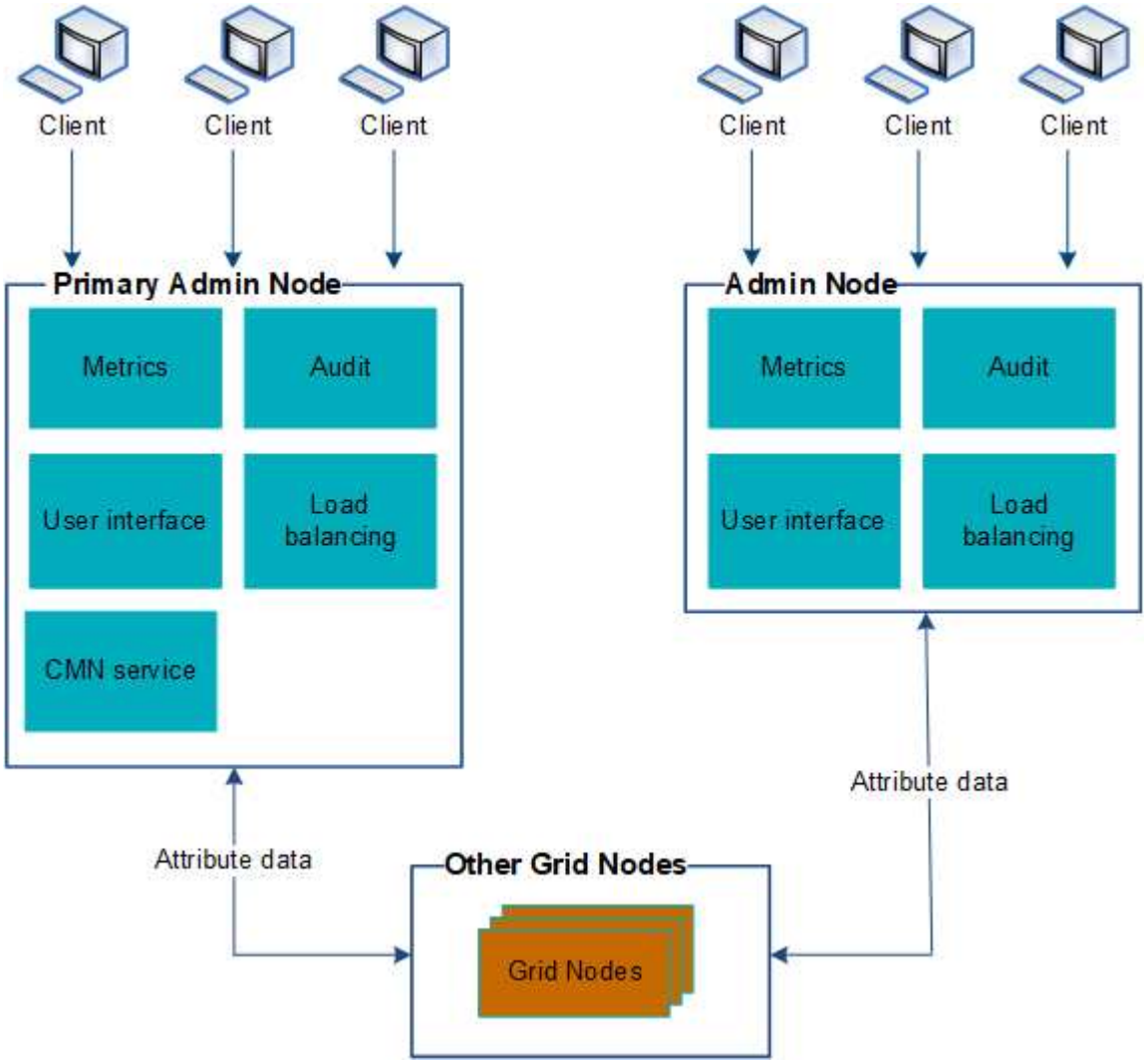
Admin-Knoten verwalten

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

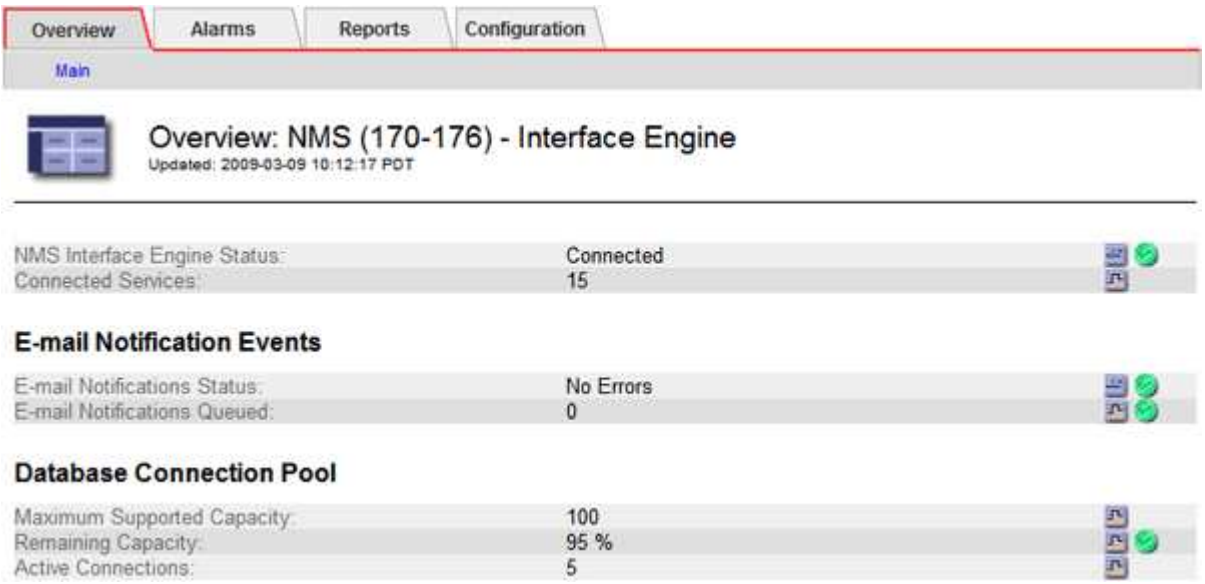
1. Wählen Sie **NODES**.
2. Geben Sie **primary** in das Suchfeld ein.

   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.

Objekte mit ILM verwalten

Objekte mit ILM verwalten

Die Regeln für das Information Lifecycle Management (ILM) in einer ILM-Richtlinie weisen StorageGRID an, wie Kopien von Objektdaten erstellt und verteilt und wie diese Kopien im Laufe der Zeit verwaltet werden.

Zu dieser Anleitung

Das Entwerfen und Implementieren von ILM-Regeln und -Richtlinien erfordert eine sorgfältige Planung. Sie müssen Ihre Betriebsanforderungen, die Topologie Ihres StorageGRID -Systems, Ihren Bedarf an Objektschutz und die verfügbaren Speichertypen verstehen. Anschließend müssen Sie festlegen, wie die verschiedenen Objekttypen kopiert, verteilt und gespeichert werden sollen.

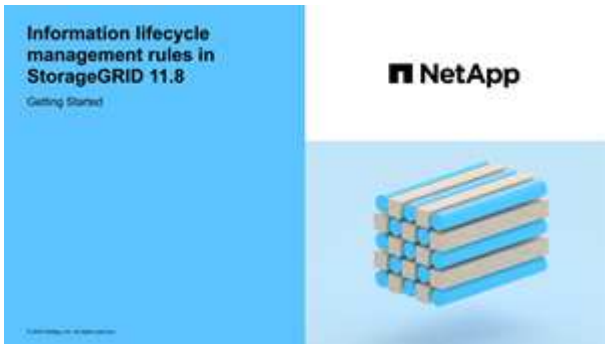
Verwenden Sie diese Anweisungen, um:

- Erfahren Sie mehr über StorageGRID ILM, einschließlich"wie ILM während der gesamten Lebensdauer eines Objekts funktioniert" .
- Erfahren Sie, wie Sie konfigurieren"Speicherpools" ,"Cloud-Speicherpools" , Und"ILM-Regeln" .
- Erfahren Sie, wie Sie"Erstellen, Simulieren und Aktivieren einer ILM-Richtlinie" das Objektdaten an einem oder mehreren Standorten schützt.
- Erfahren Sie, wie Sie"Objekte mit S3 Object Lock verwalten" , wodurch sichergestellt wird, dass Objekte in bestimmten S3-Buckets für einen bestimmten Zeitraum nicht gelöscht oder überschrieben werden.

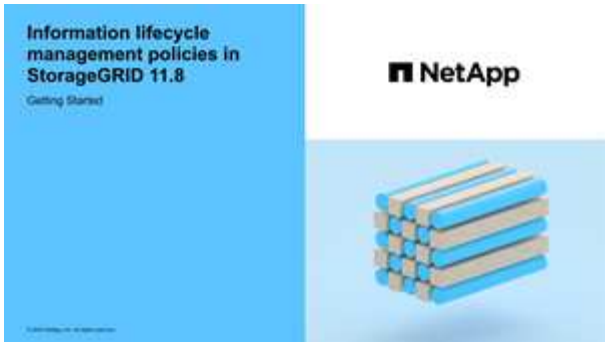
Mehr erfahren

Um mehr zu erfahren, sehen Sie sich diese Videos an:

- "Video: Übersicht über ILM-Regeln" .



- "Video: Übersicht über ILM-Richtlinien"



ILM und Objektlebenszyklus

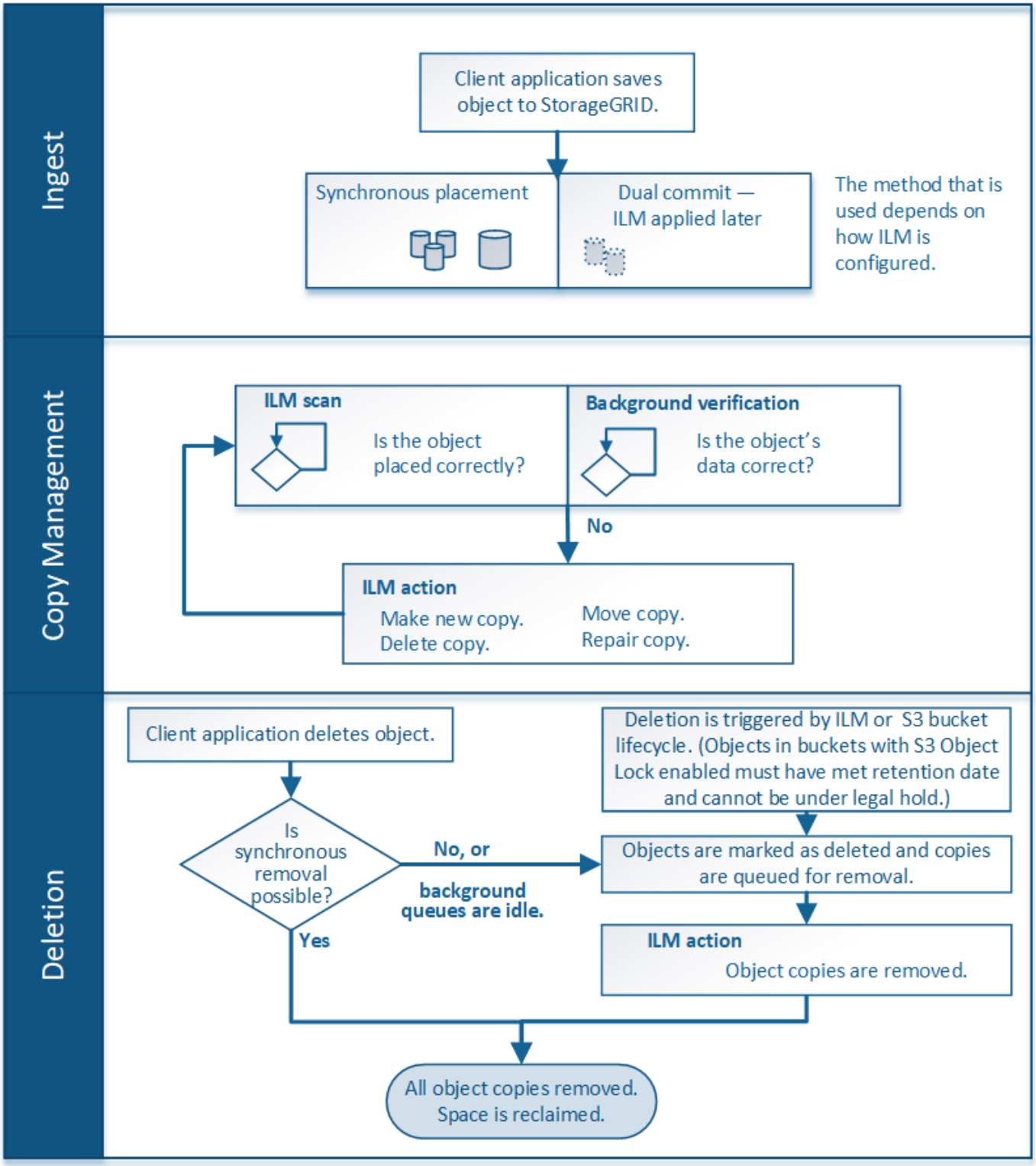
Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts

Wenn Sie verstehen, wie StorageGRID ILM verwendet, um Objekte in jeder Phase ihres Lebenszyklus zu verwalten, können Sie eine effektivere Richtlinie entwerfen.

- **Aufnahme**: Die Aufnahme beginnt, wenn eine S3-Clientanwendung eine Verbindung herstellt, um ein Objekt im StorageGRID -System zu speichern, und ist abgeschlossen, wenn StorageGRID dem Client die Meldung „Aufnahme erfolgreich“ zurückgibt. Der Schutz der Objektdaten erfolgt während der Aufnahme entweder durch sofortiges Anwenden von ILM-Anweisungen (synchrone Platzierung) oder durch Erstellen von Zwischenkopien und späteres Anwenden von ILM (Dual Commit), je nachdem, wie die ILM-Anforderungen festgelegt wurden.
- **Kopienverwaltung**: Nachdem die Anzahl und Art der Objektkopien erstellt wurden, die in den Platzierungsanweisungen des ILM angegeben sind, verwaltet StorageGRID die Objektstandorte und schützt Objekte vor Verlust.
  - **ILM-Scan und -Auswertung**: StorageGRID scannt kontinuierlich die Liste der im Grid gespeicherten Objekte und prüft, ob die aktuellen Kopien die ILM-Anforderungen erfüllen. Wenn unterschiedliche Typen, Anzahlen oder Speicherorte von Objektkopien erforderlich sind, erstellt, löscht oder verschiebt StorageGRID Kopien nach Bedarf.
  - **Hintergrundüberprüfung**: StorageGRID führt kontinuierlich eine Hintergrundüberprüfung durch, um die Integrität der Objektdaten zu überprüfen. Wenn ein Problem gefunden wird, erstellt StorageGRID automatisch eine neue Objektkopie oder ein Ersatz-Löschcodiertes Objektfragment an einem Speicherort, der den aktuellen ILM-Anforderungen entspricht. Sehen "Überprüfen der Objektintegrität" .
- **Objektlöschung**: Die Verwaltung eines Objekts endet, wenn alle Kopien aus dem StorageGRID -System entfernt wurden. Objekte können aufgrund einer Löschanforderung eines Clients oder aufgrund einer Löschung durch ILM oder einer Löschung aufgrund des Ablaufs des Lebenszyklus eines S3-Buckets entfernt werden.

> Objekte in einem Bucket mit aktivierter S3-Objektsperre können nicht gelöscht werden, wenn sie einer rechtlichen Sperre unterliegen oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erreicht wurde.

Das Diagramm fasst zusammen, wie ILM während des gesamten Lebenszyklus eines Objekts funktioniert.



Wie Objekte aufgenommen werden

Aufnahmeoptionen

Wenn Sie eine ILM-Regel erstellen, geben Sie eine von drei Optionen zum Schutz von Objekten bei der Aufnahme an: Dual Commit, Streng oder Ausgewogen.

Je nach Ihrer Wahl erstellt StorageGRID Zwischenkopien und stellt die Objekte für eine spätere ILM-

Auswertung in die Warteschlange oder verwendet die synchrone Platzierung und erstellt sofort Kopien, um die ILM-Anforderungen zu erfüllen.

Flussdiagramm der Aufnahmeoptionen

Das Flussdiagramm zeigt, was passiert, wenn Objekte mit einer ILM-Regel abgeglichen werden, die jede der drei Aufnahmeoptionen verwendet.

Doppeltes Commit

Wenn Sie die Option „Dual Commit“ auswählen, erstellt StorageGRID sofort vorläufige Objektkopien auf zwei verschiedenen Speicherknoten und gibt die Meldung „Aufnahme erfolgreich“ an den Client zurück. Das Objekt wird zur ILM-Auswertung in die Warteschlange gestellt und später werden Kopien erstellt, die den Platzierungsanweisungen der Regel entsprechen. Wenn die ILM-Richtlinie nicht unmittelbar nach dem doppelten Commit verarbeitet werden kann, kann es einige Zeit dauern, bis der Site-Loss-Schutz erreicht ist.

Verwenden Sie in einem der folgenden Fälle die Option „Dual Commit“:

- Sie verwenden ILM-Regeln für mehrere Standorte und die Latenzzeit bei der Clientaufnahme ist Ihr Hauptanliegen. Wenn Sie Dual Commit verwenden, müssen Sie sicherstellen, dass Ihr Grid die zusätzliche Arbeit des Erstellens und Entfernens der Dual-Commit-Kopien ausführen kann, wenn diese ILM nicht erfüllen. Speziell:
  - Die Netzbelastung muss gering genug sein, um einen ILM-Rückstau zu verhindern.
  - Das Grid muss über überschüssige Hardwareressourcen (IOPS, CPU, Speicher, Netzwerkbandbreite usw.) verfügen.
- Sie verwenden ILM-Regeln für mehrere Standorte und die WAN-Verbindung zwischen den Standorten weist normalerweise eine hohe Latenz oder begrenzte Bandbreite auf. In diesem Szenario kann die Verwendung der Option „Dual Commit“ dazu beitragen, Client-Timeouts zu verhindern. Bevor Sie sich für die Option „Dual Commit“ entscheiden, sollten Sie die Clientanwendung mit realistischen Arbeitslasten testen.

Ausgeglichen (Standard)

Wenn Sie die Option „Ausgewogen“ auswählen, verwendet StorageGRID auch die synchrone Platzierung bei der Aufnahme und erstellt sofort alle in den Platzierungsanweisungen der Regel angegebenen Kopien. Im Gegensatz zur Option „Streng“ verwendet StorageGRID stattdessen „Dual Commit“, wenn es nicht sofort alle Kopien erstellen kann. Wenn die ILM-Richtlinie Platzierungen auf mehreren Sites verwendet und kein sofortiger Schutz vor Site-Verlust erreicht werden kann, wird die Warnung „ILM-Platzierung nicht erreichbar“ ausgelöst.

Verwenden Sie die Option „Ausgewogen“, um die beste Kombination aus Datenschutz, Grid-Leistung und Aufnahmeerfolg zu erzielen. „Ausgeglichen“ ist die Standardoption im Assistenten „ILM-Regel erstellen“.

Strikt

Wenn Sie die Option „Streng“ auswählen, verwendet StorageGRID bei der Aufnahme die synchrone Platzierung und erstellt sofort alle in den Platzierungsanweisungen der Regel angegebenen Objektkopien. Die Aufnahme schlägt fehl, wenn StorageGRID nicht alle Kopien erstellen kann, beispielsweise weil ein erforderlicher Speicherort vorübergehend nicht verfügbar ist. Der Client muss den Vorgang wiederholen.

Verwenden Sie die Option „Streng“, wenn für Sie eine betriebliche oder gesetzliche Anforderung besteht, Objekte sofort nur an den in der ILM-Regel angegebenen Orten zu speichern. Um beispielsweise eine

gesetzliche Anforderung zu erfüllen, müssen Sie möglicherweise die Option „Streng“ und einen erweiterten Filter „Standortbeschränkung“ verwenden, um sicherzustellen, dass Objekte niemals in bestimmten Rechenzentren gespeichert werden.

Sehen "Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten" .

Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen

Wenn Sie die Vor- und Nachteile der drei Optionen zum Schutz von Daten bei der Aufnahme (Balanced, Strict oder Dual Commit) kennen, können Sie leichter entscheiden, welche Option Sie für eine ILM-Regel auswählen.

Eine Übersicht über die Aufnahmeoptionen finden Sie unter"Aufnahmeoptionen" .

Vorteile der Optionen „Ausgewogen“ und „Streng“

Im Vergleich zum Dual Commit, bei dem während der Aufnahme Zwischenkopien erstellt werden, können die beiden synchronen Platzierungsoptionen die folgenden Vorteile bieten:

- **Bessere Datensicherheit**: Objektdaten werden sofort gemäß den Platzierungsanweisungen der ILM-Regel geschützt. Diese können so konfiguriert werden, dass sie vor einer Vielzahl von Fehlerbedingungen schützen, einschließlich des Ausfalls von mehr als einem Speicherort. Dual Commit kann nur vor dem Verlust einer einzigen lokalen Kopie schützen.
- **Effizienterer Grid-Betrieb**: Jedes Objekt wird bei der Aufnahme nur einmal verarbeitet. Da das StorageGRID -System keine Zwischenkopien verfolgen oder löschen muss, ist die Verarbeitungslast geringer und es wird weniger Datenbankspeicherplatz verbraucht.
- **(Ausgewogen) Empfohlen**: Die Option „Ausgewogen“ bietet optimale ILM-Effizienz. Die Verwendung der Option „Ausgewogen“ wird empfohlen, es sei denn, es ist ein striktes Aufnahmeverhalten erforderlich oder das Raster erfüllt alle Kriterien für die Verwendung von Dual Commit.
- **(Strenge) Sicherheit bezüglich der Objektstandorte**: Die Option „Strenge“ garantiert, dass Objekte sofort gemäß den Platzierungsanweisungen in der ILM-Regel gespeichert werden.

Nachteile der Optionen „Ausgewogen“ und „Streng“

Im Vergleich zu Dual Commit haben die Optionen Balanced und Strict einige Nachteile:

- **Längere Client-Aufnahmen**: Die Latenzen bei der Client-Aufnahme können länger sein. Wenn Sie die Optionen „Ausgewogen“ oder „Streng“ verwenden, wird die Meldung „Aufnahme erfolgreich“ erst dann an den Client zurückgegeben, wenn alle Erasure-Coded-Fragmente oder replizierten Kopien erstellt und gespeichert wurden. Allerdings erreichen die Objektdaten ihre endgültige Platzierung höchstwahrscheinlich viel schneller.
- **(Streng) Höhere Fehlerraten bei der Aufnahme**: Bei der Option „Streng“ schlägt die Aufnahme fehl, wenn StorageGRID nicht sofort alle in der ILM-Regel angegebenen Kopien erstellen kann. Wenn ein erforderlicher Speicherort vorübergehend offline ist oder wenn Netzwerkprobleme zu Verzögerungen beim Kopieren von Objekten zwischen Sites führen, kann es zu hohen Aufnahmefehlerraten kommen.
- **(Streng) Platzierungen von mehrteiligen S3-Uploads können unter bestimmten Umständen nicht wie erwartet erfolgen**: Bei „Streng“ erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Bei einem mehrteiligen S3-Upload wird ILM jedoch für jeden Teil des Objekts beim Einlesen und für das gesamte Objekt ausgewertet, wenn der mehrteilige Upload abgeschlossen ist. Unter folgenden Umständen kann dies zu Platzierungen führen, die anders ausfallen als erwartet:

    - **Wenn sich ILM während eines laufenden S3-Multipart-Uploads ändert**: Da jeder Teil gemäß der Regel platziert wird, die beim Aufnehmen des Teils aktiv ist, erfüllen einige Teile des Objekts möglicherweise nicht die aktuellen ILM-Anforderungen, wenn der Multipart-Upload abgeschlossen ist. In diesen Fällen schlägt die Aufnahme des Objekts nicht fehl. Stattdessen wird jedes Teil, das nicht richtig platziert ist, zur erneuten ILM-Bewertung in die Warteschlange gestellt und später an die richtige Position verschoben.
    - **Wenn ILM-Regeln nach Größe filtern**: Beim Auswerten von ILM für ein Teil filtert StorageGRID nach der Größe des Teils, nicht nach der Größe des Objekts. Dies bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn beispielsweise eine Regel angibt, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert werden, wird bei der Aufnahme jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei DC2 gespeichert. Wenn ILM für das Objekt ausgewertet wird, werden alle Teile des Objekts nach DC1 verschoben.
- **(Streng) Die Aufnahme schlägt nicht fehl, wenn Objekt-Tags oder Metadaten aktualisiert werden und neu erforderliche Platzierungen nicht vorgenommen werden können**: Bei „Streng“ erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Wenn Sie jedoch Metadaten oder Tags für ein Objekt aktualisieren, das bereits im Raster gespeichert ist, wird das Objekt nicht erneut aufgenommen. Dies bedeutet, dass alle durch das Update ausgelösten Änderungen an der Objektplatzierung nicht sofort vorgenommen werden. Platzierungsänderungen werden vorgenommen, wenn ILM durch normale ILM-Hintergrundprozesse neu ausgewertet wird. Wenn erforderliche Platzierungsänderungen nicht vorgenommen werden können (beispielsweise weil ein neu erforderlicher Speicherort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung bei, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei der Objektplatzierung mit den Optionen „Ausgewogen“ und „Streng“

Die Optionen „Ausgewogen“ oder „Streng“ können nicht für ILM-Regeln verwendet werden, die eine der folgenden Platzierungsanweisungen enthalten:

- Platzierung in einem Cloud-Speicherpool am Tag 0.
- Platzierungen in einem Cloud-Speicherpool, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit hat.

Diese Einschränkungen bestehen, weil StorageGRID keine synchronen Kopien in einem Cloud-Speicherpool erstellen kann und eine benutzerdefinierte Erstellungszeit bis zur Gegenwart reichen könnte.

Wie sich ILM-Regeln und Konsistenz auf den Datenschutz auswirken

Sowohl Ihre ILM-Regel als auch Ihre Wahl der Konsistenz wirken sich darauf aus, wie Objekte geschützt werden. Diese Einstellungen können interagieren.

Beispielsweise wirkt sich das für eine ILM-Regel ausgewählte Aufnahmeverhalten auf die anfängliche Platzierung von Objektkopien aus, während die beim Speichern eines Objekts verwendete Konsistenz die anfängliche Platzierung von Objektmetadaten beeinflusst. Da StorageGRID zur Erfüllung von Clientanforderungen Zugriff auf die Daten und Metadaten eines Objekts benötigt, kann die Auswahl passender Schutzebenen für Konsistenz und Aufnahmeverhalten einen besseren anfänglichen Datenschutz und vorhersehbarere Systemreaktionen bieten.

Hier ist eine kurze Zusammenfassung der Konsistenzwerte, die in StorageGRID verfügbar sind:

- **Alle**: Alle Knoten erhalten die Objektmetadaten sofort, andernfalls schlägt die Anforderung fehl.
- **Stark-global**: Objektmetadaten werden sofort an alle Sites verteilt. Garantiert Lese- und Schreibkonsistenz für alle Clientanforderungen auf allen Sites.

- **Strong-Site**: Objektmetadaten werden sofort an andere Knoten der Site verteilt. Garantiert die Lese- und Schreibkonsistenz für alle Clientanforderungen innerhalb einer Site.
- **Lesen nach neuem Schreiben**: Bietet Lese-nach-Schreib-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
- **Verfügbar**: Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

> Bevor Sie einen Konsistenzwert auswählen,"Lesen Sie die vollständige Beschreibung der Konsistenz" . Sie sollten die Vorteile und Einschränkungen verstehen, bevor Sie den Standardwert ändern.

Beispiel für die Interaktion von Konsistenz- und ILM-Regeln

Angenommen, Sie haben ein Grid mit zwei Sites mit der folgenden ILM-Regel und der folgenden Konsistenz:

- **ILM-Regel**: Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem Remote-Standort. Verwenden Sie ein striktes Aufnahmeverhalten.
- **Konsistenz**: Stark global (Objektmetadaten werden sofort an alle Sites verteilt).

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID Kopien beider Objekte und verteilt Metadaten an beide Sites, bevor dem Client die Erfolgsmeldung zurückgegeben wird.

Zum Zeitpunkt der erfolgreichen Aufnahme der Nachricht ist das Objekt vollständig vor Verlust geschützt. Wenn beispielsweise die lokale Site kurz nach der Aufnahme verloren geht, sind am Remote-Standort weiterhin Kopien der Objektdaten und der Objektmetadaten vorhanden. Das Objekt ist vollständig abrufbar.

Wenn Sie stattdessen dieselbe ILM-Regel und die starke Site-Konsistenz verwenden, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten auf die Remote-Site repliziert wurden, aber bevor die Objektmetadaten dorthin verteilt werden. In diesem Fall entspricht das Schutzniveau der Objektmetadaten nicht dem Schutzniveau der Objektdaten. Wenn die lokale Site kurz nach der Aufnahme verloren geht, gehen die Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenz und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp , wenn Sie Hilfe benötigen.

Ähnliche Informationen

"Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten"

Wie Objekte gespeichert werden (Replikation oder Erasure Coding)

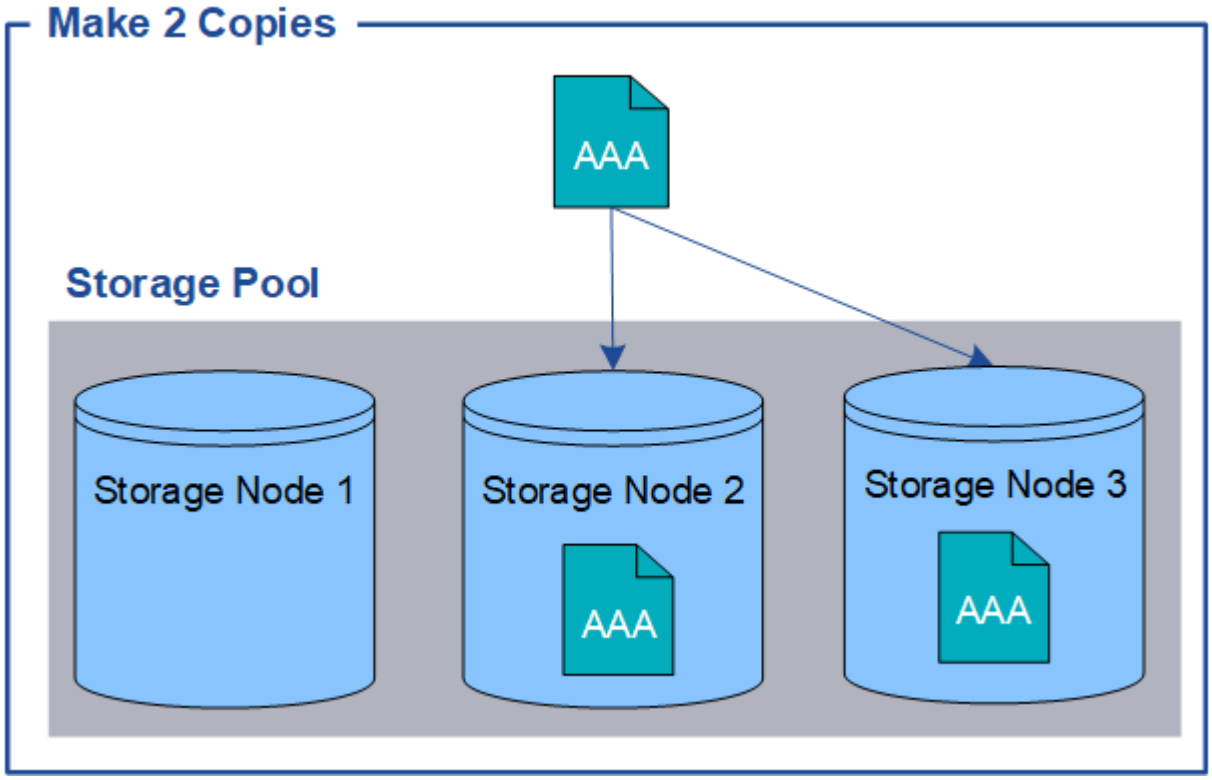
Was ist Replikation?

Die Replikation ist eine von zwei Methoden, die von StorageGRID zum Speichern von Objektdaten verwendet werden (die andere Methode ist Erasure Coding). Wenn Objekte einer ILM-Regel entsprechen, die Replikation verwendet, erstellt das System exakte Kopien der Objektdaten und speichert die Kopien auf Speicherknoten.

Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien konfigurieren, geben Sie an, wie viele Kopien erstellt werden sollen, wo diese Kopien abgelegt werden sollen und wie lange die Kopien an jedem Standort

gespeichert werden sollen.

Im folgenden Beispiel gibt die ILM-Regel an, dass zwei replizierte Kopien jedes Objekts in einem Speicherpool abgelegt werden, der drei Speicherknoten enthält.



Wenn StorageGRID Objekte mit dieser Regel abgleicht, erstellt es zwei Kopien des Objekts und platziert jede Kopie auf einem anderen Speicherknoten im Speicherpool. Die beiden Kopien können auf zwei beliebigen der drei verfügbaren Speicherknoten platziert werden. In diesem Fall platzierte die Regel Objektkopien auf den Speicherknoten 2 und 3. Da zwei Kopien vorhanden sind, kann das Objekt abgerufen werden, wenn einer der Knoten im Speicherpool ausfällt.

> StorageGRID kann auf einem bestimmten Speicherknoten nur eine replizierte Kopie eines Objekts speichern. Wenn Ihr Grid drei Speicherknoten enthält und Sie eine ILM-Regel mit 4 Kopien erstellen, werden nur drei Kopien erstellt – eine Kopie für jeden Speicherknoten. Die Warnung **ILM-Platzierung nicht erreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Ähnliche Informationen

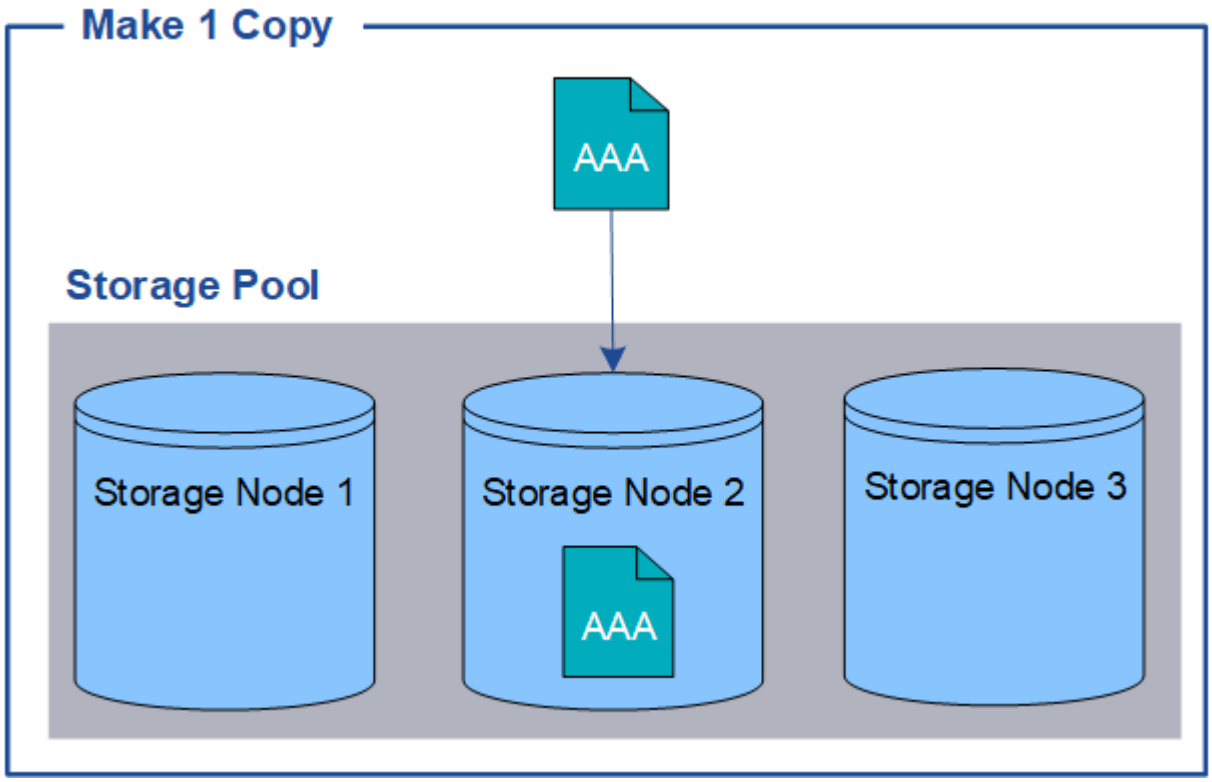
- "Was ist Erasure Coding"
- "Was ist ein Speicherpool?"
- "Aktivieren Sie den Site-Loss-Schutz durch Replikation und Erasure Coding"

Warum Sie keine Einzelkopiereplikation verwenden sollten

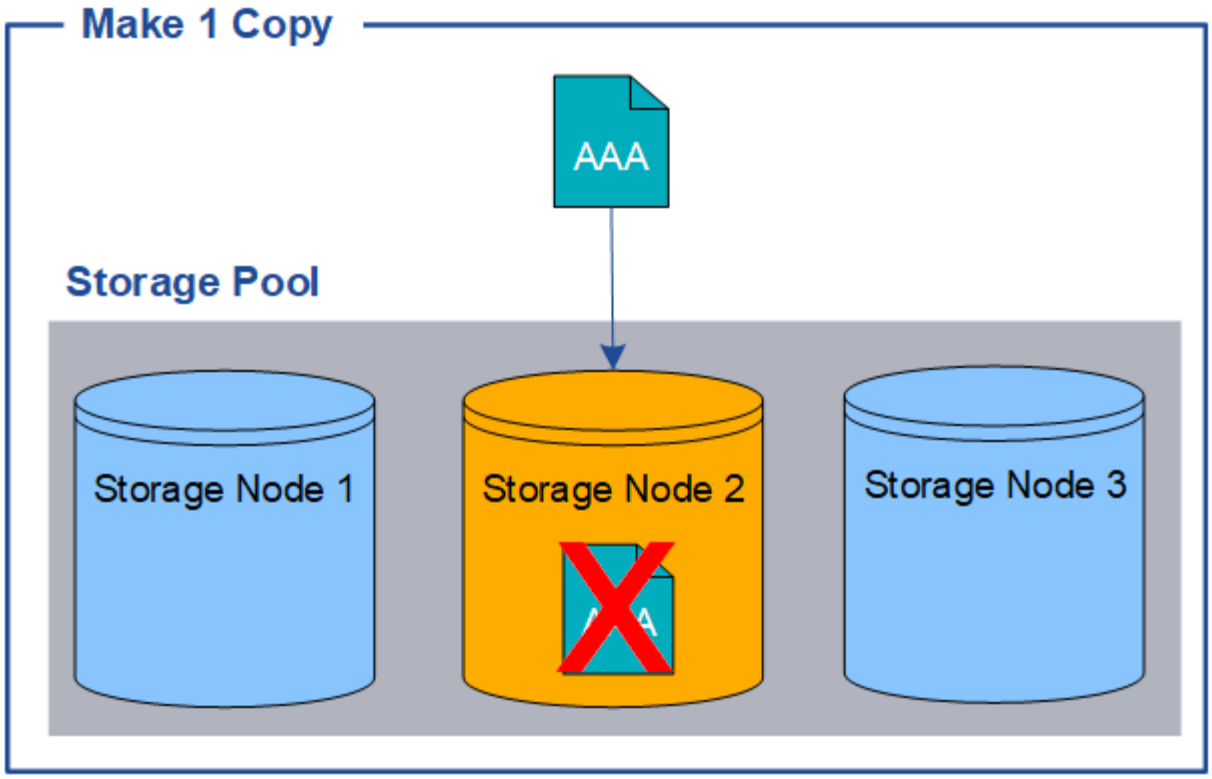
Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien erstellen, sollten Sie in den Platzierungsanweisungen immer mindestens zwei Kopien für einen beliebigen Zeitraum angeben.

Verwenden Sie keine ILM-Regel, die für einen bestimmten Zeitraum nur eine replizierte Kopie erstellt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

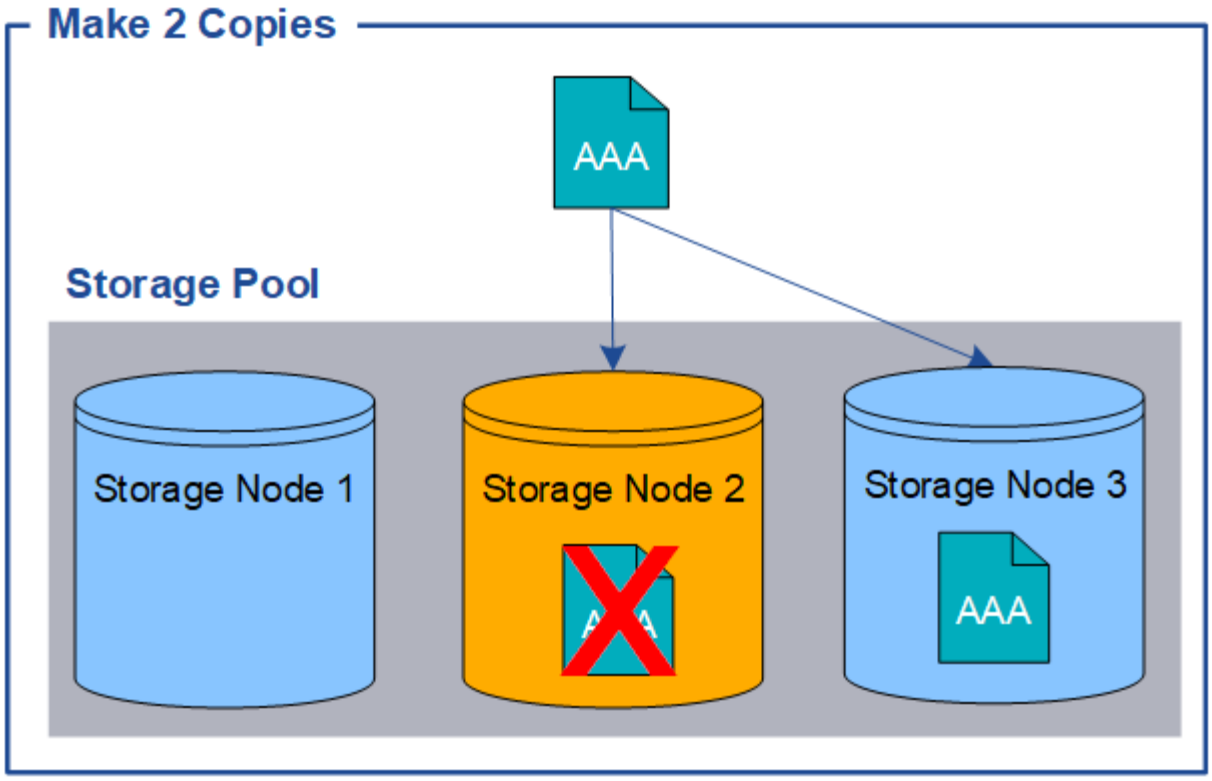
Im folgenden Beispiel gibt die ILM-Regel „1 Kopie erstellen“ an, dass eine replizierte Kopie eines Objekts in einem Speicherpool abgelegt wird, der drei Speicherknoten enthält. Wenn ein Objekt aufgenommen wird, das dieser Regel entspricht, platziert StorageGRID eine einzelne Kopie auf nur einem Speicherknoten.



Wenn eine ILM-Regel nur eine replizierte Kopie eines Objekts erstellt, ist der Zugriff auf das Objekt nicht mehr möglich, wenn der Speicherknoten nicht verfügbar ist. In diesem Beispiel verlieren Sie vorübergehend den Zugriff auf Objekt AAA, wenn Speicherknoten 2 offline ist, beispielsweise während eines Upgrades oder eines anderen Wartungsvorgangs. Sie verlieren Objekt AAA vollständig, wenn Speicherknoten 2 ausfällt.



Um den Verlust von Objektdaten zu vermeiden, sollten Sie immer mindestens zwei Kopien aller Objekte erstellen, die Sie durch Replikation schützen möchten. Wenn zwei oder mehr Kopien vorhanden sind, können Sie weiterhin auf das Objekt zugreifen, wenn ein Speicherknoten ausfällt oder offline geht.



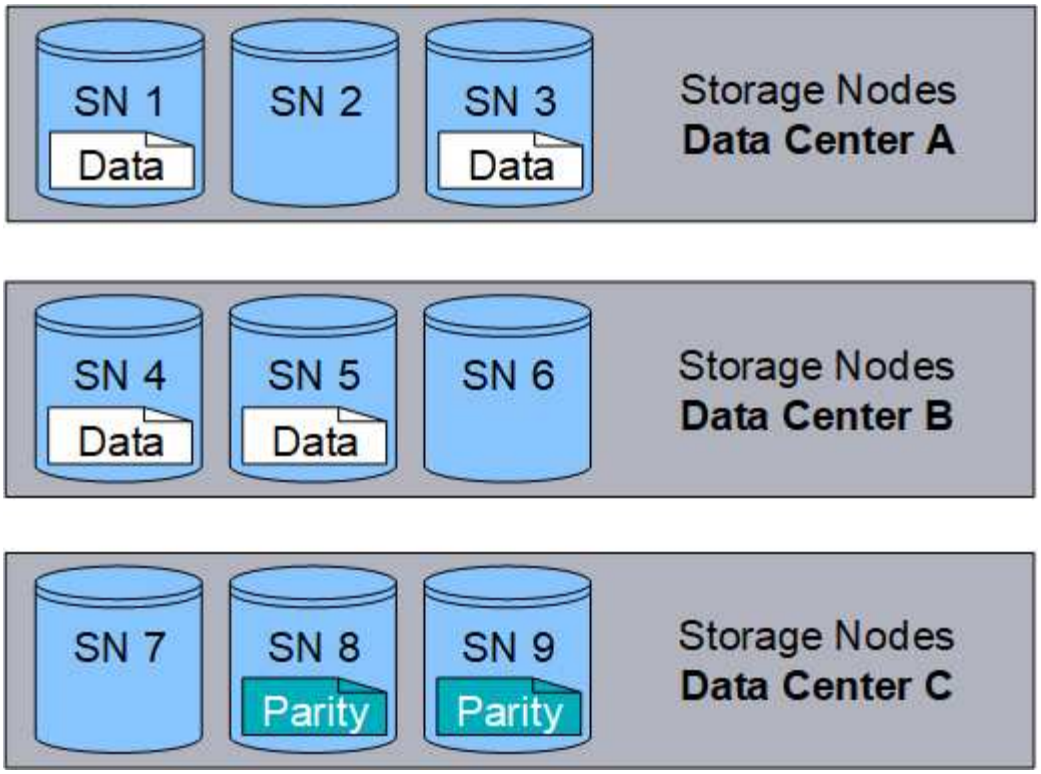
Was ist Erasure Coding?

Erasure Coding ist eine von zwei Methoden, die StorageGRID zum Speichern von Objektdaten verwendet (die andere Methode ist Replikation). Wenn Objekte einer ILM-Regel entsprechen, die Erasure Coding verwendet, werden diese Objekte in Datenfragmente aufgeteilt, zusätzliche Paritätsfragmente werden berechnet und jedes Fragment wird auf einem anderen Speicherknoten gespeichert.

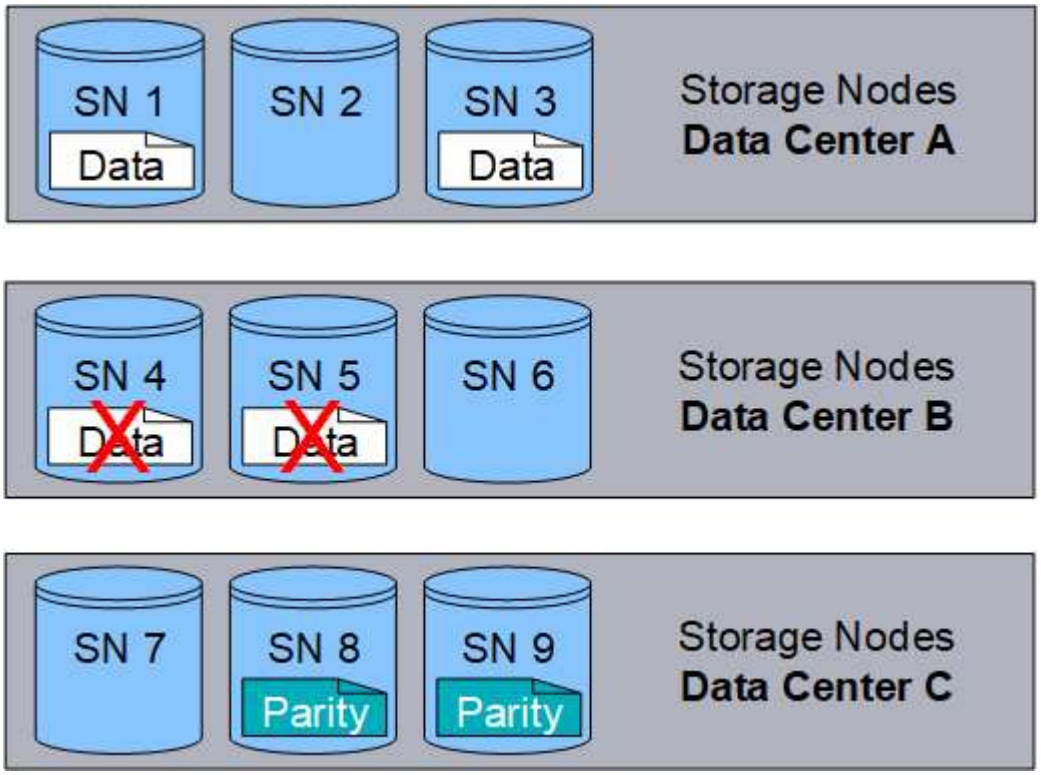
Beim Zugriff auf ein Objekt wird es anhand der gespeicherten Fragmente wieder zusammengesetzt. Wenn Daten oder ein Paritätsfragment beschädigt werden oder verloren gehen, kann der Erasure-Coding-Algorithmus dieses Fragment mithilfe einer Teilmenge der verbleibenden Daten und Paritätsfragmente wiederherstellen.

Während Sie ILM-Regeln erstellen, erstellt StorageGRID Erasure-Coding-Profile, die diese Regeln unterstützen. Sie können eine Liste der Erasure-Coding-Profile anzeigen,"Umbenennen eines Erasure-Coding-Profils" , oder"Deaktivieren Sie ein Erasure-Coding-Profil, wenn es derzeit in keinen ILM-Regeln verwendet wird." .

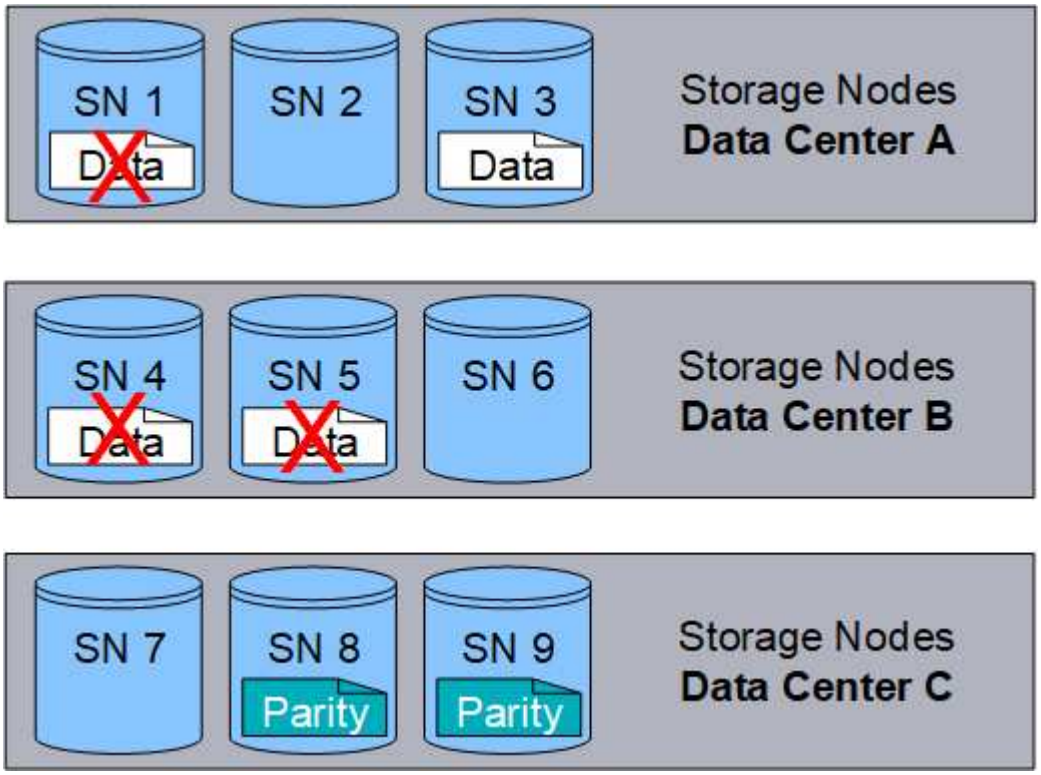
Das folgende Beispiel veranschaulicht die Verwendung eines Erasure-Coding-Algorithmus auf die Daten eines Objekts. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Erasure-Coding-Schema. Jedes Objekt wird in vier gleiche Datenfragmente aufgeteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente wird auf einem anderen Knoten an drei Rechenzentrumsstandorten gespeichert, um Datenschutz bei Knotenausfällen oder Standortverlust zu gewährleisten.



Das 4+2-Erasure-Coding-Schema kann auf verschiedene Arten konfiguriert werden. Sie können beispielsweise einen Single-Site-Speicherpool konfigurieren, der sechs Speicherknoten enthält. Für"Site-Loss-Schutz" können Sie einen Speicherpool mit drei Standorten und jeweils drei Speicherknoten an jedem Standort verwenden. Ein Objekt kann abgerufen werden, solange vier der sechs Fragmente (Daten oder Parität) verfügbar bleiben. Bis zu zwei Fragmente können verloren gehen, ohne dass die Objektdaten verloren gehen. Wenn eine ganze Site verloren geht, kann das Objekt immer noch geborgen oder repariert werden, solange alle anderen Fragmente zugänglich bleiben.



Wenn mehr als zwei Speicherknoten verloren gehen, kann das Objekt nicht wiederhergestellt werden.



Ähnliche Informationen

- "Was ist Replikation?"
- "Was ist ein Speicherpool?"
- "Was sind Erasure-Coding-Schemata?"
- "Umbenennen eines Erasure-Coding-Profils"
- "Deaktivieren eines Erasure-Coding-Profils"

Was sind Erasure-Coding-Schemata?

Erasure-Coding-Schemata steuern, wie viele Datenfragmente und wie viele Paritätsfragmente für jedes Objekt erstellt werden.

Wenn Sie eine ILM-Regel erstellen oder bearbeiten, wählen Sie ein verfügbares Erasure-Coding-Schema aus. StorageGRID erstellt automatisch Erasure-Coding-Schemata basierend auf der Anzahl der Speicherknoten und Sites, aus denen der Speicherpool besteht, den Sie verwenden möchten.

Datenschutz

Das StorageGRID -System verwendet den Reed-Solomon-Erasure-Coding-Algorithmus. Der Algorithmus zerlegt ein Objekt in `k` Datenfragmente und Berechnungen `m` Paritätsfragmente.

Der `k + m = n` Fragmente sind verteilt über `n` Speicherknoten bieten Datenschutz wie folgt:

- Um ein Objekt abzurufen oder zu reparieren, `k` Fragmente werden benötigt.
- Ein Objekt kann bis zu `m` verlorene oder beschädigte Fragmente. Je höher der Wert von `m` , desto höher ist die Fehlertoleranz.

Den besten Datenschutz bietet das Erasure-Coding-Schema mit der höchsten Knoten- oder Volume-Ausfalltoleranz innerhalb eines Speicherpools.

Speicheraufwand

Der Speicheraufwand eines Erasure-Coding-Schemas wird berechnet, indem die Anzahl der Paritätsfragmente geteilt wird(`m`) durch die Anzahl der Datenfragmente(`k`). Mithilfe des Speicher-Overheads können Sie berechnen, wie viel Speicherplatz jedes Erasure-Codierte Objekt benötigt:

```
disk space = object size + (object size * storage overhead)
```

Wenn Sie beispielsweise ein 10 MB großes Objekt mit dem 4+2-Schema speichern (das einen Speicher-Overhead von 50 % hat), verbraucht das Objekt 15 MB Grid-Speicher. Wenn Sie dasselbe 10 MB große Objekt mit dem 6+2-Schema speichern (das einen Speicher-Overhead von 33 % hat), verbraucht das Objekt ungefähr 13,3 MB.

Wählen Sie das Erasure-Coding-Schema mit dem niedrigsten Gesamtwert von `k+m` das Ihren Bedürfnissen entspricht. Erasure-Coding-Verfahren mit einer geringeren Anzahl von Fragmenten sind rechnerisch effizienter, weil:

- Pro Objekt werden weniger Fragmente erstellt und verteilt (oder abgerufen)
- Sie weisen eine bessere Leistung auf, da die Fragmentgröße größer ist
- Sie können erfordern, dass weniger Knoten in einem"Erweiterung, wenn mehr Speicherplatz benötigt wird"

Richtlinien für Speicherpools

Beachten Sie bei der Auswahl des Speicherpools für eine Regel zum Erstellen einer Löschcodierten Kopie die folgenden Richtlinien für Speicherpools:

- Der Speicherpool muss drei oder mehr Standorte oder genau einen Standort umfassen.

  > ⓘ Sie können Erasure Coding nicht verwenden, wenn der Speicherpool zwei Standorte umfasst.

  - Erasure-Coding-Schemata für Speicherpools mit drei oder mehr Standorten
  - Erasure-Coding-Schemata für Speicherpools an einem Standort
- Verwenden Sie keinen Speicherpool, der die Site „Alle Sites“ enthält.
- Der Speicherpool sollte mindestens *`k+m`* `+1` Speicherknoten, die Objektdaten speichern können.

  > ⓘ Speicherknoten können während der Installation so konfiguriert werden, dass sie nur Objektmetadaten und keine Objektdaten enthalten. Weitere Informationen finden Sie unter "Arten von Speicherknoten" .

  Die Mindestanzahl der erforderlichen Speicherknoten beträgt `k+m` . Wenn jedoch mindestens ein zusätzlicher Speicherknoten vorhanden ist, können Aufnahmefehler oder ILM-Rückstände vermieden werden, wenn ein erforderlicher Speicherknoten vorübergehend nicht verfügbar ist.

Erasure-Coding-Schemata für Speicherpools mit drei oder mehr Standorten

Die folgende Tabelle beschreibt die Erasure-Coding-Schemata, die derzeit von StorageGRID für Speicherpools

mit drei oder mehr Standorten unterstützt werden. Alle diese Systeme bieten Schutz vor Standortverlust. Eine Site kann verloren gehen, und das Objekt ist weiterhin zugänglich.

Für Erasure-Coding-Schemata, die Site-Loss-Schutz bieten, übersteigt die empfohlene Anzahl von Storage Nodes im Speicherpool `k+m +1` da für jeden Standort mindestens drei Speicherknoten erforderlich sind.

Erasure-Coding-Schema (*k+m*)	Mindestanzahl bereitgestellter Sites	Empfohlene Anzahl von Speicherknoten an jedem Standort	Empfohlene Gesamtzahl an Speicherknoten	Schutz vor Site-Verlust?	Speicheraufwand
4+2	3	3	9	Ja	50 %
6+2	4	3	12	Ja	33 %
8+2	5	3	15	Ja	25 %
6+3	3	4	12	Ja	50 %
9+3	4	4	16	Ja	33 %
2+1	3	3	9	Ja	50 %
4+1	5	3	15	Ja	25 %
6+1	7	3	21	Ja	17 %
7+5	3	5	15	Ja	71 %

StorageGRID erfordert mindestens drei Speicherknoten pro Site. Um das 7+5-Schema zu verwenden, benötigt jeder Standort mindestens vier Speicherknoten. Es wird empfohlen, fünf Speicherknoten pro Site zu verwenden.

Wägen Sie bei der Auswahl eines Löschcodierungsschemas, das Site-Schutz bietet, die relative Bedeutung der folgenden Faktoren ab:

- **Anzahl der Fragmente**: Leistung und Erweiterungsflexibilität sind im Allgemeinen besser, wenn die Gesamtzahl der Fragmente geringer ist.
- **Fehlertoleranz**: Die Fehlertoleranz wird durch mehr Paritätssegmente erhöht (d. h. wenn `m` hat einen höheren Wert.)
- **Netzwerkverkehr**: Bei der Wiederherstellung nach Fehlern wird ein Schema mit mehr Fragmenten verwendet (d. h. eine höhere Gesamtzahl für `k+m`) erzeugt mehr Netzwerkverkehr.
- **Speicher-Overhead**: Schemata mit höherem Overhead erfordern mehr Speicherplatz pro Objekt.

Wenn Sie sich beispielsweise zwischen einem 4+2-Schema und einem 6+3-Schema entscheiden (die beide einen Speicher-Overhead von 50 % haben), wählen Sie das 6+3-Schema, wenn zusätzliche Fehlertoleranz erforderlich ist. Wählen Sie das 4+2-Schema, wenn die Netzwerkressourcen eingeschränkt sind. Wenn alle anderen Faktoren gleich sind, wählen Sie 4+2, da dies eine geringere Gesamtzahl an Fragmenten ergibt.

Wenn Sie sich nicht sicher sind, welches Schema Sie verwenden sollen, wählen Sie 4+2 oder 6+3 oder wenden Sie sich an den technischen Support.

Erasure-Coding-Schemata für Speicherpools an einem Standort

Ein Speicherpool für einen Standort unterstützt alle für drei oder mehr Standorte definierten Erasure-Coding-Schemata, vorausgesetzt, der Standort verfügt über genügend Speicherknoten.

Die Mindestanzahl der erforderlichen Speicherknoten beträgt `k+m` , sondern ein Speicherpool mit `k+m +1` Speicherknoten werden empfohlen. Beispielsweise erfordert das 2+1-Erasure-Coding-Schema einen Speicherpool mit mindestens drei Speicherknoten, empfohlen werden jedoch vier Speicherknoten.

Erasure-Coding-Schema (*k+m*)	Mindestanzahl an Speicherknoten	Empfohlene Anzahl von Speicherknoten	Speicheraufwand
4+2	6	7	50 %
6+2	8	9	33 %
8+2	10	11	25 %
6+3	9	10	50 %
9+3	12	13	33 %
2+1	3	4	50 %
4+1	5	6	25 %
6+1	7	8	17 %
7+5	12	13	71 %

Vorteile, Nachteile und Voraussetzungen für Erasure Coding

Bevor Sie sich entscheiden, ob Sie Replikation oder Erasure Coding zum Schutz von Objektdaten vor Verlust verwenden, sollten Sie die Vor- und Nachteile sowie die Anforderungen von Erasure Coding verstehen.

Vorteile der Erasure Coding

Im Vergleich zur Replikation bietet Erasure Coding eine verbesserte Zuverlässigkeit, Verfügbarkeit und Speichereffizienz.

- **Zuverlässigkeit**: Die Zuverlässigkeit wird anhand der Fehlertoleranz gemessen, d. h. anhand der Anzahl gleichzeitiger Fehler, die ohne Datenverlust toleriert werden können. Bei der Replikation werden mehrere identische Kopien auf verschiedenen Knoten und an verschiedenen Standorten gespeichert. Beim Erasure Coding wird ein Objekt in Daten- und Paritätsfragmente kodiert und auf viele Knoten und Standorte verteilt. Diese Verteilung bietet sowohl Site- als auch Knotenausfallschutz. Im Vergleich zur Replikation bietet

Erasure Coding eine verbesserte Zuverlässigkeit bei vergleichbaren Speicherkosten.

- **Verfügbarkeit**: Verfügbarkeit kann als die Fähigkeit definiert werden, Objekte abzurufen, wenn Speicherknoten ausfallen oder nicht mehr zugänglich sind. Im Vergleich zur Replikation bietet Erasure Coding eine höhere Verfügbarkeit bei vergleichbaren Speicherkosten.
- **Speichereffizienz**: Bei vergleichbarer Verfügbarkeit und Zuverlässigkeit verbrauchen durch Erasure Coding geschützte Objekte weniger Speicherplatz als dieselben Objekte, die durch Replikation geschützt wären. Beispielsweise verbraucht ein 10 MB großes Objekt, das an zwei Standorten repliziert wird, 20 MB Speicherplatz (zwei Kopien), während ein Objekt, das an drei Standorten mit einem 6+3-Erasure-Coding-Schema löschcodiert wird, nur 15 MB Speicherplatz verbraucht.

> Der Speicherplatz für Erasure-Codierte Objekte wird aus der Objektgröße plus Speicher-Overhead berechnet. Der Prozentsatz des Speicher-Overheads ist die Anzahl der Paritätsfragmente geteilt durch die Anzahl der Datenfragmente.

Nachteile der Erasure Coding

Im Vergleich zur Replikation weist Erasure Coding folgende Nachteile auf:

- Je nach Erasure-Coding-Schema wird eine erhöhte Anzahl von Speicherknoten und -standorten empfohlen. Wenn Sie dagegen Objektdaten replizieren, benötigen Sie nur einen Speicherknoten für jede Kopie. Sehen"Erasure-Coding-Schemata für Speicherpools mit drei oder mehr Standorten" Und"Erasure-Coding-Schemata für Speicherpools an einem Standort" .
- Erhöhte Kosten und Komplexität von Speichererweiterungen. Um eine Bereitstellung zu erweitern, die Replikation verwendet, fügen Sie an jedem Standort, an dem Objektkopien erstellt werden, Speicherkapazität hinzu. Um eine Bereitstellung zu erweitern, die Erasure Coding verwendet, müssen Sie sowohl das verwendete Erasure-Coding-Schema als auch den Füllstand vorhandener Speicherknoten berücksichtigen. Wenn Sie beispielsweise warten, bis vorhandene Knoten zu 100 % belegt sind, müssen Sie mindestens `k+m` Speicherknoten. Wenn Sie jedoch erweitern, wenn die vorhandenen Knoten zu 70 % belegt sind, können Sie zwei Knoten pro Site hinzufügen und trotzdem die nutzbare Speicherkapazität maximieren. Weitere Informationen finden Sie unter "Speicherkapazität für Erasure-Coded-Objekte hinzufügen" .
- Bei der Verwendung von Erasure Coding an geografisch verteilten Standorten kommt es zu längeren Abruflatenzen. Das Abrufen der Objektfragmente für ein Objekt, das mit einem Erasure Code versehen und über Remote-Standorte verteilt ist, über WAN-Verbindungen dauert länger als das Abrufen eines Objekts, das repliziert und lokal verfügbar ist (derselbe Standort, mit dem der Client eine Verbindung herstellt).
- Wenn Sie Erasure Coding an geografisch verteilten Standorten verwenden, kommt es zu einer höheren Auslastung des WAN-Netzwerkverkehrs für Abrufe und Reparaturen, insbesondere bei häufig abgerufenen Objekten oder für Objektreparaturen über WAN-Netzwerkverbindungen.
- Wenn Sie Erasure Coding standortübergreifend verwenden, sinkt der maximale Objektdurchsatz stark, da die Netzwerklatenz zwischen den Standorten zunimmt. Dieser Rückgang ist auf den entsprechenden Rückgang des TCP-Netzwerkdurchsatzes zurückzuführen, der sich darauf auswirkt, wie schnell das StorageGRID -System Objektfragmente speichern und abrufen kann.
- Höhere Nutzung von Rechenressourcen.

Wann wird Erasure Coding verwendet?

Erasure Coding eignet sich am besten für folgende Anforderungen:

- Objekte mit einer Größe von mehr als 1 MB.

Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

- Langzeit- oder Cold-Storage für selten abgerufene Inhalte.
- Hohe Datenverfügbarkeit und Zuverlässigkeit.
- Schutz vor vollständigen Site- und Knotenausfällen.
- Speichereffizienz.
- Einzelstandortbereitstellungen, die einen effizienten Datenschutz mit nur einer einzigen löschcodierten Kopie anstelle mehrerer replizierter Kopien erfordern.
- Bereitstellungen an mehreren Standorten, bei denen die Latenz zwischen den Standorten weniger als 100 ms beträgt.

So wird die Objektaufbewahrung bestimmt

StorageGRID bietet sowohl Grid-Administratoren als auch einzelnen Mandantenbenutzern Optionen zum Angeben der Speicherdauer von Objekten. Im Allgemeinen haben alle Aufbewahrungsanweisungen eines Mandantenbenutzers Vorrang vor den Aufbewahrungsanweisungen des Grid-Administrators.

So steuern Mandantenbenutzer die Objektaufbewahrung

Mandantenbenutzer können mit diesen Methoden steuern, wie lange ihre Objekte in StorageGRID gespeichert werden:

- Wenn die globale S3-Objektsperreinstellung für das Raster aktiviert ist, können S3-Mandantenbenutzer Buckets mit aktivierter S3-Objektsperre erstellen und dann für jeden Bucket eine **Standardaufbewahrungsdauer** auswählen.
- Wenn die globale Einstellung „S3 Object Lock“ für das Raster aktiviert ist, können S3-Mandantenbenutzer Buckets mit aktivierter S3 Object Lock erstellen und dann die S3 REST-API verwenden, um Einstellungen für das Aufbewahrungsdatum und die gesetzliche Aufbewahrung für jede diesem Bucket hinzugefügte Objektversion festzulegen.
  - Eine Objektversion, die einer rechtlichen Sperre unterliegt, kann mit keiner Methode gelöscht werden.
  - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version mit keiner Methode gelöscht werden.
  - Objekte in Buckets mit aktivierter S3-Objektsperre werden von ILM „für immer“ aufbewahrt. Nach Erreichen des Aufbewahrungsdatums kann eine Objektversion jedoch durch eine Clientanforderung oder den Ablauf des Bucket-Lebenszyklus gelöscht werden. Sehen "Verwalten von Objekten mit S3 Object Lock" .
- S3-Tenant-Benutzer können ihren Buckets eine Lebenszykluskonfiguration hinzufügen, die eine Ablaufaktion angibt. Wenn ein Bucket-Lebenszyklus vorhanden ist, speichert StorageGRID ein Objekt, bis das in der Ablaufaktion angegebene Datum oder die Anzahl der Tage erreicht ist, es sei denn, der Client löscht das Objekt zuerst. Sehen "Erstellen einer S3-Lebenszykluskonfiguration" .
- Ein S3-Client kann eine Anforderung zum Löschen eines Objekts stellen. StorageGRID priorisiert Client-Löschanforderungen immer gegenüber dem S3-Bucket-Lebenszyklus oder ILM, wenn entschieden wird, ob ein Objekt gelöscht oder behalten werden soll.

So steuern Grid-Administratoren die Objektaufbewahrung

Grid-Administratoren können die Objektaufbewahrung mithilfe dieser Methoden steuern:

- Legen Sie für jeden Mandanten eine maximale Aufbewahrungsdauer für S3 Object Lock fest. Anschließend können Mandantenbenutzer für jeden ihrer Buckets eine Standardaufbewahrungsdauer festlegen. Die maximale Aufbewahrungsdauer wird auch für alle neu aufgenommenen Objekte für diesen Bucket erzwungen (Aufbewahrungsdatum des Objekts).
- Erstellen Sie ILM-Platzierungsanweisungen, um zu steuern, wie lange Objekte gespeichert werden. Wenn Objekte mit einer ILM-Regel übereinstimmen, speichert StorageGRID diese Objekte, bis der letzte Zeitraum in der ILM-Regel abgelaufen ist. Objekte bleiben unbegrenzt erhalten, wenn für die Platzierungsanweisungen „für immer“ angegeben ist.
- Unabhängig davon, wer kontrolliert, wie lange Objekte aufbewahrt werden, steuern die ILM-Einstellungen, welche Arten von Objektkopien (repliziert oder löschcodiert) gespeichert werden und wo sich die Kopien befinden (Speicherknoten oder Cloud-Speicherpools).

So interagieren S3-Bucket-Lebenszyklus und ILM

Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Aktionen zum Ablauf des Lebenszyklus die ILM-Richtlinie für Objekte, die dem Lebenszyklusfilter entsprechen. Dies kann dazu führen, dass ein Objekt auch dann noch auf dem Raster verbleibt, wenn keine ILM-Anweisungen zum Platzieren des Objekts mehr vorliegen.

Beispiele für die Objektaufbewahrung

Um die Interaktionen zwischen S3 Object Lock, Bucket-Lebenszykluseinstellungen, Client-Löschanforderungen und ILM besser zu verstehen, betrachten Sie die folgenden Beispiele.

Beispiel 1: Der S3-Bucket-Lebenszyklus speichert Objekte länger als ILM

ILM

Bewahren Sie zwei Kopien für 1 Jahr (365 Tage) auf

Bucket-Lebenszyklus

Objekte laufen in 2 Jahren (730 Tagen) ab

Ergebnis

StorageGRID speichert das Objekt 730 Tage lang. StorageGRID verwendet die Bucket-Lebenszykluseinstellungen, um zu bestimmen, ob ein Objekt gelöscht oder beibehalten werden soll.

> Wenn der Bucket-Lebenszyklus vorgibt, dass Objekte länger aufbewahrt werden sollen als von ILM angegeben, verwendet StorageGRID weiterhin die ILM-Platzierungsanweisungen, um die Anzahl und den Typ der zu speichernden Kopien zu bestimmen. In diesem Beispiel werden von Tag 366 bis 730 weiterhin zwei Kopien des Objekts in StorageGRID gespeichert.

Beispiel 2: S3-Bucket-Lebenszyklus lässt Objekte vor ILM ablaufen

ILM

Bewahren Sie zwei Kopien 2 Jahre lang (730 Tage) auf.

Bucket-Lebenszyklus

Objekte laufen in 1 Jahr (365 Tagen) ab

Ergebnis

StorageGRID löscht beide Kopien des Objekts nach Tag 365.

Beispiel 3: Client-Löschen überschreibt Bucket-Lebenszyklus und ILM

ILM

Speichern Sie zwei Kopien „für immer“ auf Speicherknoten

Bucket-Lebenszyklus

Objekte laufen in 2 Jahren (730 Tagen) ab

Client-Löschanforderung

Ausgestellt am Tag 400

Ergebnis

StorageGRID löscht beide Kopien des Objekts am Tag 400 als Antwort auf die Löschanforderung des Clients.

Beispiel 4: S3 Object Lock überschreibt Client-Löschanforderung

S3-Objektsperre

Das Aufbewahrungsdatum für eine Objektversion ist der 31.03.2026. Eine rechtliche Sperre besteht nicht.

Konforme ILM-Regel

Speichern Sie zwei Kopien „für immer“ auf Speicherknoten

Client-Löschanforderung

Ausgestellt am 31.03.2024

Ergebnis

StorageGRID löscht die Objektversion nicht, da das Aufbewahrungsdatum noch 2 Jahre entfernt ist.

So werden Objekte gelöscht

StorageGRID kann Objekte entweder als direkte Reaktion auf eine Clientanforderung oder automatisch aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus oder der Anforderungen der ILM-Richtlinie löschen. Wenn Sie die verschiedenen Möglichkeiten zum Löschen von Objekten und die Art und Weise verstehen, wie StorageGRID Löschanforderungen verarbeitet, können Sie Objekte effizienter verwalten.

StorageGRID kann zum Löschen von Objekten eine von zwei Methoden verwenden:

- Synchrones Löschen: Wenn StorageGRID eine Löschanforderung des Clients erhält, werden alle Objektkopien sofort entfernt. Nach dem Entfernen der Kopien wird dem Kunden mitgeteilt, dass die Löschung erfolgreich war.
- Objekte werden zum Löschen in die Warteschlange gestellt: Wenn StorageGRID eine Löschanforderung erhält, wird das Objekt zum Löschen in die Warteschlange gestellt und der Client wird sofort darüber informiert, dass das Löschen erfolgreich war. Objektkopien werden später durch die ILM-Hintergrundverarbeitung entfernt.

Beim Löschen von Objekten verwendet StorageGRID die Methode, die die Löschleistung optimiert, potenzielle

Löschrückstände minimiert und Speicherplatz am schnellsten freigibt.

Die Tabelle fasst zusammen, wann StorageGRID welche Methode verwendet.

Methode zum Durchführen des Löschvorgangs	Bei Verwendung
Objekte werden zum Löschen in die Warteschlange gestellt	Wenn **eine** der folgenden Bedingungen zutrifft: • Die automatische Objektlöschung wurde durch eines der folgenden Ereignisse ausgelöst: ◦ Das Ablaufdatum oder die Anzahl der Tage in der Lebenszykluskonfiguration für einen S3-Bucket ist erreicht. ◦ Der letzte in einer ILM-Regel angegebene Zeitraum ist abgelaufen. **Hinweis:** Objekte in einem Bucket mit aktivierter S3-Objektsperre können nicht gelöscht werden, wenn sie einer rechtlichen Sperre unterliegen oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erreicht wurde. • Ein S3-Client fordert die Löschung an und eine oder mehrere der folgenden Bedingungen sind erfüllt: ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, weil beispielsweise ein Objektstandort vorübergehend nicht verfügbar ist. ◦ Hintergrundlöschwarteschlangen sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	Wenn ein S3-Client eine Löschanforderung stellt und **alle** der folgenden Bedingungen erfüllt sind: • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Hintergrundlöschwarteschlangen enthalten zu verarbeitende Objekte.

Wenn S3-Clients Löschanforderungen stellen, beginnt StorageGRID damit, Objekte zur Löschwarteschlange hinzuzufügen. Anschließend wird auf die synchrone Löschung umgeschaltet. Indem sichergestellt wird, dass die Löschwarteschlange im Hintergrund über zu verarbeitende Objekte verfügt, kann StorageGRID Löschvorgänge effizienter verarbeiten, insbesondere bei Clients mit geringer Parallelität. Gleichzeitig wird ein Löschrückstau bei Clients vermieden.

Zum Löschen von Objekten erforderliche Zeit

Die Art und Weise, wie StorageGRID Objekte löscht, kann sich auf die scheinbare Leistung des Systems auswirken:

- Wenn StorageGRID eine synchrone Löschung durchführt, kann es bis zu 30 Sekunden dauern, bis StorageGRID ein Ergebnis an den Client zurückgibt. Dies bedeutet, dass das Löschen scheinbar langsamer erfolgt, obwohl Kopien tatsächlich schneller entfernt werden, als dies der Fall ist, wenn StorageGRID Objekte zum Löschen in die Warteschlange stellt.
- Wenn Sie die Löschleistung während einer Massenlöschung genau überwachen, stellen Sie möglicherweise fest, dass die Löschrate nach dem Löschen einer bestimmten Anzahl von Objekten langsam zu sein scheint. Diese Änderung tritt ein, wenn StorageGRID von der Warteschlangeneinreihung von Objekten zum Löschen zur synchronen Löschung übergeht. Die scheinbare Verringerung der

Löschrate bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil, es deutet darauf hin, dass im Durchschnitt nun schneller Platz freigegeben wird.

Wenn Sie eine große Anzahl von Objekten löschen und Ihre Priorität darin besteht, schnell Speicherplatz freizugeben, sollten Sie zum Löschen von Objekten eine Clientanforderung verwenden, anstatt sie mit ILM oder anderen Methoden zu löschen. Im Allgemeinen wird Speicherplatz schneller freigegeben, wenn die Löschung durch Clients erfolgt, da StorageGRID synchrones Löschen verwenden kann.

Die zum Freigeben von Speicherplatz nach dem Löschen eines Objekts erforderliche Zeit hängt von mehreren Faktoren ab:

- Ob Objektkopien synchron entfernt oder zur späteren Entfernung in die Warteschlange gestellt werden (für Client-Löschanforderungen).
- Andere Faktoren wie die Anzahl der Objekte im Grid oder die Verfügbarkeit von Grid-Ressourcen, wenn Objektkopien zum Entfernen in die Warteschlange gestellt werden (sowohl für Client-Löschvorgänge als auch für andere Methoden).

So werden versionierte S3-Objekte gelöscht

Wenn die Versionierung für einen S3-Bucket aktiviert ist, folgt StorageGRID beim Antworten auf Löschanforderungen dem Verhalten von Amazon S3, unabhängig davon, ob diese Anforderungen von einem S3-Client, dem Ablauf eines S3-Bucket-Lebenszyklus oder den Anforderungen der ILM-Richtlinie stammen.

Wenn Objekte versioniert sind, löschen Objektlöschanforderungen nicht die aktuelle Version des Objekts und geben keinen Speicherplatz frei. Stattdessen erstellt eine Objektlöschanforderung eine Null-Byte-Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts „nicht aktuell“ wird. Eine Objektlöschmarkierung wird zu einer abgelaufenen Objektlöschmarkierung, wenn es sich um die aktuelle Version handelt und keine nicht aktuellen Versionen vorhanden sind.

Obwohl das Objekt nicht entfernt wurde, verhält sich StorageGRID so, als ob die aktuelle Version des Objekts nicht mehr verfügbar wäre. Anfragen an dieses Objekt geben 404 NotFound zurück. Da jedoch nicht aktuelle Objektdaten nicht entfernt wurden, können Anforderungen, die eine nicht aktuelle Version des Objekts angeben, erfolgreich sein.

Um beim Löschen versionierter Objekte Speicherplatz freizugeben oder Löschmarkierungen zu entfernen, verwenden Sie eine der folgenden Möglichkeiten:

- **S3-Client-Anforderung**: Geben Sie die Objektversions-ID in der S3-Anforderung „DELETE Object“ an(`DELETE /object?versionId=ID`). Beachten Sie, dass diese Anforderung nur Objektkopien für die angegebene Version entfernt (die anderen Versionen belegen weiterhin Speicherplatz).
- **Bucket-Lebenszyklus**: Verwenden Sie die `NoncurrentVersionExpiration` Aktion in der Bucket-Lebenszykluskonfiguration. Wenn die angegebene Anzahl von NoncurrentDays erreicht ist, entfernt StorageGRID dauerhaft alle Kopien nicht aktueller Objektversionen. Diese Objektversionen können nicht wiederhergestellt werden.

  Der `NewerNoncurrentVersions` Die Aktion in der Bucket-Lebenszykluskonfiguration gibt die Anzahl der nicht aktuellen Versionen an, die in einem versionierten S3-Bucket beibehalten werden. Wenn mehr nicht aktuelle Versionen vorhanden sind als `NewerNoncurrentVersions` gibt an, dass StorageGRID die älteren Versionen entfernt, wenn der Wert „NoncurrentDays“ abgelaufen ist. Der `NewerNoncurrentVersions` Schwellenwert überschreibt die von ILM bereitgestellten Lebenszyklusregeln, d. h. ein nicht aktuelles Objekt mit einer Version innerhalb des `NewerNoncurrentVersions` Der Schwellenwert bleibt erhalten, wenn ILM seine Löschung anfordert.

  Um abgelaufene Objektlöschmarkierungen zu entfernen, verwenden Sie die `Expiration` Aktion mit

einem der folgenden Tags: `ExpiredObjectDeleteMarker` , `Days` , oder `Date` .

- **ILM**:"Klonen einer aktiven Richtlinie" und fügen Sie der neuen Richtlinie zwei ILM-Regeln hinzu:
  - Erste Regel: Verwenden Sie „Nicht aktuelle Zeit“ als Referenzzeit, um die nicht aktuellen Versionen des Objekts abzugleichen. In"Schritt 1 (Details eingeben) des Assistenten „ILM-Regel erstellen“" , wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“
  - Zweite Regel: Verwenden Sie die **Aufnahmezeit**, um sie an die aktuelle Version anzupassen. Die Regel „Nicht aktuelle Zeit“ muss in der Richtlinie über der Regel **Aufnahmezeit** erscheinen.

    Um abgelaufene Objektlöschmarkierungen zu entfernen, verwenden Sie eine **Aufnahmezeit**-Regel, um die aktuellen Löschmarkierungen abzugleichen. Löschmarkierungen werden nur entfernt, wenn ein **Zeitraum** von **Tagen** verstrichen ist und die aktuelle Löschmarkierung abgelaufen ist (es gibt keine nicht aktuellen Versionen).
- **Objekte im Bucket löschen**: Verwenden Sie den Mandantenmanager, um"alle Objektversionen löschen" , einschließlich Löschmarkierungen, aus einem Bucket.

Wenn ein versioniertes Objekt gelöscht wird, erstellt StorageGRID eine Null-Byte-Löschmarkierung als aktuelle Version des Objekts. Alle Objekte und Löschmarkierungen müssen entfernt werden, bevor ein versionierter Bucket gelöscht werden kann.

- In StorageGRID 11.7 oder früher erstellte Löschmarkierungen können nur über S3-Clientanforderungen entfernt werden. Sie werden nicht durch ILM, Bucket-Lebenszyklusregeln oder Löschvorgänge für Objekte in Buckets entfernt.
- Löschmarkierungen aus einem Bucket, der in StorageGRID 11.8 oder höher erstellt wurde, können durch ILM, Bucket-Lebenszyklusregeln, Löschvorgänge für Objekte in Buckets oder eine explizite S3-Client-Löschung entfernt werden.

Ähnliche Informationen

- "Verwenden Sie die S3 REST-API"
- "Beispiel 4: ILM-Regeln und -Richtlinien für versionierte S3-Objekte"

Erstellen und Zuweisen von Speicherklassen

Speicherklassen identifizieren den von einem Speicherknoten verwendeten Speichertyp. Sie können Speicherklassen erstellen, wenn Sie möchten, dass ILM-Regeln bestimmte Objekte auf bestimmten Speicherknoten platzieren.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Wenn Sie StorageGRID zum ersten Mal installieren, wird jedem Speicherknoten in Ihrem System automatisch die Speicherklasse **Standard** zugewiesen. Bei Bedarf können Sie optional benutzerdefinierte Speicherklassen definieren und diese verschiedenen Speicherknoten zuweisen.

Durch die Verwendung benutzerdefinierter Speicherklassen können Sie ILM-Speicherpools erstellen, die nur einen bestimmten Typ von Speicherknoten enthalten. Beispielsweise möchten Sie möglicherweise, dass bestimmte Objekte auf Ihren schnellsten Speicherknoten gespeichert werden, wie etwa StorageGRID -All

-Flash-Speichergeräten.

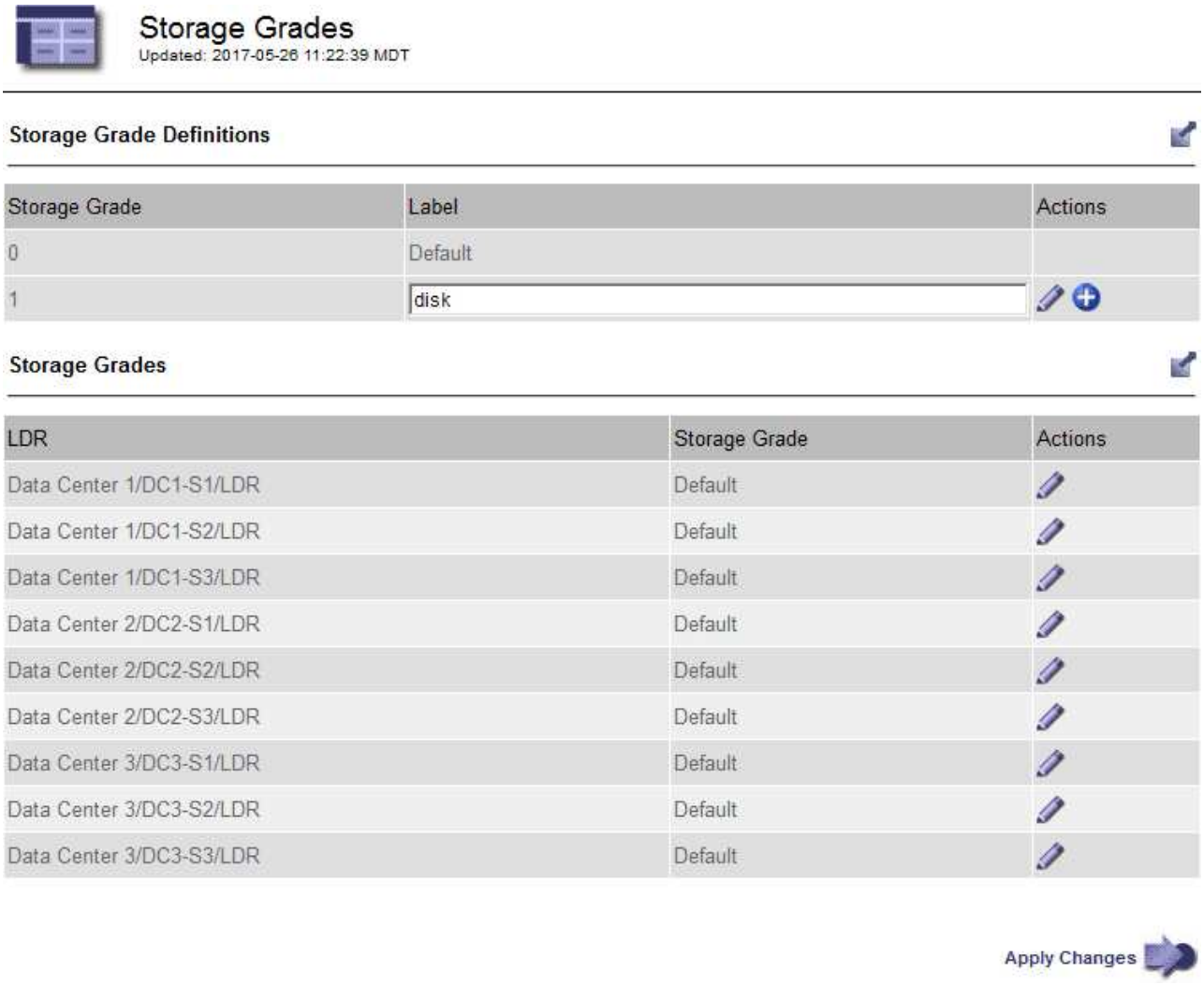
> Speicherknoten können während der Installation so konfiguriert werden, dass sie nur Objektmetadaten und keine Objektdaten enthalten. Nur Metadaten-Speicherknoten kann keine Speicherklasse zugewiesen werden. Weitere Informationen finden Sie unter "Arten von Speicherknoten" .

Wenn die Speicherqualität kein Problem darstellt (z. B. wenn alle Speicherknoten identisch sind), können Sie dieses Verfahren überspringen und die Option **beinhaltet alle Speicherqualitäten** für die Speicherqualität verwenden, wenn Sie"Speicherpools erstellen" . Durch diese Auswahl wird sichergestellt, dass der Speicherpool jeden Speicherknoten am Standort umfasst, unabhängig von seiner Speicherklasse.

> Erstellen Sie nicht mehr Speicherklassen als nötig. Erstellen Sie beispielsweise nicht für jeden Speicherknoten eine eigene Speicherklasse. Weisen Sie stattdessen jeder Speicherklasse zwei oder mehr Knoten zu. Nur einem Knoten zugewiesene Speicherklassen können zu ILM-Rückständen führen, wenn dieser Knoten nicht mehr verfügbar ist.

Schritte

1. Wählen Sie **ILM** > **Speichergrade**.
2. Definieren Sie benutzerdefinierte Speicherklassen:
   a. Wählen Sie für jede benutzerdefinierte Speicherklasse, die Sie hinzufügen möchten, *Einfügen* , um eine Zeile hinzuzufügen.
   b. Geben Sie eine beschreibende Bezeichnung ein.



c. Wählen Sie **Änderungen übernehmen**.

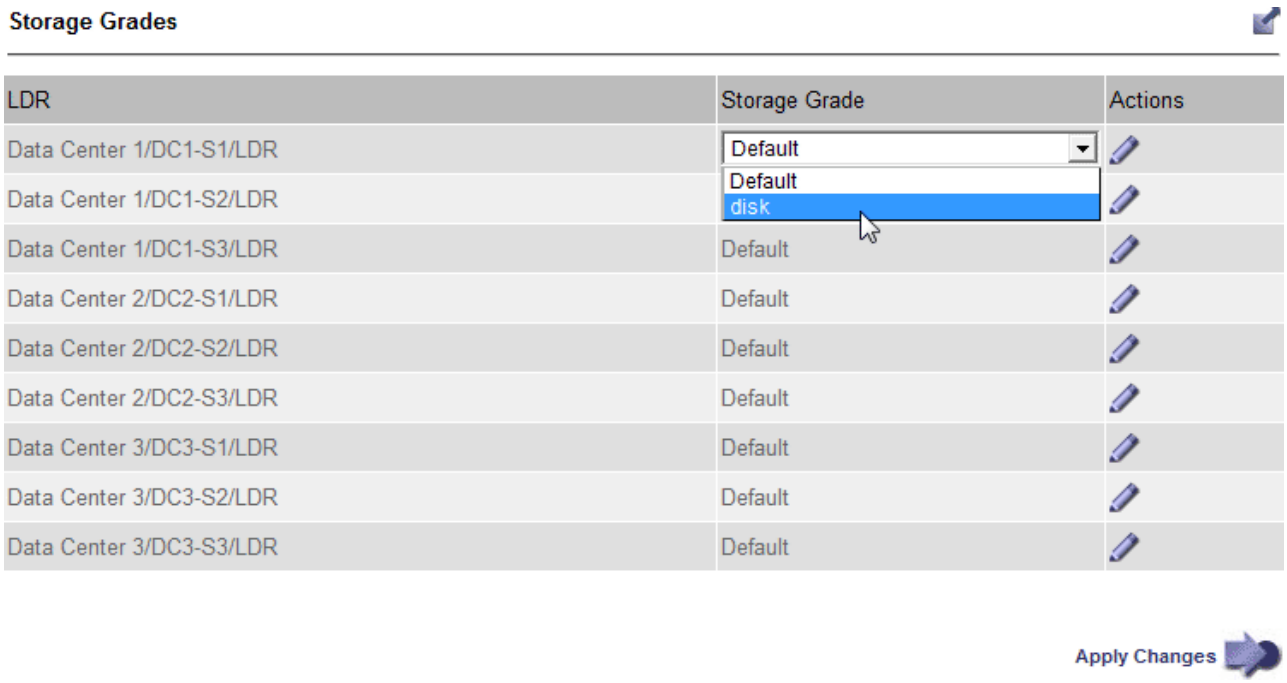
d. Wenn Sie ein gespeichertes Etikett ändern möchten, wählen Sie optional **Bearbeiten*** **und wählen Sie *Änderungen übernehmen**.

Sie können keine Speichergrade löschen.

3. Weisen Sie Speicherknoten neue Speicherklassen zu:

a. Suchen Sie den Speicherknoten in der LDR-Liste und wählen Sie das Symbol *Bearbeiten* .

b. Wählen Sie aus der Liste die entsprechende Speicherklasse aus.



Weisen Sie einem bestimmten Speicherknoten nur einmal eine Speicherklasse zu. Ein nach einem Ausfall wiederhergestellter Speicherknoten behält die zuvor zugewiesene Speicherklasse bei. Ändern Sie diese Zuweisung nicht, nachdem die ILM-Richtlinie aktiviert wurde. Bei einer Änderung der Zuordnung werden die Daten entsprechend der neuen Speicherklasse gespeichert.

a. Wählen Sie **Änderungen übernehmen**.

Verwenden von Speicherpools

Was ist ein Speicherpool?

Ein Speicherpool ist eine logische Gruppierung von Speicherknoten.

Wenn Sie StorageGRID installieren, wird automatisch ein Speicherpool pro Site erstellt. Sie können je nach Bedarf zusätzliche Speicherpools für Ihre Speicheranforderungen konfigurieren.

Speicherknoten können während der Installation so konfiguriert werden, dass sie Objektdaten und Objektmetadaten oder nur Objektmetadaten enthalten. Nur-Metadaten-Speicherknoten können nicht in Speicherpools verwendet werden. Weitere Informationen finden Sie unter "Arten von Speicherknoten" .

Speicherpools haben zwei Attribute:

- **Speicherqualität**: Bei Speicherknoten die relative Leistung des zugrunde liegenden Speichers.
- **Standort**: Das Rechenzentrum, in dem Objekte gespeichert werden.

Speicherpools werden in ILM-Regeln verwendet, um zu bestimmen, wo Objektdaten gespeichert werden und welcher Speichertyp verwendet wird. Wenn Sie ILM-Regeln für die Replikation konfigurieren, wählen Sie einen oder mehrere Speicherpools aus.

Richtlinien zum Erstellen von Speicherpools

Konfigurieren und verwenden Sie Speicherpools, um Datenverlust durch die Verteilung der Daten auf mehrere Standorte zu verhindern. Für replizierte Kopien und Erasure-Coded-Kopien sind unterschiedliche Speicherpoolkonfigurationen erforderlich.

Sehen "Beispiele für die Aktivierung des Site-Loss-Schutzes durch Replikation und Erasure Coding" .

Richtlinien für alle Speicherpools

- Halten Sie die Speicherpoolkonfigurationen so einfach wie möglich. Erstellen Sie nicht mehr Speicherpools als nötig.
- Erstellen Sie Speicherpools mit so vielen Knoten wie möglich. Jeder Speicherpool sollte zwei oder mehr Knoten enthalten. Ein Speicherpool mit unzureichenden Knoten kann zu ILM-Rückständen führen, wenn ein Knoten nicht mehr verfügbar ist.
- Vermeiden Sie das Erstellen oder Verwenden von Speicherpools, die sich überschneiden (einen oder mehrere gleiche Knoten enthalten). Wenn sich Speicherpools überschneiden, kann es sein, dass mehrere Kopien der Objektdaten auf demselben Knoten gespeichert werden.
- Verwenden Sie im Allgemeinen nicht den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) oder die Site „Alle Sites“. Diese Elemente werden automatisch aktualisiert, um alle neuen Sites einzuschließen, die Sie in einer Erweiterung hinzufügen. Dies entspricht möglicherweise nicht dem gewünschten Verhalten.

Richtlinien für Speicherpools, die für replizierte Kopien verwendet werden

- Zum Schutz vor Site-Loss mit"Replikation" , geben Sie einen oder mehrere standortspezifische Speicherpools in der"Platzierungsanweisungen für jede ILM-Regel" .

  Während der StorageGRID -Installation wird für jeden Standort automatisch ein Speicherpool erstellt.

  Durch die Verwendung eines Speicherpools für jeden Standort wird sichergestellt, dass replizierte Objektkopien genau dort abgelegt werden, wo Sie es erwarten (z. B. eine Kopie jedes Objekts an jedem Standort zum Schutz vor Standortverlust).

- Wenn Sie in einer Erweiterung eine Site hinzufügen, erstellen Sie einen neuen Speicherpool, der nur die neue Site enthält. Dann,"ILM-Regeln aktualisieren" um zu steuern, welche Objekte auf der neuen Site gespeichert werden.
- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Speicherpools, verteilt das System die Kopien, um die Festplattennutzung gleichmäßig auf die Pools zu verteilen.
- Wenn sich die Speicherpools überschneiden (dieselben Speicherknoten enthalten), werden alle Kopien des Objekts möglicherweise nur an einem Standort gespeichert. Sie müssen sicherstellen, dass die ausgewählten Speicherpools nicht dieselben Speicherknoten enthalten.

Richtlinien für Speicherpools, die für Erasure-Coded-Kopien verwendet werden

- Zum Schutz vor Site-Loss mit"Löschcodierung" , erstellen Sie Speicherpools, die aus mindestens drei Sites bestehen. Wenn ein Speicherpool nur zwei Standorte umfasst, können Sie diesen Speicherpool nicht für Erasure Coding verwenden. Für einen Speicherpool mit zwei Standorten sind keine Erasure-Coding-Schemata verfügbar.
- Die Anzahl der im Speicherpool enthaltenen Speicherknoten und Sites bestimmt, welche"Erasure-Coding-Schemata" sind verfügbar.

- Wenn möglich, sollte ein Speicherpool mehr als die Mindestanzahl an Speicherknoten enthalten, die für das von Ihnen ausgewählte Erasure-Coding-Schema erforderlich sind. Wenn Sie beispielsweise ein 6+3-Erasure-Coding-Schema verwenden, müssen Sie über mindestens neun Speicherknoten verfügen. Es wird jedoch empfohlen, mindestens einen zusätzlichen Speicherknoten pro Site zu haben.
- Verteilen Sie die Speicherknoten so gleichmäßig wie möglich auf die Standorte. Um beispielsweise ein 6+3-Erasure-Coding-Schema zu unterstützen, konfigurieren Sie einen Speicherpool, der mindestens drei Speicherknoten an drei Standorten umfasst.
- Wenn Sie hohe Durchsatzanforderungen haben, wird die Verwendung eines Speicherpools mit mehreren Sites nicht empfohlen, wenn die Netzwerklatenz zwischen den Sites größer als 100 ms ist. Mit zunehmender Latenz nimmt die Rate, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des geringeren TCP-Netzwerkdurchsatzes stark ab.

  Die Verringerung des Durchsatzes wirkt sich auf die maximal erreichbaren Raten der Objektaufnahme und des Objektabrufs aus (wenn „Balanced“ oder „Strict“ als Aufnahmeverhalten ausgewählt ist) oder kann zu Rückständen in der ILM-Warteschlange führen (wenn „Dual Commit“ als Aufnahmeverhalten ausgewählt ist). Sehen "ILM-Regelaufnahmeverhalten" .

> Wenn Ihr Grid nur eine Site umfasst, können Sie den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) oder die Site „Alle Sites“ in einem Erasure-Coding-Profil nicht verwenden. Dieses Verhalten verhindert, dass das Profil ungültig wird, wenn eine zweite Site hinzugefügt wird.

Aktivieren Sie den Site-Loss-Schutz

Wenn Ihre StorageGRID Bereitstellung mehr als einen Standort umfasst, können Sie Replikation und Erasure Coding mit entsprechend konfigurierten Speicherpools verwenden, um einen Schutz vor Standortverlust zu aktivieren.

Replikation und Erasure Coding erfordern unterschiedliche Speicherpoolkonfigurationen:

- Um die Replikation zum Schutz vor Site-Verlust zu nutzen, verwenden Sie die standortspezifischen Speicherpools, die während der StorageGRID -Installation automatisch erstellt werden. Erstellen Sie anschließend ILM-Regeln mit"Platzierungsanweisungen" die mehrere Speicherpools angeben, sodass an jedem Standort eine Kopie jedes Objekts abgelegt wird.
- Um Erasure Coding zum Schutz vor Site-Loss zu verwenden,"Erstellen Sie Speicherpools, die aus mehreren Sites bestehen" . Erstellen Sie dann ILM-Regeln, die einen Speicherpool verwenden, der aus mehreren Sites und allen verfügbaren Erasure-Coding-Schemata besteht.

> Bei der Konfiguration Ihrer StorageGRID -Bereitstellung für den Site-Loss-Schutz müssen Sie auch die Auswirkungen von"Aufnahmeoptionen" Und"Konsistenz" .

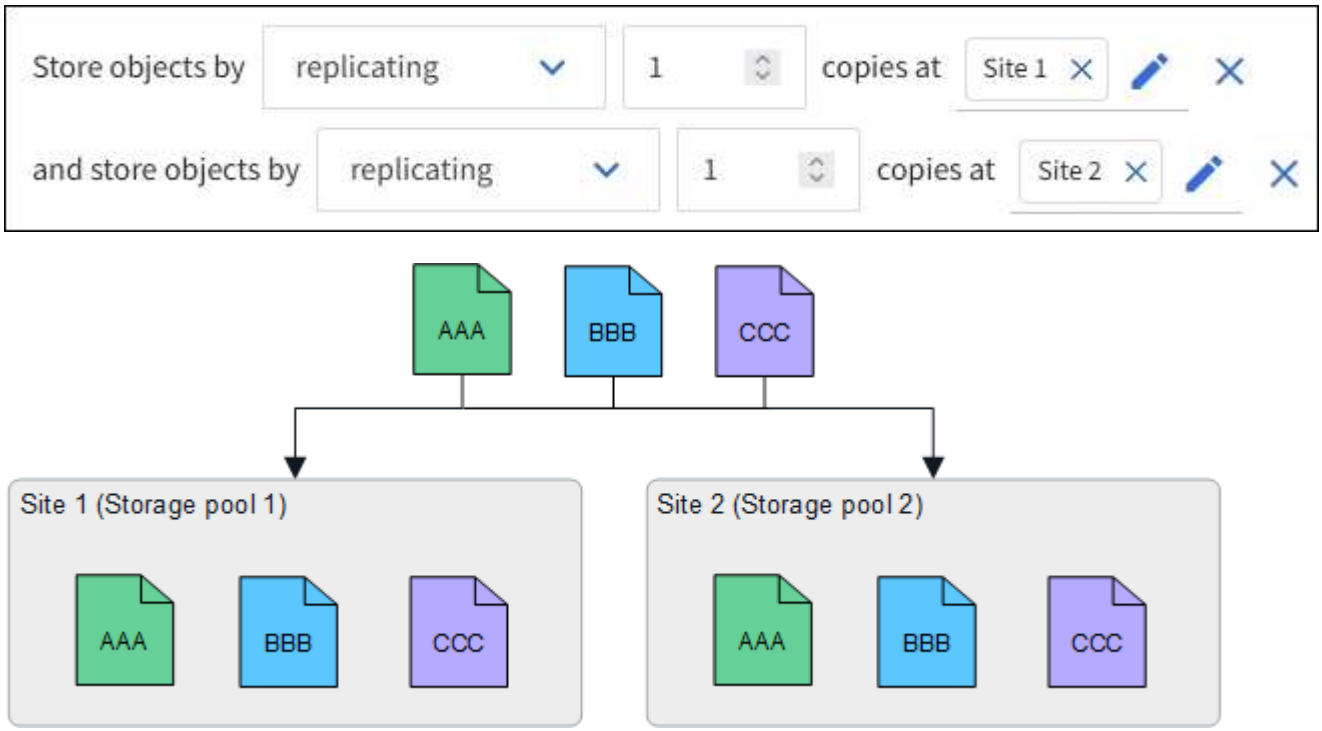
Replikationsbeispiel

Standardmäßig wird während der StorageGRID -Installation für jede Site ein Speicherpool erstellt. Wenn Sie über Speicherpools verfügen, die nur aus einem Standort bestehen, können Sie ILM-Regeln konfigurieren, die zum Schutz vor Standortverlust die Replikation verwenden. In diesem Beispiel:

- Speicherpool 1 enthält Standort 1
- Speicherpool 2 enthält Standort 2
- Die ILM-Regel enthält zwei Platzierungen:

- Speichern Sie Objekte, indem Sie 1 Kopie an Standort 1 replizieren
- Speichern Sie Objekte, indem Sie 1 Kopie an Standort 2 replizieren

ILM-Regelplatzierungen:



Bei Verlust eines Standorts sind Kopien der Objekte am anderen Standort verfügbar.

Beispiel für Erasure Coding

Wenn Sie über Speicherpools verfügen, die aus mehr als einem Standort pro Speicherpool bestehen, können Sie ILM-Regeln konfigurieren, die Erasure Coding zum Schutz vor Standortverlust verwenden. In diesem Beispiel:

- Speicherpool 1 enthält die Standorte 1 bis 3
- Die ILM-Regel enthält eine Platzierung: Speichern Sie Objekte durch Erasure Coding mit einem 4+2 EC-Schema im Speicherpool 1, der drei Standorte enthält

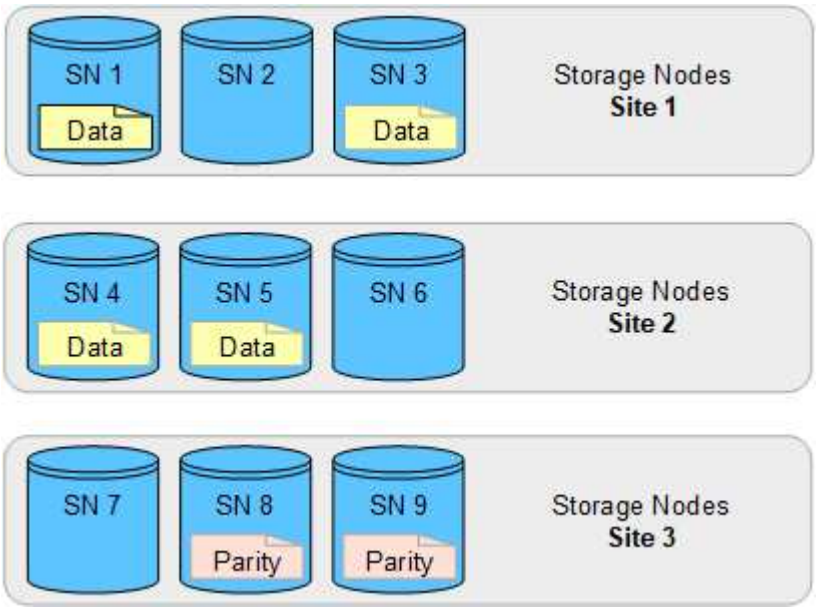
ILM-Regelplatzierungen:

In diesem Beispiel:

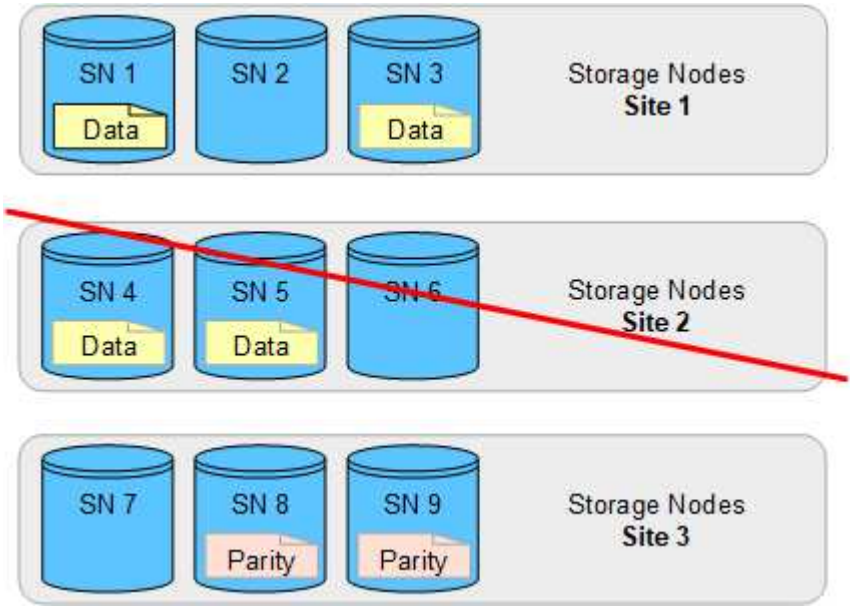
- Die ILM-Regel verwendet ein 4+2-Erasure-Coding-Schema.
- Jedes Objekt wird in vier gleiche Datenfragmente aufgeteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet.
- Jedes der sechs Fragmente wird auf einem anderen Knoten an drei Rechenzentrumsstandorten gespeichert, um Datenschutz bei Knotenausfällen oder Standortverlust zu gewährleisten.

Erasure Coding ist in Speicherpools zulässig, die eine beliebige Anzahl von Standorten enthalten, *außer* zwei Standorten.

ILM-Regel mit 4+2-Erasure-Coding-Schema:



Wenn eine Site verloren geht, können die Daten dennoch wiederhergestellt werden:



Erstellen eines Speicherpools

Sie erstellen Speicherpools, um zu bestimmen, wo das StorageGRID -System Objektdaten speichert und welche Art von Speicher verwendet wird. Jeder Speicherpool umfasst einen oder mehrere Standorte und eine oder mehrere Speicherklassen.

Wenn Sie StorageGRID 11.9 auf einem neuen Grid installieren, werden für jeden Standort automatisch Speicherpools erstellt. Wenn Sie jedoch StorageGRID 11.6 oder früher ursprünglich installiert haben, werden Speicherpools nicht automatisch für jede Site erstellt.

Wenn Sie Cloud Storage Pools erstellen möchten, um Objektdaten außerhalb Ihres StorageGRID -Systems zu speichern, lesen Sie die"Informationen zur Verwendung von Cloud Storage Pools" .

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die Richtlinien zum Erstellen von Speicherpools gelesen.

Informationen zu diesem Vorgang

Speicherpools bestimmen, wo Objektdaten gespeichert werden. Die Anzahl der benötigten Speicherpools hängt von der Anzahl der Sites in Ihrem Grid und von den gewünschten Kopietypen ab: repliziert oder erasure-coded.

- Erstellen Sie für die Replikation und die Erasure Coding-Funktion für einzelne Standorte einen Speicherpool für jeden Standort. Wenn Sie beispielsweise replizierte Objektkopien an drei Standorten speichern möchten, erstellen Sie drei Speicherpools.
- Erstellen Sie für die Erasure Coding-Funktion an drei oder mehr Standorten einen Speicherpool, der für jeden Standort einen Eintrag enthält. Wenn Sie beispielsweise Erasure-Code-Objekte an drei Standorten verwalten möchten, erstellen Sie einen Speicherpool.

> Schließen Sie die Site „Alle Sites“ nicht in einen Speicherpool ein, der in einem Erasure-Coding-Profil verwendet wird. Fügen Sie stattdessen für jede Site, in der löschcodierte Daten gespeichert werden, einen separaten Eintrag zum Speicherpool hinzu. Sehendieser Schritt für ein Beispiel.

- Wenn Sie über mehr als eine Speicherklasse verfügen, erstellen Sie keinen Speicherpool, der verschiedene Speicherklassen an einem einzigen Standort umfasst. Siehe die"Richtlinien zum Erstellen von Speicherpools" .

Schritte

1. Wählen Sie **ILM** > **Speicherpools**.

   Auf der Registerkarte „Speicherpools“ werden alle definierten Speicherpools aufgelistet.

   > Bei Neuinstallationen von StorageGRID 11.6 oder früher wird der Speicherpool „Alle Speicherknoten“ automatisch aktualisiert, wenn Sie neue Rechenzentrumsstandorte hinzufügen. Verwenden Sie diesen Pool nicht in ILM-Regeln.

2. Um einen neuen Speicherpool zu erstellen, wählen Sie **Erstellen**.
3. Geben Sie einen eindeutigen Namen für den Speicherpool ein. Verwenden Sie einen Namen, der beim Konfigurieren von Erasure-Coding-Profilen und ILM-Regeln leicht zu identifizieren ist.
4. Wählen Sie aus der Dropdown-Liste **Site** eine Site für diesen Speicherpool aus.

   Wenn Sie eine Site auswählen, wird die Anzahl der Speicherknoten in der Tabelle automatisch aktualisiert.

   Verwenden Sie die Site „Alle Sites“ grundsätzlich nicht in einem Speicherpool. ILM-Regeln, die einen All-Sites-Speicherpool verwenden, platzieren Objekte an jedem verfügbaren Standort, wodurch Sie weniger Kontrolle über die Objektplatzierung haben. Außerdem verwendet ein All-Sites-Speicherpool die Speicherknoten an einem neuen Standort sofort, was möglicherweise nicht dem von Ihnen erwarteten Verhalten entspricht.

5. Wählen Sie aus der Dropdown-Liste **Speichergrad** den Speichertyp aus, der verwendet wird, wenn eine ILM-Regel diesen Speicherpool verwendet.

   Die Speicherklasse, *umfasst alle Speicherklassen*, umfasst alle Speicherknoten am ausgewählten Standort. Wenn Sie zusätzliche Speicherklassen für die Speicherknoten in Ihrem Raster erstellt haben, werden diese in der Dropdown-Liste aufgeführt.

6. Wenn Sie den Speicherpool in einem Erasure-Coding-Profil für mehrere Sites verwenden möchten, wählen Sie **Weitere Knoten hinzufügen**, um dem Speicherpool für jede Site einen Eintrag hinzuzufügen.

   > Sie werden gewarnt, wenn Sie für eine Site mehr als einen Eintrag mit unterschiedlichen Speicherklassen hinzufügen.

   Um einen Eintrag zu entfernen, wählen Sie das Löschsymbol ✕ .

7. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie **Speichern**.

   Der neue Speicherpool wird der Liste hinzugefügt.

Anzeigen von Speicherpooldetails

Sie können die Details eines Speicherpools anzeigen, um festzustellen, wo der Speicherpool verwendet wird und welche Knoten und Speicherklassen enthalten sind.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **ILM** > **Speicherpools**.

   Die Tabelle „Speicherpools“ enthält die folgenden Informationen für jeden Speicherpool, der Speicherknoten enthält:

   - **Name**: Der eindeutige Anzeigename des Speicherpools.
   - **Knotenanzahl**: Die Anzahl der Knoten im Speicherpool.
   - **Speichernutzung**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten auf diesem Knoten verwendet wurde. Dieser Wert enthält keine Objektmetadaten.
   - **Gesamtkapazität**: Die Größe des Speicherpools, die der Gesamtmenge des nutzbaren Speicherplatzes für Objektdaten für alle Knoten im Speicherpool entspricht.
   - **ILM-Nutzung**: Wie der Speicherpool derzeit genutzt wird. Ein Speicherpool wird möglicherweise nicht verwendet oder in einer oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beidem verwendet.

2. Um Details zu einem bestimmten Speicherpool anzuzeigen, wählen Sie seinen Namen aus.

   Die Detailseite für den Speicherpool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Knoten** an, um mehr über die im Speicherpool enthaltenen Speicherknoten zu erfahren.

   Die Tabelle enthält für jeden Knoten die folgenden Informationen:

- Knotenname
- Sitename
- Lagerqualität
- Speichernutzung: Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der für den Speicherknoten verwendet wurde.

> ⓘ Derselbe Wert für die Speichernutzung (%) wird auch im Diagramm „Speichernutzung – Objektdaten“ für jeden Speicherknoten angezeigt (wählen Sie **KNOTEN** > ***Speicherknoten*** > **Speicher**).

4. Sehen Sie sich die Registerkarte **ILM-Nutzung** an, um festzustellen, ob der Speicherpool derzeit in ILM-Regeln oder Erasure-Coding-Profilen verwendet wird.
5. Optional können Sie auf die **ILM-Regelseite** gehen, um mehr über die Regeln zu erfahren und diese zu verwalten, die den Speicherpool verwenden.

   Siehe die"Anleitung zum Arbeiten mit ILM-Regeln" .

Speicherpool bearbeiten

Sie können einen Speicherpool bearbeiten, um seinen Namen zu ändern oder Standorte und Speicherklassen zu aktualisieren.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die"Richtlinien zum Erstellen von Speicherpools" .
- Wenn Sie einen Speicherpool bearbeiten möchten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, haben Sie berücksichtigt, wie sich Ihre Änderungen auf die Platzierung der Objektdaten auswirken.

Informationen zu diesem Vorgang

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, einen neuen Standort oder eine neue Speicherklasse hinzufügen, beachten Sie, dass die Speicherknoten am neuen Standort oder in der neuen Speicherklasse nicht automatisch verwendet werden. Um StorageGRID zur Verwendung einer neuen Site oder Speicherklasse zu zwingen, müssen Sie nach dem Speichern des bearbeiteten Speicherpools eine neue ILM-Richtlinie aktivieren.

Schritte

1. Wählen Sie **ILM** > **Speicherpools**.
2. Aktivieren Sie das Kontrollkästchen für den Speicherpool, den Sie bearbeiten möchten.

   Sie können den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) nicht bearbeiten.

3. Wählen Sie **Bearbeiten**.
4. Ändern Sie bei Bedarf den Namen des Speicherpools.
5. Wählen Sie bei Bedarf andere Standorte und Lagerklassen aus.

   Sie können den Standort oder die Speicherklasse nicht ändern, wenn der Speicherpool in einem Erasure-

Coding-Profil verwendet wird und die Änderung dazu führen würde, dass das Erasure-Coding-Schema ungültig wird. Wenn beispielsweise ein in einem Erasure-Coding-Profil verwendeter Speicherpool derzeit eine Speicherklasse mit nur einem Standort enthält, können Sie keine Speicherklasse mit zwei Standorten verwenden, da die Änderung das Erasure-Coding-Schema ungültig machen würde.

> Durch das Hinzufügen oder Entfernen von Sites aus einem vorhandenen Speicherpool werden keine vorhandenen, löschcodierten Daten verschoben. Wenn Sie die vorhandenen Daten von der Site verschieben möchten, müssen Sie einen neuen Speicherpool und ein neues EC-Profil erstellen, um die Daten neu zu kodieren.

6. Wählen Sie **Speichern**.

Nach Abschluss

Wenn Sie einem in der aktiven ILM-Richtlinie verwendeten Speicherpool eine neue Site oder Speicherklasse hinzugefügt haben, aktivieren Sie eine neue ILM-Richtlinie, um StorageGRID zur Verwendung der neuen Site oder Speicherklasse zu zwingen. Klonen Sie beispielsweise Ihre vorhandene ILM-Richtlinie und aktivieren Sie dann den Klon. Sehen "Arbeiten mit ILM-Regeln und ILM-Richtlinien" .

Entfernen eines Speicherpools

Sie können einen Speicherpool entfernen, der nicht verwendet wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **ILM** > **Speicherpools**.
2. Sehen Sie sich die Spalte „ILM-Nutzung“ in der Tabelle an, um festzustellen, ob Sie den Speicherpool entfernen können.

   Sie können einen Speicherpool nicht entfernen, wenn er in einer ILM-Regel oder in einem Erasure-Coding-Profil verwendet wird. Wählen Sie bei Bedarf ***Speicherpoolname*** > **ILM-Verwendung** aus, um zu bestimmen, wo der Speicherpool verwendet wird.

3. Wenn der Speicherpool, den Sie entfernen möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen.
4. Wählen Sie **Entfernen**.
5. Wählen Sie **OK**.

Verwenden Sie Cloud-Speicherpools

Was ist ein Cloud-Speicherpool?

Mit einem Cloud-Speicherpool können Sie mithilfe von ILM Objektdaten außerhalb Ihres StorageGRID Systems verschieben. Beispielsweise möchten Sie möglicherweise selten aufgerufene Objekte in einen kostengünstigeren Cloud-Speicher verschieben, etwa Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archivzugriffsebene im Microsoft Azure Blob-Speicher. Oder Sie möchten möglicherweise ein Cloud-Backup von StorageGRID -Objekten verwalten, um die Notfallwiederherstellung zu verbessern.

Aus ILM-Sicht ähnelt ein Cloud-Speicherpool einem Speicherpool. Um Objekte an einem der beiden Speicherorte zu speichern, wählen Sie den Pool aus, wenn Sie die Platzierungsanweisungen für eine ILM-Regel erstellen. Während Speicherpools jedoch aus Speicherknoten innerhalb des StorageGRID Systems bestehen, besteht ein Cloud-Speicherpool aus einem externen Bucket (S3) oder Container (Azure Blob-Speicher).

Die Tabelle vergleicht Speicherpools mit Cloud-Speicherpools und zeigt die allgemeinen Ähnlichkeiten und Unterschiede.

	Speicherpool	**Cloud-Speicherpool**
Wie entsteht es?	Verwenden Sie die Option **ILM** > **Speicherpools** im Grid Manager.	Verwenden Sie die Option **ILM** > **Speicherpools** > **Cloud-Speicherpools** im Grid Manager. Sie müssen den externen Bucket oder Container einrichten, bevor Sie den Cloud Storage Pool erstellen können.
Wie viele Pools können Sie erstellen?	Unbegrenzt.	Bis zu 10.
Wo werden Objekte gespeichert?	Auf einem oder mehreren Speicherknoten innerhalb von StorageGRID.	In einem Amazon S3-Bucket, Azure Blob-Speichercontainer oder Google Cloud, der sich außerhalb des StorageGRID Systems befindet. Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist: • Sie können optional einen Bucket-Lebenszyklus konfigurieren, um Objekte in einen kostengünstigen Langzeitspeicher wie Amazon S3 Glacier oder S3 Glacier Deep Archive zu verschieben. Das externe Speichersystem muss die Glacier-Speicherklasse und die S3 RestoreObject-API unterstützen. • Sie können Cloud-Speicherpools zur Verwendung mit AWS Commercial Cloud Services (C2S) erstellen, die die AWS Secret Region unterstützen. Wenn es sich bei dem Cloud-Speicherpool um einen Azure Blob-Speichercontainer handelt, überträgt StorageGRID das Objekt in die Archivebene. **Hinweis:** Konfigurieren Sie die Lebenszyklusverwaltung des Azure Blob-Speichers grundsätzlich nicht für den Container, der für einen Cloud-Speicherpool verwendet wird. RestoreObject-Vorgänge für Objekte im Cloud-Speicherpool können durch den konfigurierten Lebenszyklus beeinflusst werden.
Was steuert die Objektplatzierung?	Eine ILM-Regel in den aktiven ILM-Richtlinien.	Eine ILM-Regel in den aktiven ILM-Richtlinien.

	Speicherpool	Cloud-Speicherpool
Welche Datenschutzmethode wird verwendet?	Replikation oder Erasure Coding.	Replikation.
Wie viele Kopien jedes Objekts sind zulässig?	Mehrere.	Eine Kopie im Cloud Storage Pool und optional eine oder mehrere Kopien in StorageGRID. **Hinweis:** Sie können ein Objekt nicht gleichzeitig in mehr als einem Cloud-Speicherpool speichern.
Was sind die Vorteile?	Objekte sind jederzeit schnell zugänglich.	Kostengünstige Lagerung. **Hinweis**: FabricPool Daten können nicht in Cloud-Speicherpools gestaffelt werden.

Lebenszyklus eines Cloud Storage Pool-Objekts

Überprüfen Sie vor der Implementierung von Cloud-Speicherpools den Lebenszyklus der Objekte, die in den einzelnen Arten von Cloud-Speicherpools gespeichert sind.

S3: Lebenszyklus eines Cloud Storage Pool-Objekts

Die Schritte beschreiben die Lebenszyklusphasen eines Objekts, das in einem S3 Cloud Storage Pool gespeichert ist.

> ⓘ „Glacier“ bezieht sich sowohl auf die Speicherklasse Glacier als auch auf die Speicherklasse Glacier Deep Archive, mit einer Ausnahme: Die Speicherklasse Glacier Deep Archive unterstützt die Ebene „Expedited Restore“ nicht. Es wird nur der Massen- oder Standardabruf unterstützt.

> ⓘ Die Google Cloud Platform (GCP) unterstützt das Abrufen von Objekten aus dem Langzeitspeicher, ohne dass ein POST-Wiederherstellungsvorgang erforderlich ist.

1. *Objekt in StorageGRID gespeichert *

   Um den Lebenszyklus zu starten, speichert eine Clientanwendung ein Objekt in StorageGRID.

2. **Objekt in S3 Cloud Storage Pool verschoben**
   - Wenn das Objekt einer ILM-Regel entspricht, die einen S3-Cloud-Speicherpool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den vom Cloud-Speicherpool angegebenen externen S3-Bucket.
   - Wenn das Objekt in den S3 Cloud Storage Pool verschoben wurde, kann die Clientanwendung es mithilfe einer S3 GetObject-Anforderung von StorageGRID abrufen, es sei denn, das Objekt wurde in den Glacier-Speicher verschoben.
3. **Objekt in Glacier überführt (nicht abrufbarer Zustand)**

- Optional kann das Objekt in den Glacier-Speicher übertragen werden. Beispielsweise kann der externe S3-Bucket die Lebenszykluskonfiguration verwenden, um ein Objekt sofort oder nach einer bestimmten Anzahl von Tagen in den Glacier-Speicher zu übertragen.

  > Wenn Sie Objekte übertragen möchten, müssen Sie eine Lebenszykluskonfiguration für den externen S3-Bucket erstellen und eine Speicherlösung verwenden, die die Glacier-Speicherklasse implementiert und die S3 RestoreObject-API unterstützt.

- Während des Übergangs kann die Clientanwendung eine S3 HeadObject-Anforderung verwenden, um den Status des Objekts zu überwachen.

4. **Objekt aus dem Glacier-Speicher wiederhergestellt**

   Wenn ein Objekt in den Glacier-Speicher verschoben wurde, kann die Clientanwendung eine S3 RestoreObject-Anforderung ausgeben, um eine abrufbare Kopie im S3 Cloud Storage Pool wiederherzustellen. Die Anforderung gibt an, wie viele Tage die Kopie im Cloud-Speicherpool verfügbar sein soll und welche Datenzugriffsebene für den Wiederherstellungsvorgang verwendet werden soll (Beschleunigt, Standard oder Massen). Wenn das Ablaufdatum der abrufbaren Kopie erreicht ist, wird die Kopie automatisch in einen nicht abrufbaren Zustand zurückversetzt.

   > Wenn eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, ist es nicht erforderlich, das Objekt durch Ausgeben einer RestoreObject-Anforderung aus Glacier wiederherzustellen. Stattdessen kann die lokale Kopie direkt mithilfe einer GetObject-Anforderung abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt wiederhergestellt wurde, kann die Clientanwendung eine GetObject-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Azure: Lebenszyklus eines Cloud Storage Pool-Objekts

Die Schritte beschreiben die Lebenszyklusphasen eines Objekts, das in einem Azure Cloud Storage Pool gespeichert ist.

1. *Objekt in StorageGRID gespeichert *

   Um den Lebenszyklus zu starten, speichert eine Clientanwendung ein Objekt in StorageGRID.

2. **Objekt in Azure Cloud Storage Pool verschoben**

   Wenn das Objekt einer ILM-Regel entspricht, die einen Azure Cloud Storage Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den vom Cloud Storage Pool angegebenen externen Azure Blob-Speichercontainer.

3. **Objekt in die Archivebene überführt (nicht abrufbarer Zustand)**

   Unmittelbar nach dem Verschieben des Objekts in den Azure Cloud Storage Pool überträgt StorageGRID das Objekt automatisch in die Archivebene des Azure Blob-Speichers.

4. **Objekt aus Archivebene wiederhergestellt**

   Wenn ein Objekt in die Archivebene verschoben wurde, kann die Clientanwendung eine S3 RestoreObject-Anforderung ausgeben, um eine abrufbare Kopie im Azure Cloud Storage Pool wiederherzustellen.

Wenn StorageGRID das RestoreObject empfängt, überträgt es das Objekt vorübergehend in die Cool-Ebene des Azure Blob-Speichers. Sobald das Ablaufdatum in der RestoreObject-Anforderung erreicht ist, überträgt StorageGRID das Objekt zurück in die Archivebene.

> Wenn eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, ist es nicht erforderlich, das Objekt durch Ausgeben einer RestoreObject-Anforderung aus der Archivzugriffsebene wiederherzustellen. Stattdessen kann die lokale Kopie direkt mithilfe einer GetObject-Anforderung abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt im Azure Cloud Storage Pool wiederhergestellt wurde, kann die Clientanwendung eine GetObject-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Ähnliche Informationen

"Verwenden Sie die S3 REST-API"

Wann Sie Cloud-Speicherpools verwenden sollten

Mithilfe von Cloud-Speicherpools können Sie Daten an einem externen Speicherort sichern oder stufenweise speichern. Darüber hinaus können Sie Daten in mehr als einer Cloud sichern oder stufenweise speichern.

Sichern Sie StorageGRID Daten an einem externen Speicherort

Sie können einen Cloud-Speicherpool verwenden, um StorageGRID -Objekte an einem externen Speicherort zu sichern.

Wenn auf die Kopien in StorageGRID nicht zugegriffen werden kann, können die Objektdaten im Cloud Storage Pool zum Bearbeiten von Clientanforderungen verwendet werden. Möglicherweise müssen Sie jedoch eine S3 RestoreObject-Anforderung stellen, um auf die Sicherungsobjektkopie im Cloud-Speicherpool zuzugreifen.

Die Objektdaten in einem Cloud-Speicherpool können auch verwendet werden, um Daten wiederherzustellen, die aufgrund eines Speichervolumes oder Speicherknotenausfalls aus StorageGRID verloren gegangen sind. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Speicherknoten.

So implementieren Sie eine Backup-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Speicherpool.
2. Konfigurieren Sie eine ILM-Regel, die gleichzeitig Objektkopien auf Speicherknoten (als replizierte oder erasure-coded Kopien) und eine einzelne Objektkopie im Cloud-Speicherpool speichert.
3. Fügen Sie die Regel zu Ihrer ILM-Richtlinie hinzu. Simulieren und aktivieren Sie dann die Richtlinie.

Daten von StorageGRID an einen externen Speicherort verschieben

Sie können einen Cloud-Speicherpool verwenden, um Objekte außerhalb des StorageGRID Systems zu speichern. Nehmen wir beispielsweise an, Sie müssen eine große Anzahl von Objekten aufbewahren, rechnen aber damit, dass Sie nur selten oder nie auf diese Objekte zugreifen werden. Sie können einen Cloud-Speicherpool verwenden, um die Objekte auf kostengünstigeren Speicher zu verschieben und Speicherplatz in

StorageGRID freizugeben.

So implementieren Sie eine Tiering-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Speicherpool.
2. Konfigurieren Sie eine ILM-Regel, die selten verwendete Objekte von Speicherknoten in den Cloud-Speicherpool verschiebt.
3. Fügen Sie die Regel zu Ihrer ILM-Richtlinie hinzu. Simulieren und aktivieren Sie dann die Richtlinie.

Verwalten Sie mehrere Cloud-Endpunkte

Sie können mehrere Cloud Storage Pool-Endpunkte konfigurieren, wenn Sie Objektdaten in mehreren Clouds schichten oder sichern möchten. Mit den Filtern in Ihren ILM-Regeln können Sie angeben, welche Objekte in jedem Cloud-Speicherpool gespeichert werden. Beispielsweise möchten Sie möglicherweise Objekte einiger Mandanten oder Buckets in Amazon S3 Glacier und Objekte anderer Mandanten oder Buckets im Azure Blob-Speicher speichern. Oder Sie möchten Daten zwischen Amazon S3 Glacier und Azure Blob Storage verschieben.

> Wenn Sie mehrere Cloud Storage Pool-Endpunkte verwenden, beachten Sie, dass ein Objekt jeweils nur in einem Cloud Storage Pool gespeichert werden kann.

So implementieren Sie mehrere Cloud-Endpunkte:

1. Erstellen Sie bis zu 10 Cloud-Speicherpools.
2. Konfigurieren Sie ILM-Regeln, um die entsprechenden Objektdaten zum entsprechenden Zeitpunkt in jedem Cloud-Speicherpool zu speichern. Speichern Sie beispielsweise Objekte aus Bucket A in Cloud Storage Pool A und Objekte aus Bucket B in Cloud Storage Pool B. Oder speichern Sie Objekte für eine gewisse Zeit in Cloud Storage Pool A und verschieben Sie sie dann in Cloud Storage Pool B.
3. Fügen Sie die Regeln zu Ihrer ILM-Richtlinie hinzu. Simulieren und aktivieren Sie dann die Richtlinie.

Überlegungen zu Cloud-Speicherpools

Wenn Sie planen, einen Cloud-Speicherpool zum Verschieben von Objekten aus dem StorageGRID System zu verwenden, müssen Sie die Überlegungen zur Konfiguration und Verwendung von Cloud-Speicherpools überprüfen.

Allgemeine Überlegungen

- Im Allgemeinen ist Cloud-Archivspeicher wie Amazon S3 Glacier oder Azure Blob Storage ein kostengünstiger Ort zum Speichern von Objektdaten. Allerdings sind die Kosten für den Abruf von Daten aus Cloud-Archivspeichern relativ hoch. Um die Gesamtkosten so gering wie möglich zu halten, müssen Sie berücksichtigen, wann und wie oft Sie auf die Objekte im Cloud-Speicherpool zugreifen. Die Verwendung eines Cloud-Speicherpools wird nur für Inhalte empfohlen, auf die Sie voraussichtlich nur selten zugreifen.
- Die Verwendung von Cloud Storage Pools mit FabricPool wird aufgrund der zusätzlichen Latenz beim Abrufen eines Objekts vom Cloud Storage Pool-Ziel nicht unterstützt.
- Objekte mit aktivierter S3-Objektsperre können nicht in Cloud-Speicherpools platziert werden.
- Wenn für den Ziel-S3-Bucket eines Cloud Storage Pools die S3-Objektsperre aktiviert ist, schlägt der Versuch, die Bucket-Replikation (PutBucketReplication) zu konfigurieren, mit einem AccessDenied-Fehler fehl.

- Die folgenden Plattform-, Authentifizierungs- und Protokollkombinationen mit S3-Objektsperre werden für Cloud-Speicherpools nicht unterstützt:
  - **Plattformen**: Google Cloud Platform und Azure
  - **Authentifizierungstypen**: IAM Roles Anywhere und anonymer Zugriff
  - **Protokoll**: HTTP

Überlegungen zu den für Cloud Storage Pools verwendeten Ports

Um sicherzustellen, dass die ILM-Regeln Objekte zum und vom angegebenen Cloud-Speicherpool verschieben können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die die Speicherknoten Ihres Systems enthalten. Sie müssen sicherstellen, dass die folgenden Ports mit dem Cloud-Speicherpool kommunizieren können.

Standardmäßig verwenden Cloud Storage Pools die folgenden Ports:

- **80**: Für Endpunkt-URIs, die mit http beginnen
- **443**: Für Endpunkt-URIs, die mit https beginnen

Sie können beim Erstellen oder Bearbeiten eines Cloud-Speicherpools einen anderen Port angeben.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie außerdem"Konfigurieren eines Speicherproxys" um das Senden von Nachrichten an externe Endpunkte zu ermöglichen, beispielsweise an einen Endpunkt im Internet.

Überlegungen zu den Kosten

Der Zugriff auf Speicher in der Cloud mithilfe eines Cloud-Speicherpools erfordert eine Netzwerkverbindung zur Cloud. Sie müssen die Kosten der Netzwerkinfrastruktur berücksichtigen, die Sie für den Zugriff auf die Cloud verwenden, und diese entsprechend bereitstellen, basierend auf der Datenmenge, die Sie voraussichtlich mithilfe des Cloud Storage Pools zwischen StorageGRID und der Cloud verschieben werden.

Wenn StorageGRID eine Verbindung zum externen Cloud Storage Pool-Endpunkt herstellt, sendet es verschiedene Anfragen, um die Konnektivität zu überwachen und sicherzustellen, dass die erforderlichen Vorgänge ausgeführt werden können. Obwohl mit diesen Anfragen einige zusätzliche Kosten verbunden sind, sollten die Kosten für die Überwachung eines Cloud-Speicherpools nur einen kleinen Bruchteil der Gesamtkosten für die Speicherung von Objekten in S3 oder Azure ausmachen.

Wenn Sie Objekte von einem externen Cloud Storage Pool-Endpunkt zurück zu StorageGRID verschieben müssen, können höhere Kosten anfallen. In einem der folgenden Fälle können Objekte zurück zu StorageGRID verschoben werden:

- Die einzige Kopie des Objekts befindet sich in einem Cloud-Speicherpool und Sie entscheiden sich, das Objekt stattdessen in StorageGRID zu speichern. In diesem Fall konfigurieren Sie Ihre ILM-Regeln und -Richtlinien neu. Bei der ILM-Auswertung sendet StorageGRID mehrere Anfragen, um das Objekt aus dem Cloud-Speicherpool abzurufen. StorageGRID erstellt dann lokal die angegebene Anzahl replizierter oder löschcodierter Kopien. Nachdem das Objekt zurück zu StorageGRID verschoben wurde, wird die Kopie im Cloud Storage Pool gelöscht.
- Aufgrund eines Speicherknotenfehlers gehen Objekte verloren. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Speicherknoten.

Wenn Objekte aus einem Cloud Storage Pool zurück zu StorageGRID verschoben werden, sendet StorageGRID für jedes Objekt mehrere Anfragen an den Endpunkt des Cloud Storage Pools. Bevor Sie eine große Anzahl von Objekten verschieben, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Zeitrahmens und der damit verbundenen Kosten zu erhalten.

S3: Für den Cloud Storage Pool-Bucket erforderliche Berechtigungen

Die Richtlinien für den externen S3-Bucket, der für einen Cloud Storage Pool verwendet wird, müssen StorageGRID die Berechtigung erteilen, ein Objekt in den Bucket zu verschieben, den Status eines Objekts abzurufen, ein Objekt bei Bedarf aus dem Glacier-Speicher wiederherzustellen und mehr. Idealerweise sollte StorageGRID vollen Zugriff auf den Bucket haben(`s3:*`); wenn dies jedoch nicht möglich ist, muss die Bucket-Richtlinie StorageGRID die folgenden S3-Berechtigungen erteilen:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Überlegungen zum Lebenszyklus des externen Buckets

Die Bewegung von Objekten zwischen StorageGRID und dem im Cloud Storage Pool angegebenen externen S3-Bucket wird durch ILM-Regeln und die aktiven ILM-Richtlinien in StorageGRID gesteuert. Im Gegensatz dazu wird der Übergang von Objekten aus dem im Cloud Storage Pool angegebenen externen S3-Bucket zu Amazon S3 Glacier oder S3 Glacier Deep Archive (oder zu einer Speicherlösung, die die Glacier-Speicherklasse implementiert) durch die Lebenszykluskonfiguration dieses Buckets gesteuert.

Wenn Sie Objekte aus dem Cloud Storage Pool übertragen möchten, müssen Sie die entsprechende Lebenszykluskonfiguration im externen S3-Bucket erstellen und eine Speicherlösung verwenden, die die Glacier-Speicherklasse implementiert und die S3 RestoreObject-API unterstützt.

Angenommen, Sie möchten, dass alle Objekte, die von StorageGRID in den Cloud Storage Pool verschoben werden, sofort in den Amazon S3 Glacier-Speicher übertragen werden. Sie würden eine Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen, die eine einzelne Aktion (**Übergang**) wie folgt angibt:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Diese Regel würde alle Bucket-Objekte am Tag ihrer Erstellung (d. h. am Tag ihrer Verschiebung von StorageGRID in den Cloud Storage Pool) auf Amazon S3 Glacier übertragen.

> Verwenden Sie beim Konfigurieren des Lebenszyklus des externen Buckets niemals **Ablauf** -Aktionen, um zu definieren, wann Objekte ablaufen. Ablaufaktionen führen dazu, dass das externe Speichersystem abgelaufene Objekte löscht. Wenn Sie später versuchen, auf ein abgelaufenes Objekt von StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Wenn Sie Objekte im Cloud Storage Pool in das S3 Glacier Deep Archive (statt in Amazon S3 Glacier) übertragen möchten, geben Sie an `<StorageClass>DEEP_ARCHIVE</StorageClass>` im Bucket-Lebenszyklus. Beachten Sie jedoch, dass Sie die `Expedited` Ebene zum Wiederherstellen von Objekten aus S3 Glacier Deep Archive.

Azure: Überlegungen zur Zugriffsebene

Wenn Sie ein Azure-Speicherkonto konfigurieren, können Sie die Standardzugriffsebene auf „Heiß“ oder „Kalt“ festlegen. Wenn Sie ein Speicherkonto zur Verwendung mit einem Cloud-Speicherpool erstellen, sollten Sie die Hot-Tier-Ebene als Standardebene verwenden. Obwohl StorageGRID die Stufe sofort auf „Archiv“ setzt, wenn es Objekte in den Cloud Storage Pool verschiebt, stellt die Verwendung der Standardeinstellung „Hot“ sicher, dass Ihnen für Objekte, die vor Ablauf der Mindestdauer von 30 Tagen aus der Stufe „Cool“ entfernt werden, keine Gebühr für die vorzeitige Löschung berechnet wird.

Azure: Lebenszyklusverwaltung wird nicht unterstützt

Verwenden Sie für den mit einem Cloud-Speicherpool verwendeten Container nicht die Azure Blob-Speicherlebenszyklusverwaltung. Die Lebenszyklusvorgänge können die Vorgänge des Cloud Storage Pools beeinträchtigen.

Ähnliche Informationen

"Erstellen Sie einen Cloud-Speicherpool"

Vergleichen Sie Cloud Storage Pools und CloudMirror-Replikation

Wenn Sie mit der Verwendung von Cloud Storage Pools beginnen, kann es hilfreich sein, die Ähnlichkeiten und Unterschiede zwischen Cloud Storage Pools und dem

StorageGRID CloudMirror-Replikationsdienst zu verstehen.

	Cloud-Speicherpool	CloudMirror-Replikationsdienst
Was ist der Hauptzweck?	Fungiert als Archivierungsziel. Die Objektkopie im Cloud Storage Pool kann die einzige Kopie des Objekts oder eine zusätzliche Kopie sein. Das heißt, anstatt zwei Kopien vor Ort aufzubewahren, können Sie eine Kopie in StorageGRID aufbewahren und eine Kopie an den Cloud Storage Pool senden.	Ermöglicht einem Mandanten, Objekte automatisch aus einem Bucket in StorageGRID (Quelle) in einen externen S3-Bucket (Ziel) zu replizieren. Erstellt eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur.
Wie ist es eingerichtet?	Auf die gleiche Weise wie Speicherpools definiert, mithilfe des Grid Managers oder der Grid Management API. Kann als Platzierungsort in einer ILM-Regel ausgewählt werden. Während ein Speicherpool aus einer Gruppe von Speicherknoten besteht, wird ein Cloud-Speicherpool mithilfe eines Remote-S3- oder Azure-Endpunkts (IP-Adresse, Anmeldeinformationen usw.) definiert.	Ein Mandantenbenutzer"konfiguriert die CloudMirror-Replikation" durch Definieren eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.) mithilfe des Tenant Managers oder der S3-API. Nachdem der CloudMirror-Endpunkt eingerichtet wurde, kann jeder Bucket, der diesem Mandantenkonto gehört, so konfiguriert werden, dass er auf den CloudMirror-Endpunkt verweist.
Wer ist für die Einrichtung verantwortlich?	Normalerweise ist ein Grid-Administrator	Normalerweise ist ein Mieterbenutzer
Was ist das Ziel?	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3) • Azure Blob Archive-Ebene • Google Cloud Platform (GCP)	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Eine oder mehrere ILM-Regeln in den aktiven ILM-Richtlinien. Die ILM-Regeln definieren, welche Objekte StorageGRID in den Cloud Storage Pool verschiebt und wann die Objekte verschoben werden.	Der Vorgang der Aufnahme eines neuen Objekts in einen Quell-Bucket, 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.

	Cloud-Speicherpool	CloudMirror-Replikationsdienst
Wie werden Objekte abgerufen?	Anwendungen müssen Anfragen an StorageGRID stellen, um Objekte abzurufen, die in einen Cloud-Speicherpool verschoben wurden. Wenn die einzige Kopie eines Objekts in den Archivspeicher übertragen wurde, verwaltet StorageGRID den Wiederherstellungsprozess des Objekts, sodass es abgerufen werden kann.	Da es sich bei der gespiegelten Kopie im Ziel-Bucket um eine unabhängige Kopie handelt, können Anwendungen das Objekt abrufen, indem sie Anfragen 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.
Können Sie direkt vom Ziel lesen?	Nein. In einen Cloud-Speicherpool verschobene Objekte werden von StorageGRID verwaltet. Leseanforderungen müssen an StorageGRID gerichtet werden (und StorageGRID ist für den Abruf aus dem Cloud Storage Pool verantwortlich).	Ja, da es sich bei der gespiegelten Kopie um eine unabhängige Kopie handelt.
Was passiert, wenn ein Objekt aus der Quelle gelöscht wird?	Das Objekt wird auch aus dem Cloud-Speicherpool gelöscht.	Die Löschaktion wird nicht repliziert. Ein gelöschtes Objekt ist im StorageGRID Bucket nicht mehr vorhanden, im Ziel-Bucket jedoch weiterhin. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass dies Auswirkungen auf die Quelle hat.
Wie greifen Sie nach einem Desaster (StorageGRID-System nicht betriebsbereit) auf Objekte zu?	Ausgefallene StorageGRID Knoten müssen wiederhergestellt werden. Während dieses Vorgangs können Kopien replizierter Objekte mithilfe der Kopien im Cloud-Speicherpool wiederhergestellt werden.	Die Objektkopien im CloudMirror-Ziel sind unabhängig von StorageGRID, sodass auf sie direkt zugegriffen werden kann, bevor die StorageGRID Knoten wiederhergestellt werden.

Erstellen Sie einen Cloud-Speicherpool

Ein Cloud-Speicherpool gibt einen einzelnen externen Amazon S3-Bucket oder einen anderen S3-kompatiblen Anbieter oder einen Azure Blob-Speichercontainer an.

Wenn Sie einen Cloud-Speicherpool erstellen, geben Sie den Namen und den Speicherort des externen Buckets oder Containers an, den StorageGRID zum Speichern von Objekten verwenden soll, den Cloud-Anbietertyp (Amazon S3/GCP oder Azure Blob Storage) und die Informationen, die StorageGRID für den Zugriff auf den externen Bucket oder Container benötigt.

StorageGRID validiert den Cloud Storage Pool, sobald Sie ihn speichern. Sie müssen daher sicherstellen, dass der im Cloud Storage Pool angegebene Bucket oder Container vorhanden und erreichbar ist.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .
- Sie haben die"Überlegungen zu Cloud-Speicherpools" .
- Der externe Bucket oder Container, auf den der Cloud Storage Pool verweist, ist bereits vorhanden und Sie haben dieInformationen zum Dienstendpunkt .
- Um auf den Eimer oder Behälter zuzugreifen, haben Sie dieKontoinformationen für den Authentifizierungstyp du wirst wählen.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Wählen Sie **Erstellen** und geben Sie dann die folgenden Informationen ein:

Feld	Beschreibung
Name des Cloud-Speicherpools	Ein Name, der den Cloud-Speicherpool und seinen Zweck kurz beschreibt. Verwenden Sie einen Namen, der beim Konfigurieren von ILM-Regeln leicht zu identifizieren ist.
Anbietertyp	Welchen Cloud-Anbieter verwenden Sie für diesen Cloud-Speicherpool: • **Amazon S3/GCP**: Wählen Sie diese Option für einen Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) oder einen anderen S3-kompatiblen Anbieter. • **Azure Blob-Speicher**
Eimer oder Behälter	Der Name des externen S3-Buckets oder Azure-Containers. Sie können diesen Wert nicht mehr ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

3. Geben Sie basierend auf Ihrem ausgewählten Providertyp die Service-Endpunktinformationen ein.

Amazon S3/GCP

a. Wählen Sie als Protokoll entweder HTTPS oder HTTP aus.

> Verwenden Sie keine HTTP-Verbindungen für vertrauliche Daten.

b. Geben Sie den Hostnamen ein. Beispiel:

`s3-aws-region.amazonaws.com`

c. Wählen Sie den URL-Stil aus:

Option	Beschreibung
Automatische Erkennung	Versuchen Sie, anhand der bereitgestellten Informationen automatisch zu erkennen, welcher URL-Stil verwendet werden soll. Wenn Sie beispielsweise eine IP-Adresse angeben, verwendet StorageGRID eine URL im Pfadstil. Wählen Sie diese Option nur, wenn Sie nicht wissen, welchen bestimmten Stil Sie verwenden sollen.
Virtuell gehosteter Stil	Verwenden Sie eine URL im virtuell gehosteten Stil, um auf den Bucket zuzugreifen. URLs im virtuell gehosteten Stil enthalten den Bucket-Namen als Teil des Domänennamens. Beispiel: `https://bucket-name.s3.company.com/key-name`
Pfad-Stil	Verwenden Sie eine URL im Pfadstil, um auf den Bucket zuzugreifen. URLs im Pfadstil enthalten am Ende den Bucket-Namen. Beispiel: `https://s3.company.com/bucket-name/key-name` **Hinweis:** Die URL-Option im Pfadstil wird nicht empfohlen und wird in einer zukünftigen Version von StorageGRID veraltet sein.

d. Geben Sie optional die Portnummer ein oder verwenden Sie den Standardport: 443 für HTTPS oder 80 für HTTP.

Azure Blob Storage

a. Geben Sie die URI für den Service-Endpunkt in einem der folgenden Formate ein.

- `https://host:port`
- `http://host:port`

Beispiel: `https://myaccount.blob.core.windows.net:443`

Wenn Sie keinen Port angeben, wird standardmäßig Port 443 für HTTPS und Port 80 für HTTP verwendet.

4. Wählen Sie **Weiter**. Wählen Sie dann den Authentifizierungstyp aus und geben Sie die erforderlichen Informationen für den Cloud Storage Pool-Endpunkt ein:

Zugriffsschlüssel

Für Amazon S3/GCP oder andere S3-kompatible Anbieter

a. **Zugriffsschlüssel-ID**: Geben Sie die Zugriffsschlüssel-ID für das Konto ein, dem der externe Bucket gehört.

b. **Geheimer Zugriffsschlüssel**: Geben Sie den geheimen Zugriffsschlüssel ein.

IAM-Rollen überall

Für den AWS IAM Roles Anywhere-Dienst

StorageGRID verwendet den AWS Security Token Service (STS), um dynamisch ein kurzlebiges Token für den Zugriff auf AWS-Ressourcen zu generieren.

a. **AWS IAM Roles Anywhere-Region**: Wählen Sie die Region für den Cloud-Speicherpool aus. Beispiel: `us-east-1` .

b. **Trust Anchor URN**: Geben Sie die URN des Trust Anchor ein, der Anfragen für kurzlebige STS-Anmeldeinformationen validiert. Kann eine Stamm- oder Zwischenzertifizierungsstelle sein.

c. **Profil-URN**: Geben Sie die URN des IAM Roles Anywhere-Profils ein, das die Rollen auflistet, die für jede vertrauenswürdige Person übernommen werden können.

d. **Rollen-URN**: Geben Sie die URN der IAM-Rolle ein, die für jeden vertrauenswürdigen Benutzer übernommen werden kann.

e. **Sitzungsdauer**: Geben Sie die Dauer der temporären Sicherheitsanmeldeinformationen und der Rollensitzung ein. Geben Sie mindestens 15 Minuten und höchstens 12 Stunden ein.

f. **Server-CA-Zertifikat** (optional): Ein oder mehrere vertrauenswürdige CA-Zertifikate im PEM-Format zur Überprüfung des IAM Roles Anywhere-Servers. Wenn es weggelassen wird, wird der Server nicht überprüft.

g. **Endentitätszertifikat**: Der öffentliche Schlüssel im PEM-Format des vom Vertrauensanker signierten X509-Zertifikats. AWS IAM Roles Anywhere verwendet diesen Schlüssel, um ein STS-Token auszustellen.

h. **Privater End-Entity-Schlüssel**: Der private Schlüssel für das End-Entity-Zertifikat.

CAP (C2S-Zugangsportal)

Für Commercial Cloud Services (C2S) S3-Dienst

a. **URL für temporäre Anmeldeinformationen**: Geben Sie die vollständige URL ein, die StorageGRID verwendet, um temporäre Anmeldeinformationen vom CAP-Server abzurufen, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.

b. **Server-CA-Zertifikat**: Wählen Sie **Durchsuchen** und laden Sie das CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwenden wird. Das Zertifikat muss PEM-kodiert und von einer entsprechenden staatlichen Zertifizierungsstelle (CA) ausgestellt sein.

c. **Client-Zertifikat**: Wählen Sie **Durchsuchen** und laden Sie das Zertifikat hoch, mit dem StorageGRID sich beim CAP-Server identifiziert. Das Client-Zertifikat muss PEM-codiert sein, von einer entsprechenden staatlichen Zertifizierungsstelle (CA) ausgestellt worden sein und Zugriff auf Ihr C2S-Konto haben.

d. **Privater Schlüssel des Clients**: Wählen Sie **Durchsuchen** und laden Sie den PEM-codierten privaten Schlüssel für das Client-Zertifikat hoch.

e. Wenn der private Schlüssel des Clients verschlüsselt ist, geben Sie die Passphrase zum Entschlüsseln des privaten Schlüssels des Clients ein. Andernfalls lassen Sie das Feld **Passphrase für den privaten Clientschlüssel** leer.

> Wenn das Client-Zertifikat verschlüsselt wird, verwenden Sie das herkömmliche Format für die Verschlüsselung. Das verschlüsselte PKCS #8-Format wird nicht unterstützt.

Azure Blob Storage

Für Azure Blob Storage, nur gemeinsam genutzter Schlüssel

a. **Kontoname**: Geben Sie den Namen des Speicherkontos ein, dem der externe Container gehört

b. **Kontoschlüssel**: Geben Sie den geheimen Schlüssel für das Speicherkonto ein

Sie können diese Werte über das Azure-Portal ermitteln.

Anonym

Es sind keine weiteren Angaben erforderlich.

5. Wählen Sie **Weiter**. Wählen Sie dann die Art der Serverüberprüfung aus, die Sie verwenden möchten:

Option	Beschreibung
Verwenden Sie Stamm-CA-Zertifikate im Storage Node OS	Verwenden Sie die auf dem Betriebssystem installierten Grid CA-Zertifikate, um Verbindungen zu sichern.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Wählen Sie **Durchsuchen** und laden Sie das PEM-codierte Zertifikat hoch.
Zertifikat nicht überprüfen	Wenn Sie diese Option auswählen, sind TLS-Verbindungen zum Cloud-Speicherpool nicht sicher.

6. Wählen Sie **Speichern**.

   Wenn Sie einen Cloud-Speicherpool speichern, führt StorageGRID Folgendes aus:

   - Überprüft, ob der Bucket oder Container und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Anmeldeinformationen erreicht werden können.
   - Schreibt eine Markierungsdatei in den Bucket oder Container, um ihn als Cloud-Speicherpool zu identifizieren. Entfernen Sie niemals diese Datei mit dem Namen `x-ntap-sgws-cloud-pool-uuid`.

     Wenn die Validierung des Cloud Storage Pools fehlschlägt, erhalten Sie eine Fehlermeldung mit der Erklärung, warum die Validierung fehlgeschlagen ist. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatsfehler vorliegt oder wenn der von Ihnen angegebene Bucket oder Container noch nicht vorhanden ist.

7. Wenn ein Fehler auftritt, lesen Sie die"Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools" , beheben Sie alle Probleme und versuchen Sie dann erneut, den Cloud-Speicherpool zu speichern.

Details zum Cloud-Speicherpool anzeigen

Sie können die Details eines Cloud-Speicherpools anzeigen, um festzustellen, wo er verwendet wird und welche Knoten und Speicherklassen enthalten sind.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.

   Die Tabelle „Cloud Storage Pools“ enthält die folgenden Informationen für jeden Cloud Storage Pool, der Speicherknoten enthält:

   - **Name**: Der eindeutige Anzeigename des Pools.
   - **URI**: Der Uniform Resource Identifier des Cloud Storage Pools.
   - **Anbietertyp**: Welcher Cloud-Anbieter wird für diesen Cloud-Speicherpool verwendet.
   - **Container**: Der Name des Buckets, der für den Cloud Storage Pool verwendet wird.
   - **ILM-Nutzung**: Wie der Pool derzeit genutzt wird. Ein Cloud-Speicherpool wird möglicherweise nicht verwendet oder in einer oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beidem verwendet.
   - **Letzter Fehler**: Der letzte Fehler, der während einer Integritätsprüfung dieses Cloud-Speicherpools erkannt wurde.

2. Um Details zu einem bestimmten Cloud-Speicherpool anzuzeigen, wählen Sie seinen Namen aus.

   Die Detailseite für den Pool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Authentifizierung** an, um mehr über den Authentifizierungstyp für diesen Cloud-Speicherpool zu erfahren und die Authentifizierungsdetails zu bearbeiten.
4. Sehen Sie sich die Registerkarte **Serverüberprüfung** an, um mehr über die Überprüfungsdetails zu erfahren, die Überprüfung zu bearbeiten, ein neues Zertifikat herunterzuladen oder das Zertifikat PEM zu kopieren.
5. Sehen Sie sich die Registerkarte **ILM-Nutzung** an, um festzustellen, ob der Cloud-Speicherpool derzeit in ILM-Regeln oder Erasure-Coding-Profilen verwendet wird.
6. Optional können Sie auf die **ILM-Regelseite** gehen, um"Informieren Sie sich über alle Regeln und verwalten Sie diese." die den Cloud-Speicherpool verwenden.

Bearbeiten eines Cloud-Speicherpools

Sie können einen Cloud-Speicherpool bearbeiten, um seinen Namen, den Dienstendpunkt oder andere Details zu ändern. Sie können jedoch den S3-Bucket oder Azure-Container für einen Cloud-Speicherpool nicht ändern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die"Überlegungen zu Cloud-Speicherpools" .

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.

   In der Tabelle „Cloud Storage Pools“ sind die vorhandenen Cloud Storage Pools aufgeführt.

2. Aktivieren Sie das Kontrollkästchen für den Cloud-Speicherpool, den Sie bearbeiten möchten, und wählen Sie dann **Aktionen** > **Bearbeiten**.

   Alternativ können Sie den Namen des Cloud-Speicherpools und dann **Bearbeiten** auswählen.

3. Ändern Sie nach Bedarf den Namen des Cloud-Speicherpools, den Dienstendpunkt, die Authentifizierungsdaten oder die Methode zur Zertifikatsüberprüfung.

   > Sie können den Anbietertyp oder den S3-Bucket oder Azure-Container für einen Cloud-Speicherpool nicht ändern.

   Wenn Sie zuvor ein Server- oder Client-Zertifikat hochgeladen haben, können Sie das Akkordeon **Zertifikatdetails** erweitern, um das aktuell verwendete Zertifikat zu überprüfen.

4. Wählen Sie **Speichern**.

   Wenn Sie einen Cloud Storage Pool speichern, überprüft StorageGRID , ob der Bucket oder Container und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Anmeldeinformationen erreicht werden können.

   Wenn die Validierung des Cloud Storage Pools fehlschlägt, wird eine Fehlermeldung angezeigt. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatsfehler vorliegt.

   Siehe die Anweisungen für"Fehlerbehebung bei Cloud-Speicherpools" , beheben Sie das Problem und versuchen Sie dann erneut, den Cloud-Speicherpool zu speichern.

Entfernen eines Cloud-Speicherpools

Sie können einen Cloud-Speicherpool entfernen, wenn er nicht in einer ILM-Regel verwendet wird und keine Objektdaten enthält.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Verwenden Sie bei Bedarf ILM, um Objektdaten zu verschieben

Wenn der Cloud-Speicherpool, den Sie entfernen möchten, Objektdaten enthält, müssen Sie ILM verwenden, um die Daten an einen anderen Speicherort zu verschieben. Sie können die Daten beispielsweise auf Speicherknoten in Ihrem Grid oder in einen anderen Cloud-Speicherpool verschieben.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Sehen Sie sich die Spalte „ILM-Nutzung“ in der Tabelle an, um festzustellen, ob Sie den Cloud-Speicherpool entfernen können.

   Sie können einen Cloud-Speicherpool nicht entfernen, wenn er in einer ILM-Regel oder in einem Erasure-

Coding-Profil verwendet wird.

3. Wenn der Cloud-Speicherpool verwendet wird, wählen Sie ***Name des Cloud-Speicherpools*** > **ILM-Nutzung**.
4. "Klonen Sie jede ILM-Regel"das derzeit Objekte im Cloud-Speicherpool platziert, die Sie entfernen möchten.
5. Bestimmen Sie, wohin Sie die vorhandenen Objekte verschieben möchten, die von jeder geklonten Regel verwaltet werden.

   Sie können einen oder mehrere Speicherpools oder einen anderen Cloud-Speicherpool verwenden.

6. Bearbeiten Sie jede der geklonten Regeln.

   Wählen Sie in Schritt 2 des Assistenten zum Erstellen einer ILM-Regel den neuen Speicherort aus dem Feld **Kopien in** aus.

7. "Erstellen einer neuen ILM-Richtlinie"und ersetzen Sie jede der alten Regeln durch eine geklonte Regel.
8. Aktivieren Sie die neue Richtlinie.
9. Warten Sie, bis ILM Objekte aus dem Cloud-Speicherpool entfernt und am neuen Speicherort abgelegt hat.

Cloud-Speicherpool löschen

Wenn der Cloud-Speicherpool leer ist und in keinen ILM-Regeln verwendet wird, können Sie ihn löschen.

Bevor Sie beginnen

- Sie haben alle ILM-Regeln entfernt, die den Pool möglicherweise verwendet haben.
- Sie haben bestätigt, dass der S3-Bucket oder Azure-Container keine Objekte enthält.

  Wenn Sie versuchen, einen Cloud-Speicherpool zu entfernen, der Objekte enthält, tritt ein Fehler auf. Sehen "Fehlerbehebung bei Cloud-Speicherpools" .

> ⓘ Wenn Sie einen Cloud-Speicherpool erstellen, schreibt StorageGRID eine Markierungsdatei in den Bucket oder Container, um ihn als Cloud-Speicherpool zu identifizieren. Entfernen Sie diese Datei nicht. Sie trägt den Namen `x-ntap-sgws-cloud-pool-uuid`.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Wenn in der Spalte „ILM-Nutzung“ angegeben ist, dass der Cloud-Speicherpool nicht verwendet wird, aktivieren Sie das Kontrollkästchen.
3. Wählen Sie **Aktionen** > **Entfernen**.
4. Wählen Sie **OK**.

Fehlerbehebung bei Cloud-Speicherpools

Verwenden Sie diese Schritte zur Fehlerbehebung, um Fehler zu beheben, die beim Erstellen, Bearbeiten oder Löschen eines Cloud-Speicherpools auftreten können.

Feststellen, ob ein Fehler aufgetreten ist

StorageGRID führt einen einfachen Integritätscheck für jeden Cloud Storage Pool durch, indem es das bekannte Objekt liest `x-ntap-sgws-cloud-pool-uuid` um sicherzustellen, dass auf den Cloud Storage Pool zugegriffen werden kann und dieser ordnungsgemäß funktioniert. Wenn StorageGRID auf einen Fehler am Endpunkt stößt, führt es jede Minute eine Integritätsprüfung von jedem Speicherknoten aus durch. Wenn der Fehler behoben ist, werden die Integritätsprüfungen beendet. Wenn bei einer Integritätsprüfung ein Problem erkannt wird, wird in der Spalte „Letzter Fehler“ der Tabelle „Cloud-Speicherpools“ auf der Seite „Speicherpools“ eine Meldung angezeigt.

Die Tabelle zeigt den zuletzt erkannten Fehler für jeden Cloud-Speicherpool und gibt an, wie lange der Fehler her ist.

Darüber hinaus wird eine Warnung **Verbindungsfehler im Cloud Storage Pool** ausgelöst, wenn die Integritätsprüfung erkennt, dass innerhalb der letzten 5 Minuten ein oder mehrere neue Fehler im Cloud Storage Pool aufgetreten sind. Wenn Sie eine E-Mail-Benachrichtigung zu dieser Warnung erhalten, gehen Sie zur Seite „Speicherpools“ (wählen Sie **ILM** > **Speicherpools**), überprüfen Sie die Fehlermeldungen in der Spalte „Letzter Fehler“ und beachten Sie die nachstehenden Richtlinien zur Fehlerbehebung.

Überprüfen Sie, ob ein Fehler behoben wurde

Nachdem Sie alle zugrunde liegenden Probleme behoben haben, können Sie feststellen, ob der Fehler behoben wurde. Wählen Sie auf der Seite „Cloud-Speicherpool“ den Endpunkt aus und wählen Sie „Fehler löschen“ aus. Eine Bestätigungsmeldung zeigt an, dass StorageGRID den Fehler für den Cloud Storage Pool behoben hat.

Wenn das zugrunde liegende Problem behoben wurde, wird die Fehlermeldung nicht mehr angezeigt. Wenn das zugrunde liegende Problem jedoch nicht behoben wurde (oder ein anderer Fehler auftritt), wird die Fehlermeldung innerhalb weniger Minuten in der Spalte „Letzter Fehler“ angezeigt.

Fehler: Integritätsprüfung fehlgeschlagen. Fehler vom Endpunkt

Dieser Fehler kann auftreten, wenn Sie S3 Object Lock mit Standardaufbewahrung für Ihren Amazon S3-Bucket aktivieren, nachdem Sie diesen Bucket für einen Cloud Storage Pool verwenden. Dieser Fehler tritt auf, wenn der PUT-Vorgang keinen HTTP-Header mit einem Nutzlast-Prüfsummenwert wie `Content-MD5` . Dieser Header-Wert wird von AWS für PUT-Operationen in Buckets mit aktivierter S3-Objektsperre benötigt.

Um dieses Problem zu beheben, befolgen Sie die Schritte in"Bearbeiten eines Cloud-Speicherpools" ohne Änderungen vorzunehmen. Diese Aktion löst die Validierung der Cloud Storage Pool-Konfiguration aus, die das S3 Object Lock-Flag in einer Cloud Storage Pool-Endpunktkonfiguration automatisch erkennt und aktualisiert.

Fehler: Dieser Cloud-Speicherpool enthält unerwartete Inhalte

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen, zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Bucket oder Container Folgendes enthält: `x-ntap-sgws-cloud-pool-uuid` Markerdatei, aber diese Datei verfügt nicht über das Metadatenfeld mit der erwarteten UUID.

Normalerweise wird dieser Fehler nur angezeigt, wenn Sie einen neuen Cloud-Speicherpool erstellen und eine andere Instanz von StorageGRID bereits denselben Cloud-Speicherpool verwendet.

Versuchen Sie, das Problem mit einem der folgenden Schritte zu beheben:

- Wenn Sie einen neuen Cloud Storage Pool konfigurieren und der Bucket die `x-ntap-sgws-cloud-`

`pool-uuid` Datei und zusätzliche Objektschlüssel ähnlich dem folgenden Beispiel, erstellen Sie einen neuen Bucket und verwenden Sie stattdessen diesen neuen Bucket.

Beispiel für einen zusätzlichen Objektschlüssel: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Wenn die `x-ntap-sgws-cloud-pool-uuid` Datei das einzige Objekt im Bucket ist, löschen Sie diese Datei.

Wenn diese Schritte nicht auf Ihr Szenario zutreffen, wenden Sie sich an den Support.

Fehler: Cloud-Speicherpool konnte nicht erstellt oder aktualisiert werden. Fehler vom Endpunkt

Dieser Fehler kann unter den folgenden Umständen auftreten:

- Wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten.
- Wenn Sie während der Konfiguration eines neuen Cloud-Speicherpools eine nicht unterstützte Plattform-, Authentifizierungs- oder Protokollkombination mit S3 Object Lock auswählen. Sehen "Überlegungen zu Cloud-Speicherpools" .

Dieser Fehler weist darauf hin, dass ein Verbindungs- oder Konfigurationsproblem StorageGRID daran hindert, in den Cloud-Speicherpool zu schreiben.

Um das Problem zu beheben, überprüfen Sie die Fehlermeldung vom Endpunkt.

- Wenn die Fehlermeldung enthält `Get *url*: EOF` , überprüfen Sie, dass der für den Cloud Storage Pool verwendete Dienstendpunkt kein HTTP für einen Container oder Bucket verwendet, der HTTPS erfordert.
- Wenn die Fehlermeldung enthält `Get *url*: net/http: request canceled while waiting for connection` , überprüfen Sie, ob die Netzwerkkonfiguration Speicherknoten den Zugriff auf den für den Cloud-Speicherpool verwendeten Dienstendpunkt ermöglicht.
- Wenn der Fehler auf eine nicht unterstützte Plattform, Authentifizierung oder ein nicht unterstütztes Protokoll zurückzuführen ist, wechseln Sie zu einer unterstützten Konfiguration mit S3 Object Lock und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.
- Versuchen Sie bei allen anderen Endpunkt-Fehlermeldungen eine oder mehrere der folgenden Methoden:
  - Erstellen Sie einen externen Container oder Bucket mit demselben Namen, den Sie für den Cloud Storage Pool eingegeben haben, und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.
  - Korrigieren Sie den Container- oder Bucket-Namen, den Sie für den Cloud Storage Pool angegeben haben, und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.

Fehler: Das CA-Zertifikat konnte nicht analysiert werden.

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Der Fehler tritt auf, wenn StorageGRID das Zertifikat, das Sie beim Konfigurieren des Cloud Storage Pools eingegeben haben, nicht analysieren konnte.

Um das Problem zu beheben, überprüfen Sie das von Ihnen bereitgestellte CA-Zertifikat auf Probleme.

Fehler: Ein Cloud-Speicherpool mit dieser ID wurde nicht gefunden

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Endpunkt eine 404-Antwort zurückgibt, was Folgendes bedeuten kann:

- Die für den Cloud Storage Pool verwendeten Anmeldeinformationen verfügen nicht über die Leseberechtigung für den Bucket.
- Der für den Cloud Storage Pool verwendete Bucket enthält nicht die `x-ntap-sgws-cloud-pool-uuid` Markierungsdatei.

Versuchen Sie einen oder mehrere dieser Schritte, um das Problem zu beheben:

- Überprüfen Sie, ob der mit dem konfigurierten Zugriffsschlüssel verknüpfte Benutzer über die erforderlichen Berechtigungen verfügt.
- Bearbeiten Sie den Cloud-Speicherpool mit Anmeldeinformationen, die über die erforderlichen Berechtigungen verfügen.
- Wenn die Berechtigungen korrekt sind, wenden Sie sich an den Support.

Fehler: Der Inhalt des Cloud-Speicherpools konnte nicht überprüft werden. Fehler vom Endpunkt

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Dieser Fehler weist darauf hin, dass ein Verbindungs- oder Konfigurationsproblem StorageGRID daran hindert, den Inhalt des Cloud Storage Pool-Buckets zu lesen.

Um das Problem zu beheben, überprüfen Sie die Fehlermeldung vom Endpunkt.

Fehler: In diesem Bucket wurden bereits Objekte platziert

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Sie können einen Cloud-Speicherpool nicht löschen, wenn er Daten enthält, die von ILM dorthin verschoben wurden, Daten, die sich im Bucket befanden, bevor Sie den Cloud-Speicherpool konfiguriert haben, oder Daten, die nach der Erstellung des Cloud-Speicherpools von einer anderen Quelle in den Bucket gelegt wurden.

Versuchen Sie einen oder mehrere dieser Schritte, um das Problem zu beheben:

- Befolgen Sie die Anweisungen zum Zurückverschieben von Objekten zu StorageGRID unter „Lebenszyklus eines Cloud Storage Pool-Objekts“.
- Wenn Sie sicher sind, dass die verbleibenden Objekte nicht von ILM im Cloud Storage Pool abgelegt wurden, löschen Sie die Objekte manuell aus dem Bucket.

> ⓘ Löschen Sie niemals manuell Objekte aus einem Cloud-Speicherpool, die möglicherweise von ILM dort abgelegt wurden. Wenn Sie später versuchen, auf ein manuell gelöschtes Objekt aus StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Fehler: Beim Versuch, den Cloud-Speicherpool zu erreichen, ist beim Proxy ein externer Fehler aufgetreten

Dieser Fehler kann auftreten, wenn Sie einen nicht transparenten Speicherproxy zwischen Speicherknoten und dem für den Cloud-Speicherpool verwendeten externen S3-Endpunkt konfiguriert haben. Dieser Fehler tritt auf, wenn der externe Proxyserver den Endpunkt des Cloud Storage Pools nicht erreichen kann. Beispielsweise kann der DNS-Server den Hostnamen möglicherweise nicht auflösen oder es liegt ein externes Netzwerkproblem vor.

Versuchen Sie einen oder mehrere dieser Schritte, um das Problem zu beheben:

- Überprüfen Sie die Einstellungen für den Cloud-Speicherpool (**ILM** > **Speicherpools**).
- Überprüfen Sie die Netzwerkkonfiguration des Speicherproxyservers.

Fehler: Das X.509-Zertifikat hat seine Gültigkeitsdauer überschritten

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Dieser Fehler tritt auf, wenn für die Authentifizierung ein X.509-Zertifikat erforderlich ist, um sicherzustellen, dass der richtige externe Cloud Storage Pool validiert wird und der externe Pool leer ist, bevor die Cloud Storage Pool-Konfiguration gelöscht wird.

Versuchen Sie, das Problem mit den folgenden Schritten zu beheben:

- Aktualisieren Sie das für die Authentifizierung beim Cloud-Speicherpool konfigurierte Zertifikat.
- Stellen Sie sicher, dass alle Warnungen zum Ablauf des Zertifikats in diesem Cloud-Speicherpool behoben werden.

Ähnliche Informationen

"Lebenszyklus eines Cloud Storage Pool-Objekts"

Verwalten von Erasure-Coding-Profilen

Sie können die Details eines Erasure-Coding-Profils anzeigen und ein Profil bei Bedarf umbenennen. Sie können ein Erasure-Coding-Profil deaktivieren, wenn es derzeit in keinen ILM-Regeln verwendet wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Details zum Erasure-Coding-Profil anzeigen

Sie können die Details eines Erasure-Coding-Profils anzeigen, um dessen Status, das verwendete Erasure-Coding-Schema und andere Informationen zu ermitteln.

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Erasure Coding**.
2. Wählen Sie das Profil aus. Die Detailseite für das Profil wird angezeigt.
3. Optional können Sie auf der Registerkarte „ILM-Regeln“ eine Liste der ILM-Regeln anzeigen, die das Profil verwenden, sowie die ILM-Richtlinien, die diese Regeln verwenden.
4. Optional können Sie auf der Registerkarte „Speicherknoten“ Details zu jedem Speicherknoten im Speicherpool des Profils anzeigen, z. B. den Standort und die Speichernutzung.

Umbenennen eines Erasure-Coding-Profils

Möglicherweise möchten Sie ein Erasure-Coding-Profil umbenennen, um deutlicher zu machen, was das Profil macht.

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Erasure Coding**.
2. Wählen Sie das Profil aus, das Sie umbenennen möchten.
3. Wählen Sie **Umbenennen**.
4. Geben Sie einen eindeutigen Namen für das Erasure-Coding-Profil ein.

Der Name des Erasure-Coding-Profils wird in der Platzierungsanweisung für eine ILM-Regel an den Speicherpoolnamen angehängt.

> Die Namen der Erasure-Coding-Profile müssen eindeutig sein. Wenn Sie den Namen eines vorhandenen Profils verwenden, tritt ein Validierungsfehler auf, auch wenn dieses Profil deaktiviert wurde.

5. Wählen Sie **Speichern**.

Deaktivieren eines Erasure-Coding-Profils

Sie können ein Erasure-Coding-Profil deaktivieren, wenn Sie es nicht mehr verwenden möchten und das Profil derzeit in keinen ILM-Regeln verwendet wird.

> Stellen Sie sicher, dass keine Vorgänge zur Reparatur von Erasure-Code-Daten oder Außerbetriebnahmen im Gange sind. Wenn Sie versuchen, ein Erasure-Coding-Profil zu deaktivieren, während einer dieser Vorgänge ausgeführt wird, wird eine Fehlermeldung zurückgegeben.

Informationen zu diesem Vorgang

StorageGRID verhindert, dass Sie ein Erasure-Coding-Profil deaktivieren, wenn einer der folgenden Punkte zutrifft:

- Das Erasure-Coding-Profil wird derzeit in einer ILM-Regel verwendet.
- Das Erasure-Coding-Profil wird in keinen ILM-Regeln mehr verwendet, Objektdaten und Paritätsfragmente für das Profil sind jedoch weiterhin vorhanden.

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Erasure Coding**.
2. Überprüfen Sie auf der Registerkarte „Aktiv“ die Spalte **Status**, um sicherzustellen, dass das Erasure-Coding-Profil, das Sie deaktivieren möchten, in keinen ILM-Regeln verwendet wird.

   Sie können ein Erasure-Coding-Profil nicht deaktivieren, wenn es in einer ILM-Regel verwendet wird. Im Beispiel wird das Profil 2+1 Data Center 1 in mindestens einer ILM-Regel verwendet.

Profile name	Status	Storage pool	Erasure-coding scheme
2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
New profile	Deactivated	Data Center 1	2+1

3. Wenn das Profil in einer ILM-Regel verwendet wird, gehen Sie folgendermaßen vor:
   a. Wählen Sie **ILM** > **Regeln**.
   b. Wählen Sie jede Regel aus und überprüfen Sie das Aufbewahrungsdiagramm, um festzustellen, ob die Regel das Erasure-Coding-Profil verwendet, das Sie deaktivieren möchten.
   c. Wenn die ILM-Regel das Erasure-Coding-Profil verwendet, das Sie deaktivieren möchten, ermitteln Sie, ob die Regel in einer ILM-Richtlinie verwendet wird.
   d. Führen Sie die zusätzlichen Schritte in der Tabelle aus, je nachdem, wo das Erasure-Coding-Profil

verwendet wird.

Wo wurde das Profil verwendet?	Zusätzliche Schritte vor der Deaktivierung des Profils	Beachten Sie diese zusätzlichen Anweisungen
Wird nie in einer ILM-Regel verwendet	Keine weiteren Schritte erforderlich. Fahren Sie mit diesem Verfahren fort.	*Keiner*
In einer ILM-Regel, die noch nie in einer ILM-Richtlinie verwendet wurde	i. Bearbeiten oder löschen Sie alle betroffenen ILM-Regeln. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure-Coding-Profil verwenden. ii. Fahren Sie mit diesem Verfahren fort.	"Arbeiten mit ILM-Regeln und ILM-Richtlinien"
In einer ILM-Regel, die sich derzeit in einer aktiven ILM-Richtlinie befindet	i. Klonen Sie die Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Erasure-Coding-Profil verwendet. iii. Fügen Sie eine oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass Objekte geschützt sind. iv. Speichern, simulieren und aktivieren Sie die neue Richtlinie. v. Warten Sie, bis die neue Richtlinie angewendet wird und vorhandene Objekte basierend auf den von Ihnen hinzugefügten neuen Regeln an neue Speicherorte verschoben werden. **Hinweis:** Abhängig von der Anzahl der Objekte und der Größe Ihres StorageGRID -Systems kann es Wochen oder sogar Monate dauern, bis ILM-Vorgänge die Objekte basierend auf den neuen ILM-Regeln an neue Speicherorte verschieben. Sie können zwar gefahrlos versuchen, ein Erasure-Coding-Profil zu deaktivieren, solange es noch mit Daten verknüpft ist, der Deaktivierungsvorgang schlägt jedoch fehl. Eine Fehlermeldung informiert Sie, wenn das Profil noch nicht zur Deaktivierung bereit ist. vi. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure-Coding-Profil verwenden. vii. Fahren Sie mit diesem Verfahren fort.	"Erstellen einer ILM-Richtlinie" "Arbeiten mit ILM-Regeln und ILM-Richtlinien"

Wo wurde das Profil verwendet?	Zusätzliche Schritte vor der Deaktivierung des Profils	Beachten Sie diese zusätzlichen Anweisungen
In einer ILM-Regel, die sich derzeit in einer ILM-Richtlinie befindet	i. Bearbeiten Sie die Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Erasure-Coding-Profil verwendet. iii. Fügen Sie eine oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass alle Objekte geschützt sind. iv. Speichern Sie die Richtlinie. v. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure-Coding-Profil verwenden. vi. Fahren Sie mit diesem Verfahren fort.	"Erstellen einer ILM-Richtlinie" "Arbeiten mit ILM-Regeln und ILM-Richtlinien"

e. Aktualisieren Sie die Seite „Erasure-Coding-Profile“, um sicherzustellen, dass das Profil nicht in einer ILM-Regel verwendet wird.

4. Wenn das Profil nicht in einer ILM-Regel verwendet wird, aktivieren Sie das Optionsfeld und wählen Sie **Deaktivieren**. Das Dialogfeld „Erasure-Coding-Profil deaktivieren“ wird angezeigt.

> Sie können mehrere Profile gleichzeitig zur Deaktivierung auswählen, solange die einzelnen Profile nicht in einer Regel verwendet werden.

5. Wenn Sie sicher sind, dass Sie das Profil deaktivieren möchten, wählen Sie **Deaktivieren**.

Ergebnisse

- Wenn StorageGRID das Erasure-Coding-Profil deaktivieren kann, lautet sein Status „Deaktiviert“. Sie können dieses Profil nicht mehr für eine ILM-Regel auswählen. Sie können ein deaktiviertes Profil nicht reaktivieren.
- Wenn StorageGRID das Profil nicht deaktivieren kann, wird eine Fehlermeldung angezeigt. Beispielsweise erscheint eine Fehlermeldung, wenn noch Objektdaten mit diesem Profil verknüpft sind. Möglicherweise müssen Sie mehrere Wochen warten, bevor Sie den Deaktivierungsvorgang erneut versuchen.

Regionen konfigurieren (optional und nur S3)

ILM-Regeln können Objekte basierend auf den Regionen filtern, in denen S3-Buckets erstellt werden, sodass Sie Objekte aus verschiedenen Regionen an verschiedenen Speicherorten speichern können.

Wenn Sie eine S3-Bucket-Region als Filter in einer Regel verwenden möchten, müssen Sie zuerst die Regionen erstellen, die von den Buckets in Ihrem System verwendet werden können.

> Sie können die Region für einen Bucket nicht mehr ändern, nachdem der Bucket erstellt wurde.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Beim Erstellen eines S3-Buckets können Sie angeben, dass der Bucket in einer bestimmten Region erstellt werden soll. Durch die Angabe einer Region kann sich der Bucket geografisch in der Nähe seiner Benutzer befinden, wodurch die Latenz optimiert, die Kosten minimiert und gesetzliche Anforderungen erfüllt werden können.

Wenn Sie eine ILM-Regel erstellen, möchten Sie möglicherweise die mit einem S3-Bucket verknüpfte Region als erweiterten Filter verwenden. Sie können beispielsweise eine Regel entwerfen, die nur für Objekte in S3-Buckets gilt, die im `us-west-2` Region. Sie können dann angeben, dass Kopien dieser Objekte auf Speicherknoten an einem Rechenzentrumsstandort innerhalb dieser Region abgelegt werden, um die Latenz zu optimieren.

Befolgen Sie beim Konfigurieren von Regionen die folgenden Richtlinien:

- Standardmäßig werden alle Buckets als zugehörig betrachtet zum `us-east-1` Region.
- Sie müssen die Regionen mit dem Grid Manager erstellen, bevor Sie beim Erstellen von Buckets mit dem Tenant Manager oder der Tenant Management API oder mit dem LocationConstraint-Anforderungselement für S3 PUT Bucket API-Anforderungen eine nicht standardmäßige Region angeben können. Ein Fehler tritt auf, wenn eine PUT-Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.
- Sie müssen beim Erstellen des S3-Buckets den genauen Regionsnamen verwenden. Bei Regionsnamen wird zwischen Groß- und Kleinschreibung unterschieden. Gültige Zeichen sind Zahlen, Buchstaben und Bindestriche.

  EU wird nicht als Alias für eu-west-1 betrachtet. Wenn Sie die Region EU oder eu-west-1 verwenden möchten, müssen Sie den genauen Namen verwenden.

- Sie können eine Region nicht löschen oder ändern, wenn sie in einer Regel verwendet wird, die einer Richtlinie (aktiv oder inaktiv) zugewiesen ist.
- Wenn Sie eine ungültige Region als erweiterten Filter in einer ILM-Regel verwenden, können Sie diese Regel keiner Richtlinie hinzufügen.

  Eine ungültige Region kann entstehen, wenn Sie eine Region als erweiterten Filter in einer ILM-Regel verwenden, diese Region aber später löschen, oder wenn Sie die Grid Management-API zum Erstellen einer Regel verwenden und eine Region angeben, die Sie nicht definiert haben.

- Wenn Sie eine Region löschen, nachdem Sie sie zum Erstellen eines S3-Buckets verwendet haben, müssen Sie die Region erneut hinzufügen, wenn Sie jemals den erweiterten Filter „Standortbeschränkung“ verwenden möchten, um Objekte in diesem Bucket zu finden.

Schritte

1. Wählen Sie **ILM** > **Regionen**.

   Die Seite „Regionen“ wird mit einer Liste der aktuell definierten Regionen angezeigt. **Region 1** zeigt die Standardregion, `us-east-1` , die nicht geändert oder entfernt werden können.

2. So fügen Sie eine Region hinzu:
   a. Wählen Sie **Weitere Region hinzufügen**.

b. Geben Sie den Namen einer Region ein, die Sie beim Erstellen von S3-Buckets verwenden möchten.

   Sie müssen genau diesen Regionsnamen als LocationConstraint-Anforderungselement verwenden, wenn Sie den entsprechenden S3-Bucket erstellen.

3. Um eine nicht verwendete Region zu entfernen, wählen Sie das Löschsymbol ✕ .

   Wenn Sie versuchen, eine Region zu entfernen, die derzeit in einer Richtlinie (aktiv oder inaktiv) verwendet wird, wird eine Fehlermeldung angezeigt.

4. Wenn Sie mit den Änderungen fertig sind, wählen Sie **Speichern**.

   Sie können diese Regionen jetzt im Abschnitt „Erweiterte Filter“ in Schritt 1 des Assistenten „ILM-Regel erstellen“ auswählen. Sehen "Verwenden Sie erweiterte Filter in ILM-Regeln" .

ILM-Regel erstellen

Verwenden Sie ILM-Regeln zum Verwalten von Objekten

Zum Verwalten von Objekten erstellen Sie einen Satz von Regeln für das Information Lifecycle Management (ILM) und organisieren diese in einer ILM-Richtlinie.

Jedes in das System aufgenommene Objekt wird anhand der aktiven Richtlinie bewertet. Wenn eine Regel in der Richtlinie mit den Metadaten eines Objekts übereinstimmt, bestimmen die Anweisungen in der Regel, welche Aktionen StorageGRID zum Kopieren und Speichern dieses Objekts ausführt.

> ⓘ Objektmetadaten werden nicht durch ILM-Regeln verwaltet. Stattdessen werden Objektmetadaten in einer Cassandra-Datenbank in einem sogenannten Metadatenspeicher gespeichert. Um die Daten vor Verlust zu schützen, werden an jedem Standort automatisch drei Kopien der Objektmetadaten verwaltet.

Elemente einer ILM-Regel

Eine ILM-Regel besteht aus drei Elementen:

- **Filterkriterien**: Die grundlegenden und erweiterten Filter einer Regel definieren, auf welche Objekte die Regel angewendet wird. Wenn ein Objekt allen Filtern entspricht, wendet StorageGRID die Regel an und erstellt die in den Platzierungsanweisungen der Regel angegebenen Objektkopien.
- **Platzierungsanweisungen**: Die Platzierungsanweisungen einer Regel definieren die Anzahl, den Typ und den Speicherort von Objektkopien. Jede Regel kann eine Abfolge von Platzierungsanweisungen enthalten, um die Anzahl, den Typ und den Speicherort von Objektkopien im Laufe der Zeit zu ändern. Wenn der Zeitraum für eine Platzierung abläuft, werden die Anweisungen in der nächsten Platzierung automatisch von der nächsten ILM-Bewertung angewendet.
- **Aufnahmeverhalten**: Über das Aufnahmeverhalten einer Regel können Sie auswählen, wie die durch die Regel gefilterten Objekte bei der Aufnahme geschützt werden (wenn ein S3-Client ein Objekt im Raster speichert).

ILM-Regelfilterung

Wenn Sie eine ILM-Regel erstellen, geben Sie Filter an, um zu identifizieren, auf welche Objekte die Regel angewendet wird.

Im einfachsten Fall verwendet eine Regel möglicherweise keine Filter. Jede Regel, die keine Filter verwendet, gilt für alle Objekte und muss daher die letzte (Standard-)Regel in einer ILM-Richtlinie sein. Die Standardregel bietet Speicheranweisungen für Objekte, die nicht den Filtern einer anderen Regel entsprechen.

- Mithilfe von Basisfiltern können Sie unterschiedliche Regeln auf große, unterschiedliche Objektgruppen anwenden. Mit diesen Filtern können Sie eine Regel auf bestimmte Mandantenkonten, bestimmte S3-Buckets oder beides anwenden.

  Mithilfe von Basisfiltern können Sie auf einfache Weise unterschiedliche Regeln auf eine große Anzahl von Objekten anwenden. Beispielsweise müssen die Finanzunterlagen Ihres Unternehmens möglicherweise gespeichert werden, um gesetzliche Anforderungen zu erfüllen, während Daten der Marketingabteilung möglicherweise gespeichert werden müssen, um den täglichen Betrieb zu erleichtern. Nachdem Sie für jede Abteilung separate Mandantenkonten erstellt oder die Daten der verschiedenen Abteilungen in separate S3-Buckets aufgeteilt haben, können Sie ganz einfach eine Regel erstellen, die für alle Finanzunterlagen gilt, und eine zweite Regel, die für alle Marketingdaten gilt.

- Erweiterte Filter geben Ihnen eine detaillierte Kontrolle. Sie können Filter erstellen, um Objekte basierend auf den folgenden Objekteigenschaften auszuwählen:
  - Aufnahmezeit
  - Letzter Zugriffszeitpunkt
  - Der gesamte oder ein Teil des Objektnamens (Schlüssel)
  - Standortbeschränkung (nur S3)
  - Objektgröße
  - Benutzermetadaten
  - Objekt-Tag (nur S3)

Sie können Objekte nach ganz bestimmten Kriterien filtern. Beispielsweise werden Objekte, die in der Bildgebungsabteilung eines Krankenhauses gespeichert sind, möglicherweise häufig verwendet, wenn sie weniger als 30 Tage alt sind, und danach nur noch selten, während Objekte, die Informationen zu Patientenbesuchen enthalten, möglicherweise in die Abrechnungsabteilung in der Zentrale des Gesundheitsnetzwerks kopiert werden müssen. Sie können Filter erstellen, die jeden Objekttyp anhand des Objektnamens, der Größe, der S3-Objekt-Tags oder anderer relevanter Kriterien identifizieren, und dann separate Regeln erstellen, um jeden Objektsatz entsprechend zu speichern.

Sie können Filter nach Bedarf in einer einzigen Regel kombinieren. Beispielsweise möchte die Marketingabteilung große Bilddateien möglicherweise anders speichern als ihre Lieferantendatensätze, während die Personalabteilung Personaldatensätze in einer bestimmten Region und Richtlinieninformationen zentral speichern muss. In diesem Fall können Sie Regeln erstellen, die nach Mandantenkonto filtern, um die Datensätze aus jeder Abteilung zu trennen, während Sie in jeder Regel Filter verwenden, um den spezifischen Objekttyp zu identifizieren, auf den die Regel angewendet wird.

Anweisungen zur Platzierung von ILM-Regeln

Platzierungsanweisungen bestimmen, wo, wann und wie Objektdaten gespeichert werden. Eine ILM-Regel kann eine oder mehrere Platzierungsanweisungen enthalten. Jede Platzierungsanweisung gilt jeweils für einen Zeitraum.

Wenn Sie Platzierungsanweisungen erstellen:

- Sie beginnen mit der Angabe der Referenzzeit, die bestimmt, wann die Platzierungsanweisungen beginnen. Der Referenzzeitpunkt kann der Zeitpunkt der Aufnahme eines Objekts, der Zugriff auf ein Objekt, der Zeitpunkt, zu dem ein versioniertes Objekt nicht mehr aktuell ist, oder ein benutzerdefinierter

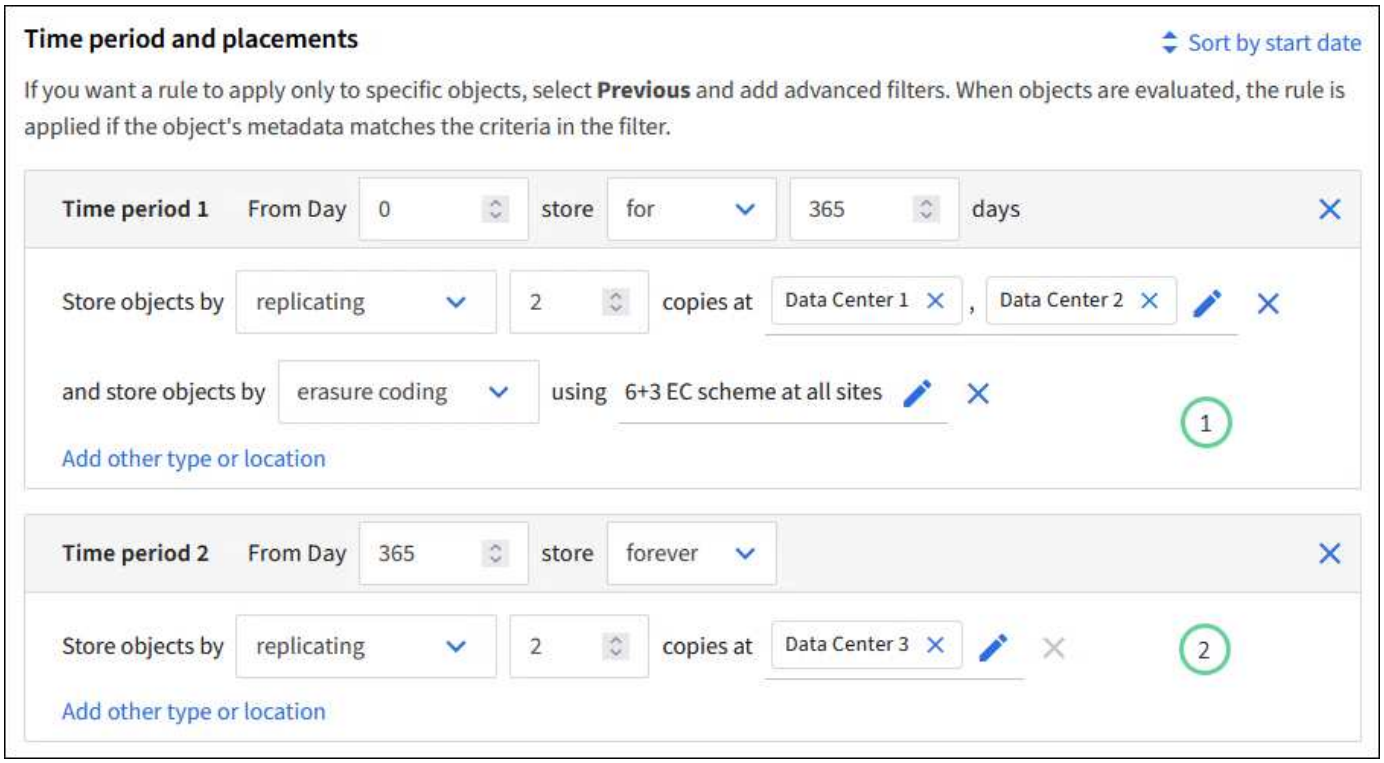
Zeitpunkt sein.

- Als Nächstes geben Sie an, wann die Platzierung relativ zur Referenzzeit angewendet wird. Beispielsweise kann eine Platzierung am Tag 0 beginnen und 365 Tage lang andauern, relativ zum Zeitpunkt der Aufnahme des Objekts.
- Abschließend geben Sie die Art der Kopien (Replikation oder Erasure Coding) und den Speicherort der Kopien an. Beispielsweise möchten Sie möglicherweise zwei replizierte Kopien an zwei verschiedenen Standorten speichern.

Jede Regel kann mehrere Platzierungen für einen einzelnen Zeitraum und unterschiedliche Platzierungen für unterschiedliche Zeiträume definieren.

- Um Objekte während eines einzelnen Zeitraums an mehreren Standorten zu platzieren, wählen Sie **Anderen Typ oder Standort hinzufügen** aus, um für diesen Zeitraum mehr als eine Zeile hinzuzufügen.
- Um Objekte an verschiedenen Orten in unterschiedlichen Zeiträumen zu platzieren, wählen Sie **Weiteren Zeitraum hinzufügen**, um den nächsten Zeitraum hinzuzufügen. Geben Sie dann eine oder mehrere Zeilen innerhalb des Zeitraums an.

Das Beispiel zeigt zwei Platzierungsanweisungen auf der Seite „Platzierungen definieren“ des Assistenten „ILM-Regel erstellen“.



Die erste Platzierungsanweisung (1) hat zwei Zeilen für das erste Jahr:

- Die erste Zeile erstellt zwei replizierte Objektkopien an zwei Rechenzentrumsstandorten.
- Die zweite Zeile erstellt eine 6+3-Löschcode-Kopie unter Verwendung aller Rechenzentrumsstandorte.

Die zweite Platzierungsanweisung (2) erstellt nach einem Jahr zwei Kopien und behält diese Kopien für immer.

Wenn Sie den Satz von Platzierungsanweisungen für eine Regel definieren, müssen Sie sicherstellen, dass

mindestens eine Platzierungsanweisung am Tag 0 beginnt, dass keine Lücken zwischen den von Ihnen definierten Zeiträumen bestehen und dass die letzte Platzierungsanweisung entweder für immer oder so lange gilt, bis Sie keine Objektkopien mehr benötigen.

Wenn jeder Zeitraum in der Regel abläuft, werden die Anweisungen zur Inhaltsplatzierung für den nächsten Zeitraum angewendet. Es werden neue Objektkopien erstellt und nicht benötigte Kopien gelöscht.

ILM-Regelaufnahmeverhalten

Das Aufnahmeverhalten steuert, ob Objektkopien sofort gemäß den Anweisungen in der Regel platziert werden oder ob Zwischenkopien erstellt werden und die Platzierungsanweisungen später angewendet werden. Für ILM-Regeln sind die folgenden Aufnahmeverhalten verfügbar:

- **Ausgeglichen**: StorageGRID versucht, bei der Aufnahme alle in der ILM-Regel angegebenen Kopien zu erstellen. Wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg wird an den Client zurückgegeben. Die in der ILM-Regel angegebenen Kopien werden nach Möglichkeit erstellt.
- **Streng**: Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor dem Client der Erfolg gemeldet wird.
- **Dual Commit**: StorageGRID erstellt sofort Zwischenkopien des Objekts und meldet den Erfolg an den Client. Wenn möglich, werden die in der ILM-Regel angegebenen Kopien erstellt.

Ähnliche Informationen

- "Aufnahmeoptionen"
- "Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen"
- "Wie sich Konsistenz und ILM-Regeln auf den Datenschutz auswirken"

Beispiel einer ILM-Regel

Beispielsweise könnte eine ILM-Regel Folgendes festlegen:

- Gilt nur für die Objekte, die Mieter A gehören.
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Ort.
- Bewahren Sie die beiden Kopien „für immer“ auf, was bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte, bis sie durch eine Löschanforderung des Clients oder durch Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die Option „Ausgewogen“ für das Aufnahmeverhalten: Die Anweisung zur Platzierung an zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, beide erforderlichen Kopien sofort zu erstellen.

  Wenn beispielsweise Site 2 nicht erreichbar ist, wenn Mandant A ein Objekt speichert, erstellt StorageGRID zwei Zwischenkopien auf Speicherknoten an Site 1. Sobald Site 2 verfügbar ist, erstellt StorageGRID die erforderliche Kopie an diesem Site.

Ähnliche Informationen

- "Was ist ein Speicherpool?"
- "Was ist ein Cloud-Speicherpool?"

Greifen Sie auf den Assistenten zum Erstellen einer ILM-Regel zu

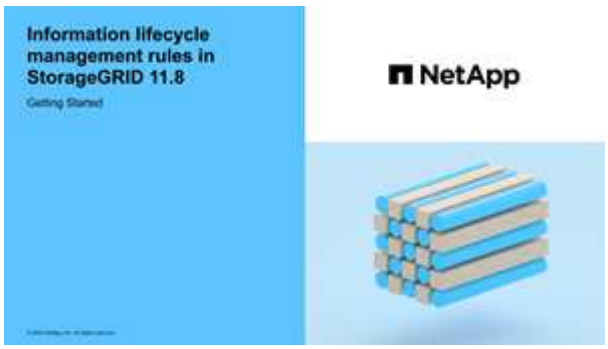
Mithilfe von ILM-Regeln können Sie die Platzierung von Objektdaten im Laufe der Zeit

verwalten. Zum Erstellen einer ILM-Regel verwenden Sie den Assistenten „ILM-Regel erstellen“.

> Wenn Sie die Standard-ILM-Regel für eine Richtlinie erstellen möchten, folgen Sie den"Anleitung zum Erstellen einer Standard-ILM-Regel" stattdessen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Wenn Sie festlegen möchten, für welche Mandantenkonten diese Regel gilt, haben Sie die"Berechtigung für Mandantenkonten" oder Sie kennen die Konto-ID für jedes Konto.
- Wenn die Regel Objekte anhand der Metadaten zum letzten Zugriffszeitpunkt filtern soll, müssen Aktualisierungen des letzten Zugriffszeitpunkts durch den S3-Bucket aktiviert werden.
- Sie haben alle Cloud-Speicherpools konfiguriert, die Sie verwenden möchten. Sehen "Cloud-Speicherpool erstellen" .
- Sie kennen die"Aufnahmeoptionen" .
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, sind Sie vertraut mit dem"Anforderungen für S3 Object Lock" .
- Optional haben Sie das Video angesehen: "Video: Übersicht über ILM-Regeln" .



Informationen zu diesem Vorgang

Beim Erstellen von ILM-Regeln:

- Berücksichtigen Sie die Topologie und Speicherkonfigurationen des StorageGRID -Systems.
- Überlegen Sie, welche Arten von Objektkopien Sie erstellen möchten (repliziert oder löschcodiert) und wie viele Kopien jedes Objekts erforderlich sind.
- Bestimmen Sie, welche Arten von Objektmetadaten in den Anwendungen verwendet werden, die eine Verbindung zum StorageGRID -System herstellen. ILM-Regeln filtern Objekte basierend auf ihren Metadaten.
- Überlegen Sie, wo Sie Objektkopien im Laufe der Zeit platzieren möchten.
- Entscheiden Sie, welche Aufnahmeoption verwendet werden soll (Balanced, Strict oder Dual Commit).

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie **Erstellen**. "Schritt 1 (Details eingeben)"des Assistenten „ILM-Regel erstellen“ wird angezeigt.

Schritt 1 von 3: Details eingeben

Im Schritt **Details eingeben** des Assistenten „ILM-Regel erstellen“ können Sie einen Namen und eine Beschreibung für die Regel eingeben und Filter für die Regel definieren.

Die Eingabe einer Beschreibung und die Definition von Filtern für die Regel sind optional.

Informationen zu diesem Vorgang

Bei der Bewertung eines Objekts anhand einer"ILM-Regel" , StorageGRID vergleicht die Objektmetadaten mit den Filtern der Regel. Wenn die Objektmetadaten allen Filtern entsprechen, verwendet StorageGRID die Regel, um das Objekt zu platzieren. Sie können eine Regel entwerfen, die auf alle Objekte angewendet wird, oder Sie können grundlegende Filter angeben, beispielsweise ein oder mehrere Mandantenkonten oder Bucket-Namen, oder erweiterte Filter, beispielsweise die Größe des Objekts oder Benutzermetadaten.

Schritte

1. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.
2. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.

   Sie sollten den Zweck bzw. die Funktion der Regel beschreiben, damit Sie die Regel später wiedererkennen.

3. Wählen Sie optional ein oder mehrere S3-Mandantenkonten aus, für die diese Regel gilt. Wenn diese Regel für alle Mieter gilt, lassen Sie dieses Feld leer.

   Wenn Sie weder über die Berechtigung „Root-Zugriff“ noch über die Berechtigung „Mandantenkonten“ verfügen, können Sie keine Mandanten aus der Liste auswählen. Geben Sie stattdessen die Mandanten-ID oder mehrere IDs als durch Kommas getrennte Zeichenfolge ein.

4. Geben Sie optional die S3-Buckets an, für die diese Regel gilt.

   Wenn **gilt für alle Buckets** ausgewählt ist (Standard), gilt die Regel für alle S3-Buckets.

5. Wählen Sie für S3-Mandanten optional **Ja** aus, um die Regel nur auf ältere Objektversionen in S3-Buckets anzuwenden, bei denen die Versionierung aktiviert ist.

   Wenn Sie **Ja** wählen, wird automatisch "Nicht aktuelle Zeit" als Referenzzeit ausgewählt in"Schritt 2 des Assistenten „ILM-Regel erstellen“" .

   > Die nicht aktuelle Zeit gilt nur für S3-Objekte in Buckets mit aktivierter Versionierung. Sehen"Operationen an Buckets, PutBucketVersioning" Und"Verwalten von Objekten mit S3 Object Lock" .

   Mit dieser Option können Sie die Speicherbelastung versionierter Objekte reduzieren, indem Sie nach nicht aktuellen Objektversionen filtern. Sehen "Beispiel 4: ILM-Regeln und -Richtlinien für versionierte S3-Objekte" .

6. Wählen Sie optional **Erweiterten Filter hinzufügen** aus, um zusätzliche Filter anzugeben.

   Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den grundlegenden Filtern entsprechen. Weitere Informationen zur erweiterten Filterung finden Sie unterVerwenden Sie erweiterte Filter in ILM-Regeln UndAngeben mehrerer Metadatentypen und -werte .

7. Wählen Sie **Weiter**. "Schritt 2 (Platzierungen definieren)"des Assistenten „ILM-Regel erstellen“ wird angezeigt.

Verwenden Sie erweiterte Filter in ILM-Regeln

Mithilfe der erweiterten Filterung können Sie ILM-Regeln erstellen, die basierend auf ihren Metadaten nur für bestimmte Objekte gelten. Wenn Sie die erweiterte Filterung für eine Regel einrichten, wählen Sie den Typ der abzugleichenden Metadaten aus, wählen einen Operator aus und geben einen Metadatenwert an. Bei der Auswertung von Objekten wird die ILM-Regel nur auf die Objekte angewendet, deren Metadaten dem erweiterten Filter entsprechen.

Die Tabelle zeigt die Metadatentypen, die Sie in erweiterten Filtern angeben können, die Operatoren, die Sie für jeden Metadatentyp verwenden können, und die erwarteten Metadatenwerte.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Aufnahmezeit	• Ist • ist nicht • ist vor • ist am oder vor • ist nach • ist am oder nach	Uhrzeit und Datum der Aufnahme des Objekts. **Hinweis:** Um Ressourcenprobleme beim Aktivieren einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter „Aufnahmezeit“ in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie die Aufnahmezeit so fest, dass sie größer oder gleich der ungefähren Zeit ist, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.
Schlüssel	• gleich • ist nicht gleich • enthält • enthält nicht • beginnt mit • beginnt nicht mit • endet mit • endet nicht mit	Der gesamte oder ein Teil eines eindeutigen S3-Objektschlüssels. Beispielsweise möchten Sie möglicherweise Objekte abgleichen, die mit enden `.txt` oder beginnen Sie mit `test-object/` .
Letzter Zugriffszeitpunkt	• Ist • ist nicht • ist vor • ist am oder vor • ist nach • ist am oder nach	Uhrzeit und Datum des letzten Abrufs (Lesens oder Anzeigens) des Objekts. **Hinweis:** Wenn Sie planen,"letzte Zugriffszeit verwenden" Als erweiterter Filter müssen Aktualisierungen der letzten Zugriffszeit für den S3-Bucket aktiviert werden.

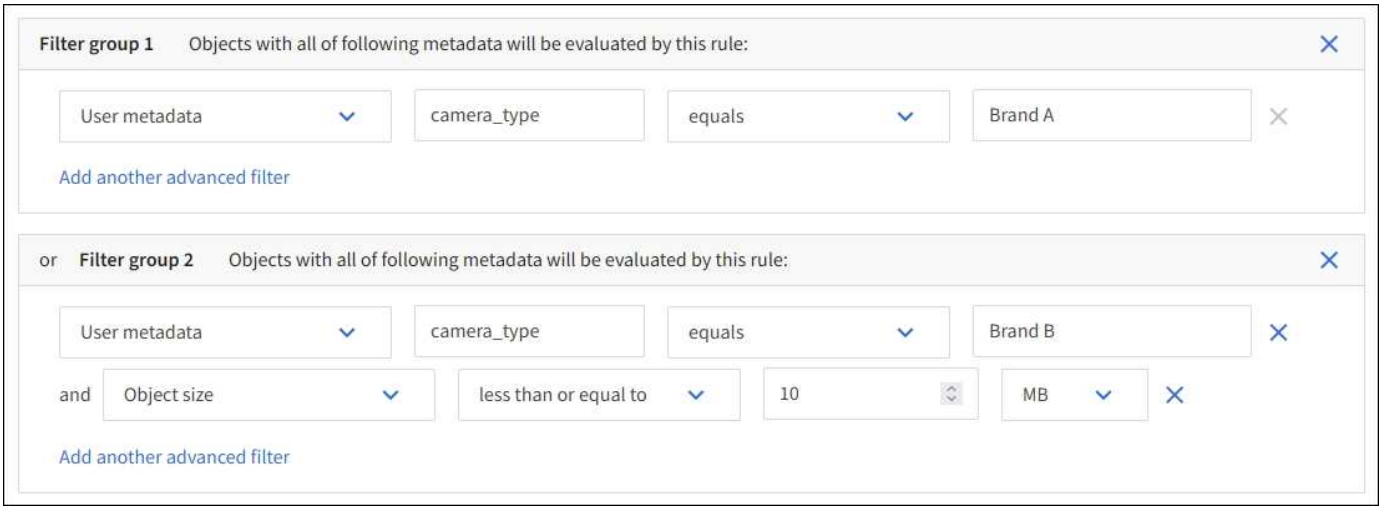
Metadatentyp	Unterstützte Operatoren	Metadatenwert
Standortbeschränkung (nur S3)	• gleich • ist nicht gleich	Die Region, in der ein S3-Bucket erstellt wurde. Verwenden Sie **ILM** > **Regionen**, um die angezeigten Regionen zu definieren. **Hinweis:** Ein Wert von us-east-1 entspricht Objekten in Buckets, die in der Region us-east-1 erstellt wurden, sowie Objekten in Buckets, für die keine Region angegeben ist. Sehen "Regionen konfigurieren (optional und nur S3)" .
Objektgröße	• gleich • ist nicht gleich • weniger als • kleiner oder gleich • größer als • größer oder gleich	Die Größe des Objekts. Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.
Benutzermetadaten	• enthält • endet mit • gleich • existiert • beginnt mit • enthält nicht • endet nicht mit • ist nicht gleich • existiert nicht • beginnt nicht mit	Schlüssel-Wert-Paar, wobei **Benutzermetadatenname** der Schlüssel und **Metadatenwert** der Wert ist. Um beispielsweise nach Objekten zu filtern, die Benutzermetadaten von `color=blue` , geben Sie an `color` für **Benutzermetadatenname**, `equals` für den Betreiber und `blue` für **Metadatenwert**. **Hinweis:** Bei Benutzermetadatennamen wird die Groß-/Kleinschreibung nicht beachtet; bei Benutzermetadatenwerten hingegen schon.
Objekt-Tag (nur S3)	• enthält • endet mit • gleich • existiert • beginnt mit • enthält nicht • endet nicht mit • ist nicht gleich • existiert nicht • beginnt nicht mit	Schlüssel-Wert-Paar, wobei **Objekt-Tag-Name** der Schlüssel und **Objekt-Tag-Wert** der Wert ist. Um beispielsweise nach Objekten zu filtern, die den Objekttag `Image=True` , geben Sie an `Image` für **Objekt-Tag-Name**, `equals` für den Betreiber und `True` für **Objekt-Tag-Wert**. **Hinweis:** Bei Objekt-Tag-Namen und Objekt-Tag-Werten wird zwischen Groß- und Kleinschreibung unterschieden. Sie müssen diese Elemente genau so eingeben, wie sie für das Objekt definiert wurden.

Angeben mehrerer Metadatentypen und -werte

Wenn Sie erweiterte Filter definieren, können Sie mehrere Metadatentypen und mehrere Metadatenwerte angeben. Wenn Sie beispielsweise möchten, dass eine Regel auf Objekte mit einer Größe zwischen 10 MB und 100 MB zutrifft, wählen Sie den Metadatentyp **Objektgröße** aus und geben zwei Metadatenwerte an.

- Der erste Metadatenwert gibt Objekte an, die größer oder gleich 10 MB sind.
- Der zweite Metadatenwert gibt Objekte an, die kleiner oder gleich 100 MB sind.

Durch die Verwendung mehrerer Einträge haben Sie eine genaue Kontrolle darüber, welche Objekte abgeglichen werden. Im folgenden Beispiel gilt die Regel für Objekte, die als Wert der Benutzermetadaten „camera_type“ die Marke A oder Marke B haben. Die Regel gilt jedoch nur für Objekte der Marke B, die kleiner als 10 MB sind.



Schritt 2 von 3: Platzierungen definieren

Im Schritt **Platzierungen definieren** des Assistenten „ILM-Regel erstellen“ können Sie die Platzierungsanweisungen definieren, die bestimmen, wie lange Objekte gespeichert werden, welche Art von Kopien (repliziert oder löschcodiert), welcher Speicherort und wie viele Kopien es sein sollen.

> Bei den gezeigten Screenshots handelt es sich um Beispiele. Ihre Ergebnisse können je nach Ihrer StorageGRID -Version variieren.

Informationen zu diesem Vorgang

Eine ILM-Regel kann eine oder mehrere Platzierungsanweisungen enthalten. Jede Platzierungsanweisung gilt jeweils für einen Zeitraum. Wenn Sie mehr als eine Anweisung verwenden, müssen die Zeiträume zusammenhängend sein und mindestens eine Anweisung muss am Tag 0 beginnen. Die Anweisungen können entweder für immer fortgesetzt werden oder bis Sie keine Objektkopien mehr benötigen.

Jede Platzierungsanweisung kann mehrere Zeilen umfassen, wenn Sie verschiedene Arten von Kopien erstellen oder während dieses Zeitraums verschiedene Standorte verwenden möchten.

In diesem Beispiel speichert die ILM-Regel für das erste Jahr eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2. Nach einem Jahr wird eine 2+1-Löschcode-Kopie erstellt und nur an einem Standort gespeichert.

Schritte

1. Wählen Sie für **Referenzzeit** den Zeittyp aus, der bei der Berechnung der Startzeit für eine Platzierungsanweisung verwendet werden soll.

Option	Beschreibung
Aufnahmezeit	Der Zeitpunkt, zu dem das Objekt aufgenommen wurde.
Letzter Zugriffszeitpunkt	Der Zeitpunkt, zu dem das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde. Um diese Option zu verwenden, müssen Aktualisierungen der letzten Zugriffszeit für den S3-Bucket aktiviert werden. Weitere Informationen finden Sie unter "Verwenden der letzten Zugriffszeit in ILM-Regeln" .
Benutzerdefinierte Erstellungszeit	Eine in benutzerdefinierten Metadaten angegebene Zeit.
Nicht aktuelle Zeit	"Nicht aktuelle Zeit" wird automatisch ausgewählt, wenn Sie **Ja** für die Frage "Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?" in"Schritt 1 des Assistenten „ILM-Regel erstellen“" .

   Wenn Sie eine *konforme* Regel erstellen möchten, müssen Sie **Aufnahmezeit** auswählen. Weitere Informationen finden Sie unter "Verwalten von Objekten mit S3 Object Lock" .

2. Geben Sie im Abschnitt **Zeitraum und Platzierungen** eine Startzeit und eine Dauer für den ersten Zeitraum ein.

   Sie möchten beispielsweise angeben, wo Objekte im ersten Jahr gespeichert werden sollen (*Ab Tag 0 365 Tage lang speichern*). Mindestens eine Anweisung muss am Tag 0 beginnen.

3. Wenn Sie replizierte Kopien erstellen möchten:
   a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Replikation** aus.
   b. Wählen Sie die Anzahl der Kopien aus, die Sie erstellen möchten.

      Wenn Sie die Anzahl der Kopien auf 1 ändern, wird eine Warnung angezeigt. Eine ILM-Regel, die für einen bestimmten Zeitraum nur eine replizierte Kopie erstellt, birgt das Risiko eines dauerhaften Datenverlusts. Weitere Informationen finden Sie unter "Warum Sie keine Einzelkopiereplikation verwenden sollten" .

      Um das Risiko zu vermeiden, führen Sie eine oder mehrere der folgenden Aktionen aus:

      - Erhöhen Sie die Anzahl der Kopien für den Zeitraum.

- Fügen Sie Kopien zu anderen Speicherpools oder einem Cloud-Speicherpool hinzu.
- Wählen Sie **Erasure Coding** anstelle von **Replikation**.

  Sie können diese Warnung getrost ignorieren, wenn diese Regel bereits mehrere Kopien für alle Zeiträume erstellt.

c. Wählen Sie im Feld **Kopien auf** die Speicherpools aus, die Sie hinzufügen möchten.

   Wenn Sie nur einen Speicherpool angeben, beachten Sie, dass StorageGRID auf einem bestimmten Speicherknoten nur eine replizierte Kopie eines Objekts speichern kann. Wenn Ihr Raster drei Speicherknoten enthält und Sie 4 als Anzahl der Kopien auswählen, werden nur drei Kopien erstellt – eine Kopie für jeden Speicherknoten.

   Die Warnung **ILM-Platzierung nicht erreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

   Wenn Sie mehr als einen Speicherpool angeben, beachten Sie die folgenden Regeln:

   - Die Anzahl der Kopien kann nicht größer sein als die Anzahl der Speicherpools.
   - Wenn die Anzahl der Kopien der Anzahl der Speicherpools entspricht, wird in jedem Speicherpool eine Kopie des Objekts gespeichert.
   - Wenn die Anzahl der Kopien geringer ist als die Anzahl der Speicherpools, wird eine Kopie am Aufnahmestandort gespeichert. Anschließend verteilt das System die verbleibenden Kopien, um die Festplattennutzung auf die Pools auszubalancieren und gleichzeitig sicherzustellen, dass kein Standort mehr als eine Kopie eines Objekts erhält.
   - Wenn sich die Speicherpools überschneiden (dieselben Speicherknoten enthalten), werden alle Kopien des Objekts möglicherweise nur an einem Standort gespeichert. Geben Sie aus diesem Grund nicht den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) und einen anderen Speicherpool an.

4. Wenn Sie eine löschcodierte Kopie erstellen möchten:

   a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Erasure Coding** aus.

      > Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

   b. Wenn Sie keinen Objektgrößenfilter für einen Wert größer als 200 KB hinzugefügt haben, wählen Sie **Zurück**, um zu Schritt 1 zurückzukehren. Wählen Sie dann **Erweiterten Filter hinzufügen** und legen Sie einen **Objektgrößen**-Filter auf einen Wert größer als 200 KB fest.

   c. Wählen Sie den Speicherpool aus, den Sie hinzufügen möchten, und das Erasure-Coding-Schema, das Sie verwenden möchten.

      Der Speicherort für eine Erasure-Coded-Kopie umfasst den Namen des Erasure-Coding-Schemas, gefolgt vom Namen des Speicherpools.

   Die verfügbaren Erasure-Coding-Schemata sind durch die Anzahl der Speicherknoten im von Ihnen ausgewählten Speicherpool begrenzt. A `Recommended` Das Abzeichen erscheint neben den Schemata, die entweder die"bester Schutz oder geringster Speicheraufwand" .

5. Optional:

a. Wählen Sie **Anderen Typ oder Speicherort hinzufügen**, um zusätzliche Kopien an anderen Speicherorten zu erstellen.

b. Wählen Sie **Weiteren Zeitraum hinzufügen**, um verschiedene Zeiträume hinzuzufügen.

> Das Löschen von Objekten erfolgt auf Grundlage der folgenden Einstellungen:
>
> - Objekte werden am Ende des letzten Zeitraums automatisch gelöscht, sofern nicht ein anderer Zeitraum mit **für immer** endet.
> - Je nach"Bucket- und Tenant-Aufbewahrungsdauereinstellungen" , werden Objekte möglicherweise nicht gelöscht, selbst wenn die ILM-Aufbewahrungsfrist endet.

6. Wenn Sie Objekte in einem Cloud-Speicherpool speichern möchten:

a. Wählen Sie in der Dropdownliste **Objekte speichern nach** die Option **Replikation** aus.

b. Wählen Sie das Feld **Kopien auf** und dann einen Cloud-Speicherpool aus.

Beachten Sie bei der Verwendung von Cloud-Speicherpools die folgenden Regeln:

- Sie können in einer einzelnen Platzierungsanweisung nicht mehr als einen Cloud-Speicherpool auswählen. Ebenso können Sie in derselben Platzierungsanweisung keinen Cloud-Speicherpool und keinen Speicherpool auswählen.
- Sie können in einem bestimmten Cloud-Speicherpool nur eine Kopie eines Objekts speichern. Wenn Sie **Kopien** auf 2 oder mehr einstellen, wird eine Fehlermeldung angezeigt.
- Sie können in keinem Cloud-Speicherpool gleichzeitig mehr als eine Objektkopie speichern. Eine Fehlermeldung wird angezeigt, wenn mehrere Platzierungen, die einen Cloud-Speicherpool verwenden, überlappende Daten aufweisen oder wenn mehrere Zeilen in derselben Platzierung einen Cloud-Speicherpool verwenden.
- Sie können ein Objekt in einem Cloud-Speicherpool speichern, während das Objekt gleichzeitig als replizierte oder löschcodierte Kopie in StorageGRID gespeichert wird. Allerdings müssen Sie in der Platzierungsanweisung für den Zeitraum mehrere Zeilen angeben, damit Sie für jeden Standort die Anzahl und Art der Kopien festlegen können.

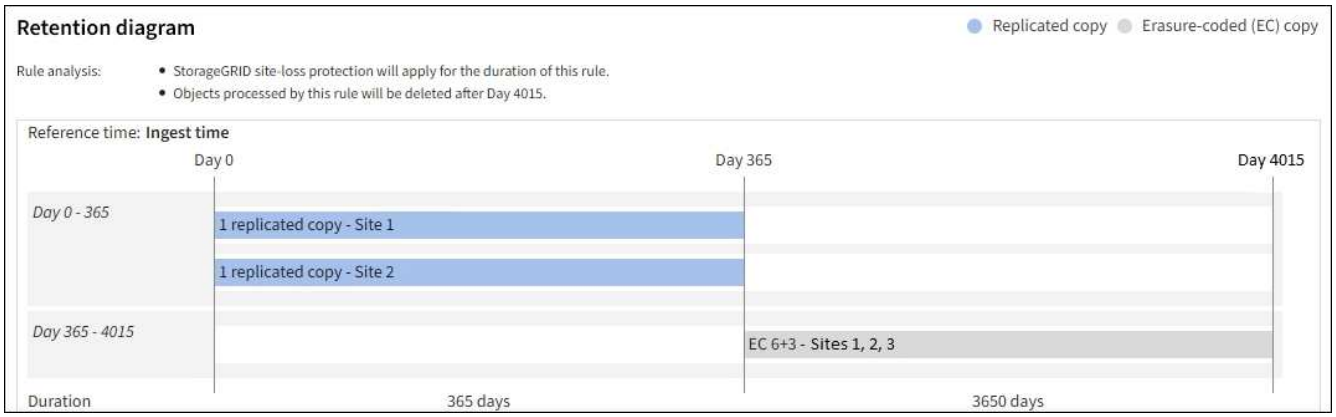
7. Bestätigen Sie im Retentionsdiagramm Ihre Platzierungsanweisungen.

In diesem Beispiel speichert die ILM-Regel für das erste Jahr eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2. Nach einem Jahr und für weitere 10 Jahre wird eine 6+3-Löschcode-Kopie an drei Standorten gespeichert. Nach insgesamt 11 Jahren werden die Objekte aus StorageGRID gelöscht.

Im Abschnitt „Regelanalyse“ des Retention-Diagramms heißt es:

- Für die Dauer dieser Regelung gilt der Site-Loss-Schutz von StorageGRID .
- Von dieser Regel verarbeitete Objekte werden nach Tag 4015 gelöscht.

Siehe "Aktivieren Sie den Site-Loss-Schutz."



8. Wählen Sie **Weiter**. "Schritt 3 (Aufnahmeverhalten auswählen)"des Assistenten „ILM-Regel erstellen“ wird angezeigt.

Verwenden der letzten Zugriffszeit in ILM-Regeln

Sie können die letzte Zugriffszeit als Referenzzeit in einer ILM-Regel verwenden. Beispielsweise möchten Sie möglicherweise Objekte, die in den letzten drei Monaten angezeigt wurden, auf lokalen Speicherknoten belassen und Objekte, die nicht so kürzlich angezeigt wurden, an einen externen Standort verschieben. Sie können die letzte Zugriffszeit auch als erweiterten Filter verwenden, wenn eine ILM-Regel nur auf Objekte angewendet werden soll, auf die zuletzt an einem bestimmten Datum zugegriffen wurde.

Informationen zu diesem Vorgang

Bevor Sie die letzte Zugriffszeit in einer ILM-Regel verwenden, sollten Sie die folgenden Überlegungen berücksichtigen:

- Wenn Sie die letzte Zugriffszeit als Referenzzeit verwenden, beachten Sie, dass das Ändern der letzten Zugriffszeit für ein Objekt keine sofortige ILM-Auswertung auslöst. Stattdessen werden die Platzierungen des Objekts bewertet und das Objekt wird nach Bedarf verschoben, wenn ILM das Objekt im Hintergrund auswertet. Dies kann nach dem Zugriff auf das Objekt zwei Wochen oder länger dauern.

  Berücksichtigen Sie diese Latenz beim Erstellen von ILM-Regeln basierend auf der letzten Zugriffszeit und vermeiden Sie Platzierungen mit kurzen Zeiträumen (weniger als ein Monat).

- Wenn Sie die letzte Zugriffszeit als erweiterten Filter oder als Referenzzeit verwenden, müssen Sie die Aktualisierung der letzten Zugriffszeit für S3-Buckets aktivieren. Sie können die"Mietermanager" oder die"Mandantenverwaltungs-API" .

  Aktualisierungen der letzten Zugriffszeit sind für S3-Buckets standardmäßig deaktiviert.

  Beachten Sie, dass die Aktivierung von Updates zur letzten Zugriffszeit die Leistung beeinträchtigen kann, insbesondere in Systemen mit kleinen Objekten. Die Leistungseinbußen entstehen dadurch, dass StorageGRID die Objekte bei jedem Abrufen mit neuen Zeitstempeln aktualisieren muss.

In der folgenden Tabelle ist zusammengefasst, ob die letzte Zugriffszeit für alle Objekte im Bucket für verschiedene Arten von Anforderungen aktualisiert wird.

Art der Anfrage	Ob die Zeit des letzten Zugriffs aktualisiert wird, wenn die Aktualisierung der Zeit des letzten Zugriffs deaktiviert ist	Ob die Zeit des letzten Zugriffs aktualisiert wird, wenn die Aktualisierung der Zeit des letzten Zugriffs aktiviert ist
Anforderung zum Abrufen eines Objekts, seiner Zugriffskontrollliste oder seiner Metadaten	Nein	Ja
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja	Ja
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
Anfrage zum Abschließen eines mehrteiligen Uploads	Ja, für das montierte Objekt	Ja, für das montierte Objekt

Schritt 3 von 3: Aufnahmeverhalten auswählen

Im Schritt **Aufnahmeverhalten auswählen** des Assistenten „ILM-Regel erstellen“ können Sie auswählen, wie die durch diese Regel gefilterten Objekte bei der Aufnahme geschützt werden.

Informationen zu diesem Vorgang

StorageGRID kann Zwischenkopien erstellen und die Objekte für eine spätere ILM-Auswertung in die Warteschlange stellen oder Kopien erstellen, um die Platzierungsanweisungen der Regel sofort zu erfüllen.

Schritte

1. Wählen Sie die"Aufnahmeverhalten" zu verwenden.

   Weitere Informationen finden Sie unter "Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen" .

   > Sie können die Option „Ausgewogen“ oder „Streng“ nicht verwenden, wenn die Regel eine dieser Platzierungen verwendet:
   >
   > - Ein Cloud-Speicherpool am Tag 0
   > - Ein Cloud-Speicherpool, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit verwendet
   >
   > Sehen "Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten" .

2. Wählen Sie **Erstellen**.

   Die ILM-Regel wird erstellt. Die Regel wird erst aktiv, wenn sie zu einem"ILM-Richtlinie" und diese Richtlinie ist aktiviert.

   Um die Details der Regel anzuzeigen, wählen Sie den Namen der Regel auf der ILM-Regelseite aus.

Erstellen einer ILM-Standardregel

Bevor Sie eine ILM-Richtlinie erstellen, müssen Sie eine Standardregel erstellen, um alle Objekte, die keiner anderen Regel entsprechen, in der Richtlinie zu platzieren. Die Standardregel kann keine Filter verwenden. Es muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

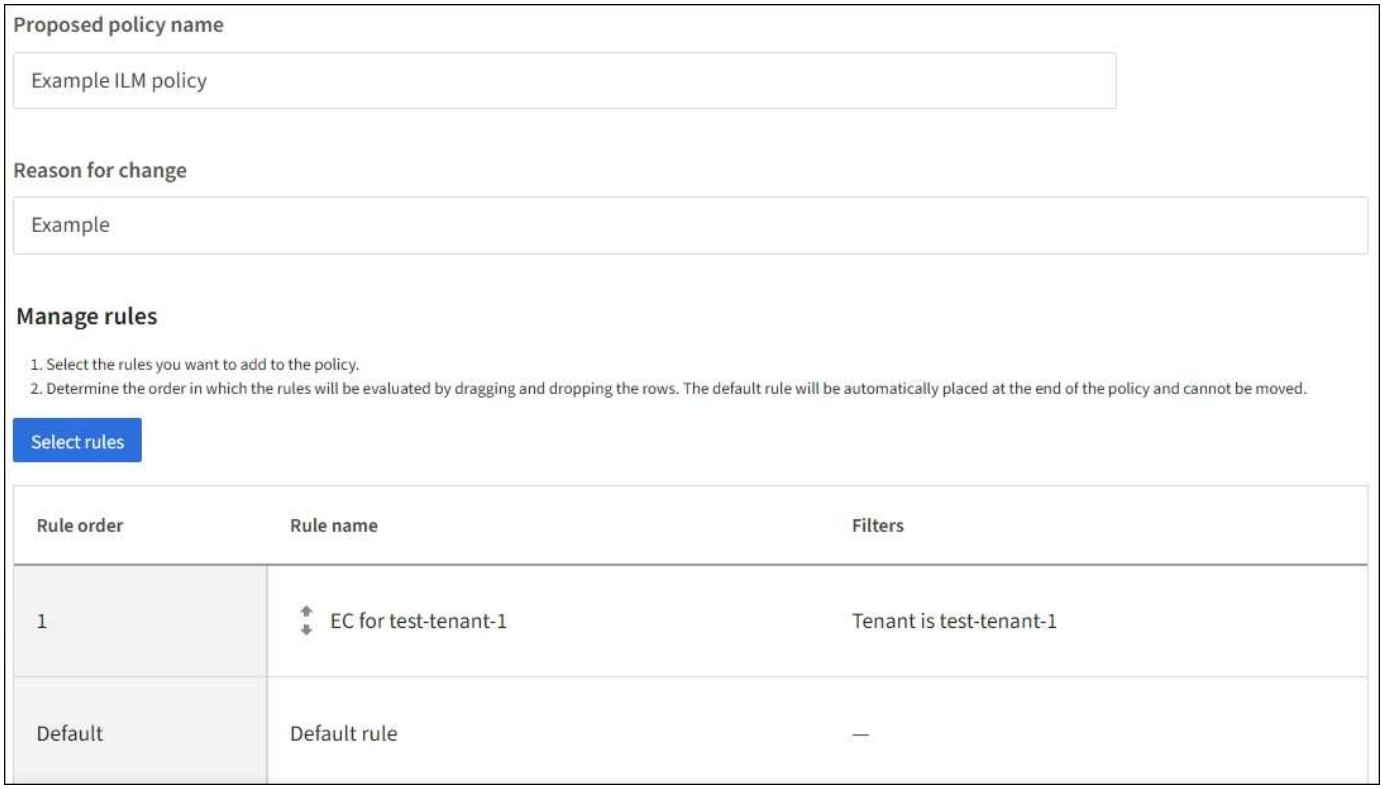
Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Die Standardregel ist die letzte Regel, die in einer ILM-Richtlinie ausgewertet wird, daher kann sie keine Filter verwenden. Die Platzierungsanweisungen für die Standardregel werden auf alle Objekte angewendet, die keiner anderen Regel in der Richtlinie entsprechen.

In dieser Beispielrichtlinie gilt die erste Regel nur für Objekte, die zu Test-Tenant-1 gehören. Die letzte Standardregel gilt für Objekte, die zu allen anderen Mandantenkonten gehören.



Beachten Sie beim Erstellen der Standardregel die folgenden Anforderungen:

- Die Standardregel wird automatisch als letzte Regel platziert, wenn Sie sie einer Richtlinie hinzufügen.
- Die Standardregel kann keine grundlegenden oder erweiterten Filter verwenden.
- Die Standardregel muss für alle Objektversionen gelten.
- Die Standardregel sollte replizierte Kopien erstellen.

Verwenden Sie keine Regel, die Erasure-Coded-Kopien erstellt, als Standardregel für eine Richtlinie. Erasure-Coding-Regeln sollten einen erweiterten Filter verwenden, um zu verhindern, dass kleinere Objekte mit Erasure-Coding behandelt werden.

- Im Allgemeinen sollte die Standardregel Objekte für immer behalten.
- Wenn Sie die globale S3-Objektsperreinstellung verwenden (oder aktivieren möchten), muss die Standardregel konform sein.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie **Erstellen**.

   Schritt 1 (Details eingeben) des Assistenten „ILM-Regel erstellen“ wird angezeigt.

3. Geben Sie im Feld **Regelname** einen eindeutigen Namen für die Regel ein.
4. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.
5. Lassen Sie das Feld **Mandantenkonten** leer.

   Die Standardregel muss für alle Mandantenkonten gelten.

6. Belassen Sie die Dropdown-Auswahl „Bucket-Name“ auf **gilt für alle Buckets**.

   Die Standardregel muss für alle S3-Buckets gelten.

7. Behalten Sie die Standardantwort **Nein** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ bei.
8. Fügen Sie keine erweiterten Filter hinzu.

   Die Standardregel kann keine Filter angeben.

9. Wählen Sie **Weiter**.

   Schritt 2 (Platzierungen definieren) wird angezeigt.

10. Wählen Sie für die Referenzzeit eine beliebige Option aus.

    Wenn Sie die Standardantwort **Nein** auf die Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ beibehalten haben, Nicht aktuelle Zeiten werden nicht in die Pulldown-Liste aufgenommen. Die Standardregel muss für alle Objektversionen gelten.

11. Geben Sie die Platzierungsanweisungen für die Standardregel an.
    - Die Standardregel sollte Objekte für immer behalten. Wenn Sie eine neue Richtlinie aktivieren und die Standardregel Objekte nicht für immer beibehält, wird eine Warnung angezeigt. Sie müssen bestätigen, dass dies das von Ihnen erwartete Verhalten ist.
    - Die Standardregel sollte replizierte Kopien erstellen.

Verwenden Sie keine Regel, die Erasure-Coded-Kopien erstellt, als Standardregel für eine Richtlinie. Erasure-Coding-Regeln sollten den erweiterten Filter **Objektgröße (MB) größer als 200 KB** enthalten, um zu verhindern, dass kleinere Objekte einem Erasure-Coding unterzogen werden.

- Wenn Sie die globale S3-Objektsperreinstellung verwenden (oder aktivieren möchten), muss die Standardregel konform sein:
  - Es müssen mindestens zwei replizierte Objektkopien oder eine Erasure-Coded-Kopie erstellt werden.
  - Diese Kopien müssen für die gesamte Dauer jeder Zeile in den Platzierungsanweisungen auf den Speicherknoten vorhanden sein.
  - Objektkopien können nicht in einem Cloud-Speicherpool gespeichert werden.
  - Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei die Aufnahmezeit als Referenzzeit verwendet wird.
  - Mindestens eine Zeile der Platzierungsanweisungen muss „für immer“ lauten.

12. Sehen Sie sich das Retentionsdiagramm an, um Ihre Platzierungsanweisungen zu bestätigen.
13. Wählen Sie **Weiter**.

    Schritt 3 (Aufnahmeverhalten auswählen) wird angezeigt.

14. Wählen Sie die zu verwendende Aufnahmeoption und wählen Sie **Erstellen**.

Verwalten von ILM-Richtlinien

Verwenden von ILM-Richtlinien

Eine Richtlinie für das Information Lifecycle Management (ILM) ist ein geordneter Satz von ILM-Regeln, der bestimmt, wie das StorageGRID -System Objektdaten im Laufe der Zeit verwaltet.

> Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Standard-ILM-Richtlinie

Wenn Sie StorageGRID installieren und Sites hinzufügen, wird automatisch eine Standard-ILM-Richtlinie wie folgt erstellt:

- Wenn Ihr Raster eine Site enthält, enthält die Standardrichtlinie eine Standardregel, die zwei Kopien jedes Objekts an dieser Site repliziert.
- Wenn Ihr Raster mehr als eine Site enthält, repliziert die Standardregel eine Kopie jedes Objekts an jeder Site.

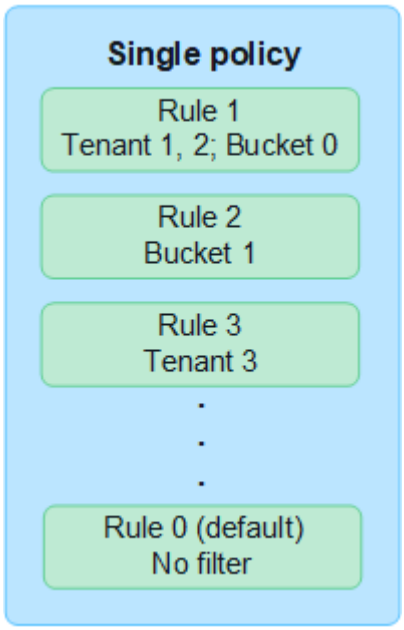
Wenn die Standardrichtlinie Ihren Speicheranforderungen nicht entspricht, können Sie Ihre eigenen Regeln und Richtlinien erstellen. Sehen"Erstellen einer ILM-Regel" Und"Erstellen einer ILM-Richtlinie" .

Eine oder mehrere aktive ILM-Richtlinien?

Sie können eine oder mehrere aktive ILM-Richtlinien gleichzeitig haben.

Eine Richtlinie

Wenn Ihr Grid ein einfaches Datenschutzschema mit wenigen mandanten- und bucketspezifischen Regeln verwendet, verwenden Sie eine einzelne aktive ILM-Richtlinie. Die ILM-Regeln können Filter enthalten, um verschiedene Buckets oder Mandanten zu verwalten.



Wenn Sie nur eine Richtlinie haben und sich die Anforderungen eines Mandanten ändern, müssen Sie eine neue ILM-Richtlinie erstellen oder die vorhandene Richtlinie klonen, um Änderungen anzuwenden, die neue ILM-Richtlinie zu simulieren und dann zu aktivieren. Änderungen an der ILM-Richtlinie können zu Objektverschiebungen führen, die mehrere Tage dauern und zu Systemlatenz führen können.

Mehrere Richtlinien

Um den Mietern unterschiedliche Servicequalitätsoptionen bereitzustellen, können Sie mehrere aktive Richtlinien gleichzeitig haben. Jede Richtlinie kann bestimmte Mandanten, S3-Buckets und Objekte verwalten. Wenn Sie eine Richtlinie für einen bestimmten Satz von Mandanten oder Objekten anwenden oder ändern, sind die auf andere Mandanten und Objekte angewendeten Richtlinien davon nicht betroffen.

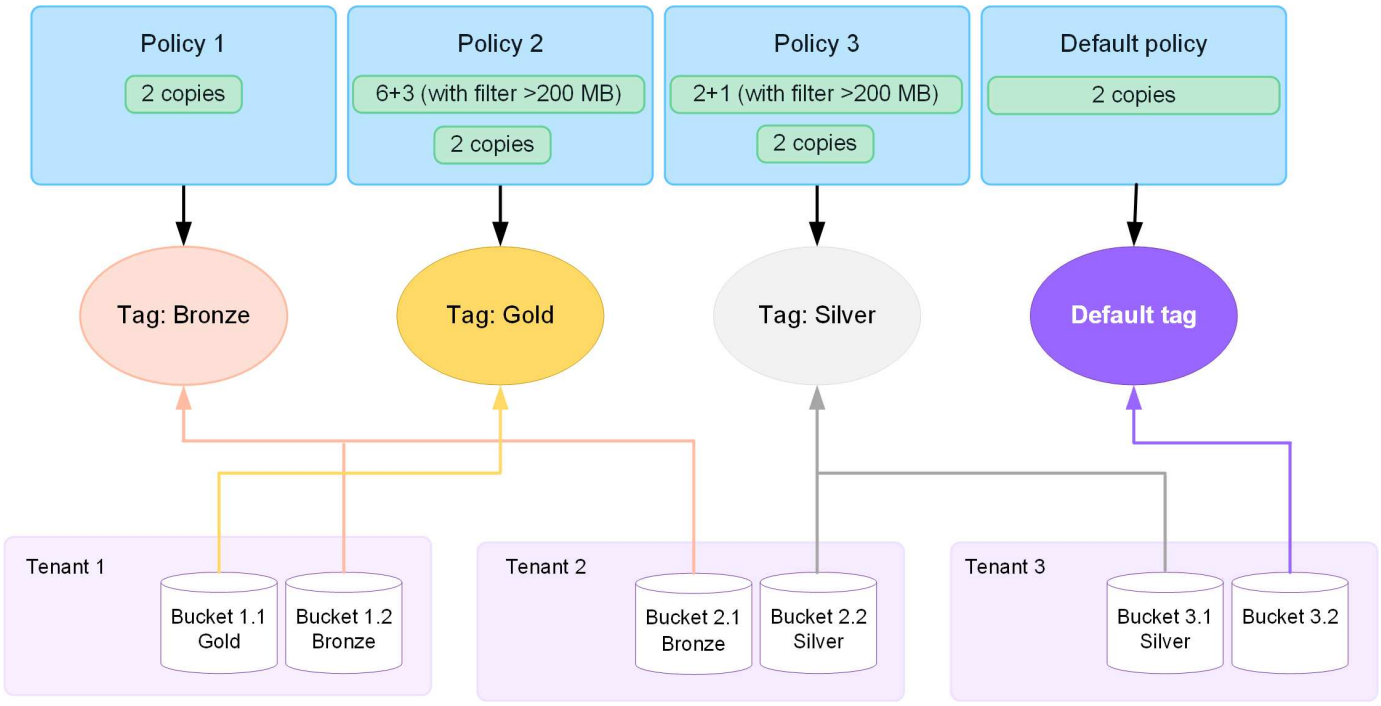
ILM-Richtlinientags

Wenn Sie es Mandanten ermöglichen möchten, problemlos zwischen mehreren Datenschutzrichtlinien pro Bucket zu wechseln, verwenden Sie mehrere ILM-Richtlinien mit *ILM-Richtlinien-Tags*. Sie weisen jeder ILM-Richtlinie ein Tag zu, und anschließend markieren Mandanten einen Bucket, um die Richtlinie auf diesen Bucket anzuwenden. Sie können ILM-Richtlinien-Tags nur auf S3-Buckets festlegen.

Sie könnten beispielsweise drei Tags mit den Namen „Gold“, „Silber“ und „Bronze“ haben. Sie können jedem Tag eine ILM-Richtlinie zuweisen, basierend darauf, wie lange und wo diese Richtlinie Objekte speichert. Mieter können durch Markieren ihrer Buckets auswählen, welche Richtlinie verwendet werden soll. Ein Bucket mit der Kennzeichnung „Gold“ wird durch die Gold-Richtlinie verwaltet und erhält die Datenschutz- und Leistungsstufe „Gold“.

Standard-ILM-Richtlinientag

Bei der Installation von StorageGRID wird automatisch ein standardmäßiges ILM-Richtlinientag erstellt. Jedes Raster muss über eine aktive Richtlinie verfügen, die dem Standardtag zugewiesen ist. Die Standardrichtlinie gilt für alle nicht markierten S3-Buckets.



Wie bewertet eine ILM-Richtlinie Objekte?

Eine aktive ILM-Richtlinie steuert die Platzierung, Dauer und den Datenschutz von Objekten.

Wenn Clients Objekte in StorageGRID speichern, werden die Objekte anhand des geordneten Satzes von ILM-Regeln in der Richtlinie wie folgt ausgewertet:

1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten dieser Regel aufgenommen und gemäß den Platzierungsanweisungen dieser Regel gespeichert.
2. Wenn die Filter für die erste Regel nicht mit dem Objekt übereinstimmen, wird das Objekt anhand jeder nachfolgenden Regel in der Richtlinie ausgewertet, bis eine Übereinstimmung gefunden wird.
3. Wenn keine Regeln mit einem Objekt übereinstimmen, werden das Aufnahmeverhalten und die Platzierungsanweisungen für die Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie. Die Standardregel muss für alle Mandanten, alle S3-Buckets und alle Objektversionen gelten und darf keine erweiterten Filter verwenden.

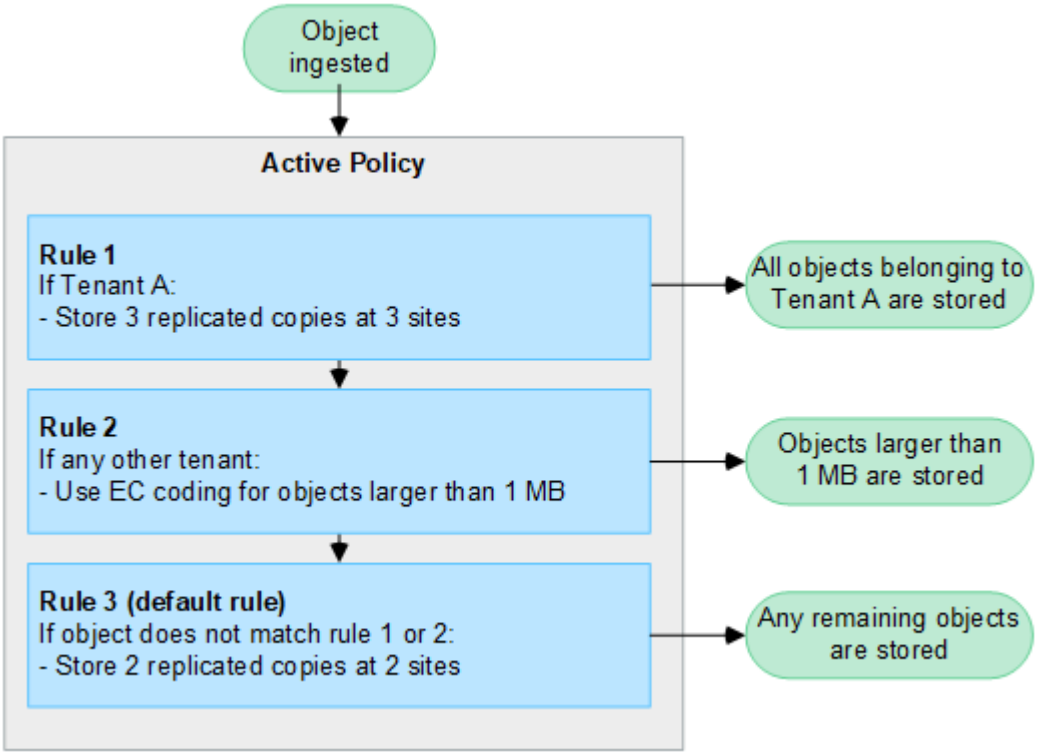
Beispiel einer ILM-Richtlinie

Beispielsweise könnte eine ILM-Richtlinie drei ILM-Regeln enthalten, die Folgendes festlegen:

- **Regel 1: Replikate für Mieter A**
  - Alle Objekte abgleichen, die zu Mieter A gehören.
  - Speichern Sie diese Objekte als drei replizierte Kopien an drei Standorten.
  - Objekte, die anderen Mandanten gehören, werden nicht mit Regel 1 abgeglichen, daher werden sie anhand von Regel 2 ausgewertet.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
  - Alle Objekte anderer Mandanten werden abgeglichen, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mittels 6+3-Erasure-Coding an drei Standorten gespeichert.
  - Stimmt nicht mit Objekten überein, die 1 MB oder kleiner sind. Daher werden diese Objekte anhand

von Regel 3 ausgewertet.

- **Regel 3: 2 Kopien, 2 Rechenzentren** (Standard)
  - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
  - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und 1 MB oder kleiner sind).



Was sind aktive und inaktive Richtlinien?

Jedes StorageGRID -System muss über mindestens eine aktive ILM-Richtlinie verfügen. Wenn Sie mehr als eine aktive ILM-Richtlinie haben möchten, erstellen Sie ILM-Richtlinien-Tags und weisen jedem Tag eine Richtlinie zu. Anschließend wenden Mandanten Tags auf S3-Buckets an. Die Standardrichtlinie wird auf alle Objekte in Buckets angewendet, denen kein Richtlinientag zugewiesen ist.

Wenn Sie zum ersten Mal eine ILM-Richtlinie erstellen, wählen Sie eine oder mehrere ILM-Regeln aus und ordnen sie in einer bestimmten Reihenfolge an. Nachdem Sie die Richtlinie simuliert haben, um ihr Verhalten zu bestätigen, aktivieren Sie sie.

Wenn Sie eine ILM-Richtlinie aktivieren, verwendet StorageGRID diese Richtlinie zum Verwalten aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Vorhandene Objekte werden möglicherweise an neue Speicherorte verschoben, wenn die ILM-Regeln in der neuen Richtlinie implementiert werden.

Wenn Sie mehrere ILM-Richtlinien gleichzeitig aktivieren und Mandanten Richtlinien-Tags auf S3-Buckets anwenden, werden die Objekte in jedem Bucket entsprechend der dem Tag zugewiesenen Richtlinie verwaltet.

Ein StorageGRID -System verfolgt den Verlauf der aktivierten oder deaktivierten Richtlinien.

Überlegungen zum Erstellen einer ILM-Richtlinie

- Verwenden Sie in Testsystemen nur die vom System bereitgestellte Richtlinie „Baseline 2-Kopienrichtlinie“. Für StorageGRID 11.6 und früher verwendet die Regel „2 Kopien erstellen“ in dieser Richtlinie den Speicherpool „Alle Speicherknoten“, der alle Sites enthält. Wenn Ihr StorageGRID -System über mehr als

einen Standort verfügt, können zwei Kopien eines Objekts am selben Standort platziert werden.

> Der Speicherpool „Alle Speicherknoten“ wird während der Installation von StorageGRID 11.6 und früher automatisch erstellt. Wenn Sie auf eine neuere Version von StorageGRID aktualisieren, bleibt der Pool „Alle Speicherknoten“ weiterhin vorhanden. Wenn Sie StorageGRID 11.7 oder höher als Neuinstallation installieren, wird der Pool „Alle Speicherknoten“ nicht erstellt.

- Berücksichtigen Sie beim Entwerfen einer neuen Richtlinie alle verschiedenen Objekttypen, die in Ihr Raster aufgenommen werden könnten. Stellen Sie sicher, dass die Richtlinie Regeln zum Abgleichen und Platzieren dieser Objekte nach Bedarf enthält.
- Halten Sie die ILM-Richtlinie so einfach wie möglich. Dadurch werden potenziell gefährliche Situationen vermieden, in denen Objektdaten nicht wie vorgesehen geschützt sind, wenn im Laufe der Zeit Änderungen am StorageGRID -System vorgenommen werden.
- Stellen Sie sicher, dass die Regeln in der Richtlinie in der richtigen Reihenfolge stehen. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte von den Regeln in der aufgeführten Reihenfolge (von oben beginnend) ausgewertet. Wenn beispielsweise die erste Regel in einer Richtlinie mit einem Objekt übereinstimmt, wird dieses Objekt von keiner anderen Regel ausgewertet.
- Die letzte Regel in jeder ILM-Richtlinie ist die Standard-ILM-Regel, die keine Filter verwenden kann. Wenn ein Objekt keiner anderen Regel entspricht, steuert die Standardregel, wo das Objekt platziert wird und wie lange es aufbewahrt wird.
- Überprüfen Sie vor der Aktivierung einer neuen Richtlinie alle Änderungen, die die Richtlinie an der Platzierung vorhandener Objekte vornimmt. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Erstellen von ILM-Richtlinien

Erstellen Sie eine oder mehrere ILM-Richtlinien, um Ihre Servicequalitätsanforderungen zu erfüllen.

Wenn Sie über eine aktive ILM-Richtlinie verfügen, können Sie dieselben ILM-Regeln auf alle Mandanten und Buckets anwenden.

Wenn Sie über mehrere aktive ILM-Richtlinien verfügen, können Sie die entsprechenden ILM-Regeln auf bestimmte Mandanten und Buckets anwenden, um mehrere Servicequalitätsanforderungen zu erfüllen.

Erstellen einer ILM-Richtlinie

Informationen zu diesem Vorgang

Bevor Sie Ihre eigene Richtlinie erstellen, überprüfen Sie, ob die"Standard-ILM-Richtlinie" entspricht nicht Ihren Speicheranforderungen.

> Verwenden Sie in Testsystemen nur die vom System bereitgestellten Richtlinien, 2 Kopien der Richtlinie (für Grids mit einem Standort) oder 1 Kopie pro Standort (für Grids mit mehreren Standorten). Für StorageGRID 11.6 und früher verwendet die Standardregel in dieser Richtlinie den Speicherpool „Alle Speicherknoten“, der alle Sites enthält. Wenn Ihr StorageGRID -System über mehr als einen Standort verfügt, können zwei Kopien eines Objekts am selben Standort platziert werden.

Wenn die"Die globale S3-Objektsperreinstellung wurde aktiviert" müssen Sie sicherstellen, dass die ILM-Richtlinie den Anforderungen von Buckets entspricht, bei denen S3 Object Lock aktiviert ist. Befolgen Sie in diesem Abschnitt die Anweisungen zur Aktivierung der S3-Objektsperre.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .
- Du hast"erstellte ILM-Regeln" basierend darauf, ob S3 Object Lock aktiviert ist.

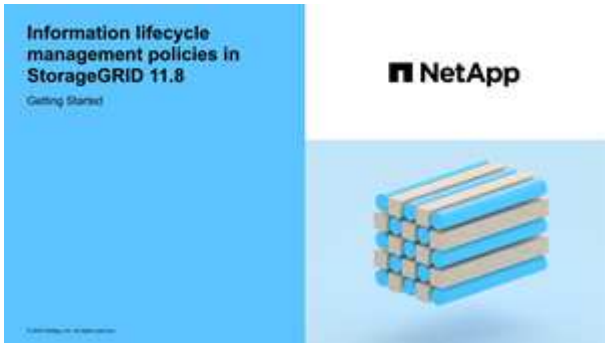
  S3-Objektsperre nicht aktiviert

  - Du hast"die ILM-Regeln erstellt" Sie der Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine Richtlinie speichern, zusätzliche Regeln erstellen und dann die Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
  - Du hast"eine Standard-ILM-Regel erstellt" das keine Filter enthält.

  S3-Objektsperre aktiviert

  - Der"Die globale S3-Objektsperreinstellung ist bereits aktiviert" für das StorageGRID -System.
  - Du hast"erstellte die konformen und nicht konformen ILM-Regeln" Sie der Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine Richtlinie speichern, zusätzliche Regeln erstellen und dann die Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
  - Du hast"eine Standard-ILM-Regel erstellt" für die konforme Richtlinie.

- Optional haben Sie das Video angesehen: "Video: Übersicht über ILM-Richtlinien"



Siehe auch "Verwenden von ILM-Richtlinien".

Schritte

1. Wählen Sie **ILM** > **Richtlinien**.

   Wenn die globale Einstellung „S3 Object Lock“ aktiviert ist, wird auf der Seite „ILM-Richtlinien“ angezeigt, welche ILM-Regeln konform sind.

2. Bestimmen Sie, wie Sie die ILM-Richtlinie erstellen möchten.

Neue Richtlinie erstellen

a. Wählen Sie **Richtlinie erstellen**.

Vorhandene Richtlinie klonen

a. Aktivieren Sie das Kontrollkästchen für die Richtlinie, mit der Sie beginnen möchten, und wählen Sie dann **Klonen** aus.

Vorhandene Richtlinie bearbeiten

a. Wenn eine Richtlinie inaktiv ist, können Sie sie bearbeiten. Aktivieren Sie das Kontrollkästchen für die inaktive Richtlinie, mit der Sie beginnen möchten, und wählen Sie dann **Bearbeiten** aus.

3. Geben Sie im Feld **Richtlinienname** einen eindeutigen Namen für die Richtlinie ein.
4. Geben Sie optional im Feld **Grund für die Änderung** den Grund für die Erstellung einer neuen Richtlinie ein.
5. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**. Wählen Sie einen Regelnamen aus, um die Einstellungen für diese Regel anzuzeigen.

   Wenn Sie eine Richtlinie klonen:

   - Die von der Richtlinie, die Sie klonen, verwendeten Regeln werden ausgewählt.
   - Wenn die Richtlinie, die Sie klonen, Regeln ohne Filter verwendet hat, die nicht die Standardregel waren, werden Sie aufgefordert, alle bis auf eine dieser Regeln zu entfernen.
   - Wenn die Standardregel einen Filter verwendet hat, werden Sie aufgefordert, eine neue Standardregel auszuwählen.
   - Wenn die Standardregel nicht die letzte Regel war, können Sie die Regel an das Ende der neuen Richtlinie verschieben.

S3-Objektsperre nicht aktiviert

a. Wählen Sie eine Standardregel für die Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite**.

   Die Standardregel gilt für alle Objekte, die keiner anderen Regel in der Richtlinie entsprechen. Die Standardregel kann keine Filter verwenden und wird immer zuletzt ausgewertet.

   > Verwenden Sie die Regel „2 Kopien erstellen“ nicht als Standardregel für eine Richtlinie. Die Regel „2 Kopien erstellen“ verwendet einen einzelnen Speicherpool, „Alle Speicherknoten“, der alle Sites enthält. Wenn Ihr StorageGRID -System über mehr als einen Standort verfügt, können zwei Kopien eines Objekts am selben Standort platziert werden.

S3-Objektsperre aktiviert

a. Wählen Sie eine Standardregel für die Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite**.

   Die Regelliste enthält nur die konformen Regeln und verwendet keine Filter.

   > Verwenden Sie die Regel „2 Kopien erstellen“ nicht als Standardregel für eine Richtlinie. Die Regel „2 Kopien erstellen“ verwendet einen einzelnen Speicherpool, „Alle Speicherknoten“, der alle Sites enthält. Wenn Sie diese Regel verwenden, können mehrere Kopien eines Objekts auf derselben Site platziert werden.

b. Wenn Sie eine andere „Standardregel“ für Objekte in nicht konformen S3-Buckets benötigen, wählen Sie **Eine Regel ohne Filter für nicht konforme S3-Buckets einschließen** und wählen Sie eine nicht konforme Regel aus, die keinen Filter verwendet.

   Beispielsweise möchten Sie möglicherweise einen Cloud-Speicherpool verwenden, um Objekte in Buckets zu speichern, für die S3 Object Lock nicht aktiviert ist.

   > Sie können nur eine nicht konforme Regel auswählen, die keinen Filter verwendet.

Siehe auch "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock".

6. Wenn Sie mit der Auswahl der Standardregel fertig sind, wählen Sie **Weiter**.
7. Wählen Sie im Schritt „Andere Regeln“ alle anderen Regeln aus, die Sie der Richtlinie hinzufügen möchten. Diese Regeln verwenden mindestens einen Filter (Mandantenkonto, Bucket-Name, erweiterter Filter oder die nicht aktuelle Referenzzeit). Wählen Sie dann **Auswählen**.

   Im Fenster „Richtlinie erstellen“ werden nun die von Ihnen ausgewählten Regeln aufgelistet. Die Standardregel steht am Ende, die anderen Regeln darüber.

   Wenn S3 Object Lock aktiviert ist und Sie auch eine nicht konforme „Standardregel“ ausgewählt haben, wird diese Regel als vorletzte Regel in der Richtlinie hinzugefügt.

Wenn eine Regel Objekte nicht für immer behält, wird eine Warnung angezeigt. Wenn Sie diese Richtlinie aktivieren, müssen Sie bestätigen, dass StorageGRID Objekte löschen soll, wenn die Platzierungsanweisungen für die Standardregel ablaufen (es sei denn, ein Bucket-Lebenszyklus behält die Objekte für einen längeren Zeitraum).

8. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln, um die Reihenfolge festzulegen, in der diese Regeln ausgewertet werden.

   Sie können die Standardregel nicht verschieben. Wenn die S3-Objektsperre aktiviert ist, können Sie die nicht konforme „Standard“-Regel auch nicht verschieben, falls eine solche ausgewählt wurde.

   Sie müssen bestätigen, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte von den Regeln in der aufgeführten Reihenfolge (von oben beginnend) ausgewertet.

9. Wählen Sie bei Bedarf **Regeln auswählen** aus, um Regeln hinzuzufügen oder zu entfernen.
10. Wenn Sie fertig sind, wählen Sie **Speichern**.
11. Wiederholen Sie diese Schritte, um weitere ILM-Richtlinien zu erstellen.
12. Simulieren einer ILM-Richtlinie . Sie sollten eine Richtlinie vor der Aktivierung immer simulieren, um sicherzustellen, dass sie wie erwartet funktioniert.

Simulieren einer Richtlinie

Simulieren Sie eine Richtlinie an Testobjekten, bevor Sie die Richtlinie aktivieren und auf Ihre Produktionsdaten anwenden.

Bevor Sie beginnen

- Sie kennen den S3-Bucket/Objektschlüssel für jedes Objekt, das Sie testen möchten.

Schritte

1. Mithilfe eines S3-Clients oder der"S3-Konsole" , nehmen Sie die zum Testen jeder Regel erforderlichen Objekte auf.
2. Aktivieren Sie auf der Seite „ILM-Richtlinien“ das Kontrollkästchen für die Richtlinie und wählen Sie dann **Simulieren** aus.
3. Geben Sie im Feld **Objekt** den S3 ein `bucket/object-key` für ein Testobjekt. Beispiel: `bucket-01/filename.png` .
4. Wenn die S3-Versionierung aktiviert ist, geben Sie optional eine Versions-ID für das Objekt in das Feld **Versions-ID** ein.
5. Wählen Sie **Simulieren**.
6. Bestätigen Sie im Abschnitt „Simulationsergebnisse“, dass jedes Objekt der richtigen Regel entspricht.
7. Um festzustellen, welcher Speicherpool oder welches Erasure-Coding-Profil wirksam ist, wählen Sie den Namen der übereinstimmenden Regel aus, um zur Seite mit den Regeldetails zu gelangen.

Überprüfen Sie alle Änderungen an der Platzierung vorhandener replizierter und löschcodierter Objekte. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Ergebnisse

Alle Änderungen an den Richtlinienregeln werden in den Simulationsergebnissen widergespiegelt und zeigen die neue und die vorherige Übereinstimmung an. Das Fenster „Richtlinie simulieren“ behält die von Ihnen getesteten Objekte bei, bis Sie entweder **Alle löschen** oder das Symbol „Entfernen“ auswählen ✕ für jedes Objekt in der Simulationsergebnisliste.

Ähnliche Informationen

"Beispielsimulationen für ILM-Richtlinien"

Aktivieren einer Richtlinie

Wenn Sie eine einzelne neue ILM-Richtlinie aktivieren, werden vorhandene und neu aufgenommene Objekte von dieser Richtlinie verwaltet. Wenn Sie mehrere Richtlinien aktivieren, bestimmen die den Buckets zugewiesenen ILM-Richtlinien-Tags die zu verwaltenden Objekte.

Bevor Sie eine neue Richtlinie aktivieren:

1. Simulieren Sie die Richtlinie, um zu bestätigen, dass sie sich wie erwartet verhält.
2. Überprüfen Sie alle Änderungen an der Platzierung vorhandener replizierter und löschcodierter Objekte. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

> ⚠ Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbarem Datenverlust führen.

Informationen zu diesem Vorgang

Wenn Sie eine ILM-Richtlinie aktivieren, verteilt das System die neue Richtlinie an alle Knoten. Allerdings wird die neue aktive Richtlinie möglicherweise erst wirksam, wenn alle Grid-Knoten für den Empfang der neuen Richtlinie verfügbar sind. In einigen Fällen wartet das System mit der Implementierung einer neuen aktiven Richtlinie, um sicherzustellen, dass Rasterobjekte nicht versehentlich entfernt werden. Speziell:

- Wenn Sie Richtlinienänderungen vornehmen, die **die Datenredundanz oder -haltbarkeit erhöhen**, werden diese Änderungen sofort implementiert. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Drei-Kopien-Regel anstelle einer Zwei-Kopien-Regel enthält, wird diese Richtlinie sofort implementiert, da sie die Datenredundanz erhöht.
- Wenn Sie Richtlinienänderungen vornehmen, die **die Datenredundanz oder -haltbarkeit verringern könnten**, werden diese Änderungen erst implementiert, wenn alle Grid-Knoten verfügbar sind. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Zwei-Kopien-Regel anstelle einer Drei-Kopien-Regel verwendet, wird die neue Richtlinie auf der Registerkarte „Aktive Richtlinie“ angezeigt, tritt jedoch erst in Kraft, wenn alle Knoten online und verfügbar sind.

Schritte

Befolgen Sie die Schritte zum Aktivieren einer oder mehrerer Richtlinien:

Aktivieren Sie eine Richtlinie

Befolgen Sie diese Schritte, wenn Sie nur eine aktive Richtlinie haben. Wenn Sie bereits über eine oder mehrere aktive Richtlinien verfügen und zusätzliche Richtlinien aktivieren, befolgen Sie die Schritte zum Aktivieren mehrerer Richtlinien.

1. Wenn Sie bereit sind, eine Richtlinie zu aktivieren, wählen Sie **ILM** > **Richtlinien**.

   Alternativ können Sie eine einzelne Richtlinie auf der Seite **ILM** > **Richtlinien-Tags** aktivieren.

2. Aktivieren Sie auf der Registerkarte „Richtlinien“ das Kontrollkästchen für die Richtlinie, die Sie aktivieren möchten, und wählen Sie dann „Aktivieren“ aus.
3. Führen Sie den entsprechenden Schritt aus:
   - Wenn Sie in einer Warnmeldung aufgefordert werden, die Aktivierung der Richtlinie zu bestätigen, wählen Sie **OK**.
   - Wenn eine Warnmeldung mit Details zur Richtlinie angezeigt wird:
     i. Überprüfen Sie die Details, um sicherzustellen, dass die Richtlinie die Daten wie erwartet verwaltet.
     ii. Wenn die Standardregel Objekte für eine begrenzte Anzahl von Tagen speichert, überprüfen Sie das Aufbewahrungsdiagramm und geben Sie diese Anzahl von Tagen in das Textfeld ein.
     iii. Wenn die Standardregel Objekte für immer speichert, eine oder mehrere andere Regeln jedoch eine begrenzte Aufbewahrungsdauer haben, geben Sie **Ja** in das Textfeld ein.
     iv. Wählen Sie **Richtlinie aktivieren**.

Mehrere Richtlinien aktivieren

Um mehrere Richtlinien zu aktivieren, müssen Sie Tags erstellen und jedem Tag eine Richtlinie zuweisen.

> Wenn mehrere Tags verwendet werden und Mandanten Richtlinien-Tags häufig Buckets neu zuweisen, kann dies die Grid-Leistung beeinträchtigen. Wenn Sie nicht vertrauenswürdige Mandanten haben, sollten Sie in Erwägung ziehen, nur das Standard-Tag zu verwenden.

1. Wählen Sie **ILM** > **Richtlinien-Tags**.
2. Wählen Sie **Erstellen**.
3. Geben Sie im Dialogfeld „Richtlinientag erstellen“ einen Tagnamen und optional eine Beschreibung für das Tag ein.

   > Tag-Namen und -Beschreibungen sind für Mieter sichtbar. Wählen Sie Werte aus, die den Mandanten dabei helfen, eine fundierte Entscheidung zu treffen, wenn sie Richtlinien-Tags auswählen, die sie ihren Buckets zuweisen möchten. Wenn die zugewiesene Richtlinie beispielsweise das Löschen von Objekten nach einer bestimmten Zeit vorsieht, können Sie dies in der Beschreibung mitteilen. Geben Sie in diese Felder keine vertraulichen Informationen ein.

4. Wählen Sie **Tag erstellen**.
5. Wählen Sie in der Tabelle mit den ILM-Richtlinien-Tags im Pulldown-Menü eine Richtlinie aus, die dem Tag zugewiesen werden soll.
6. Wenn in der Spalte „Richtlinieneinschränkungen“ Warnungen angezeigt werden, wählen Sie

Richtliniendetails anzeigen aus, um die Richtlinie zu überprüfen.

7. Stellen Sie sicher, dass jede Richtlinie die Daten wie erwartet verwaltet.
8. Wählen Sie **Zugewiesene Richtlinien aktivieren**. Oder wählen Sie **Änderungen löschen**, um die Richtlinienzuweisung zu entfernen.
9. Lesen Sie im Dialogfeld „Richtlinien mit neuen Tags aktivieren“ die Beschreibungen, wie die einzelnen Tags, Richtlinien und Regeln Objekte verwalten. Nehmen Sie die erforderlichen Änderungen vor, um sicherzustellen, dass die Richtlinien die Objekte wie erwartet verwalten.
10. Wenn Sie sicher sind, dass Sie die Richtlinien aktivieren möchten, geben Sie **Ja** in das Textfeld ein und wählen Sie dann **Richtlinien aktivieren**.

Ähnliche Informationen

"Beispiel 6: Ändern einer ILM-Richtlinie"

Beispielsimulationen für ILM-Richtlinien

Die Beispiele für ILM-Richtliniensimulationen bieten Richtlinien zum Strukturieren und Ändern von Simulationen für Ihre Umgebung.

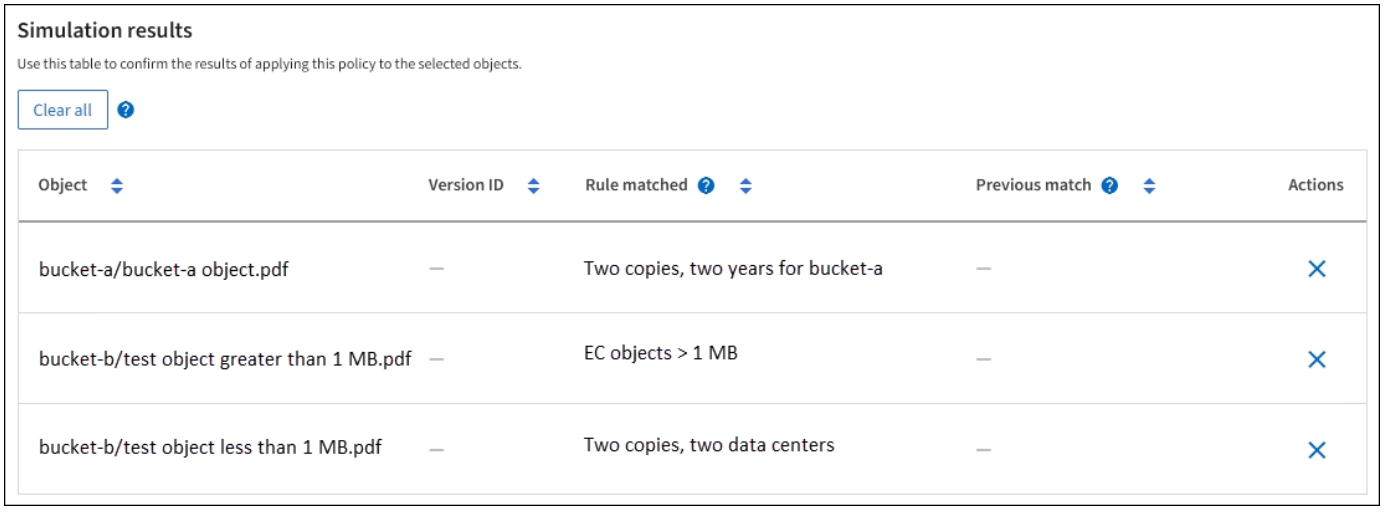
Beispiel 1: Regeln beim Simulieren einer ILM-Richtlinie überprüfen

In diesem Beispiel wird beschrieben, wie Regeln beim Simulieren einer Richtlinie überprüft werden.

In diesem Beispiel wird die **Beispiel-ILM-Richtlinie** anhand der aufgenommenen Objekte in zwei Buckets simuliert. Die Richtlinie umfasst die folgenden drei Regeln:

- Die erste Regel, **Zwei Kopien, zwei Jahre für Bucket-a**, gilt nur für Objekte in Bucket-a.
- Die zweite Regel, **EC-Objekte > 1 MB**, gilt für alle Buckets, filtert aber nach Objekten, die größer als 1 MB sind.
- Die dritte Regel, **Zwei Kopien, zwei Rechenzentren**, ist die Standardregel. Es enthält keine Filter und verwendet nicht die nicht aktuelle Referenzzeit.

Bestätigen Sie nach der Simulation der Richtlinie, dass jedes Objekt der richtigen Regel entspricht.



In diesem Beispiel:

- `bucket-a/bucket-a object.pdf`stimmte mit der ersten Regel überein, die nach Objekten filtert in `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf`ist in `bucket-b`, also entsprach es nicht der ersten Regel. Stattdessen wurde es von der zweiten Regel, die nach Objekten größer als 1 MB filtert, korrekt abgeglichen.
- `bucket-b/test object less than 1 MB.pdf`stimmte nicht mit den Filtern in den ersten beiden Regeln überein, daher wird es durch die Standardregel platziert, die keine Filter enthält.

Beispiel 2: Regeln beim Simulieren einer ILM-Richtlinie neu anordnen

Dieses Beispiel zeigt, wie Sie Regeln neu anordnen können, um die Ergebnisse beim Simulieren einer Richtlinie zu ändern.

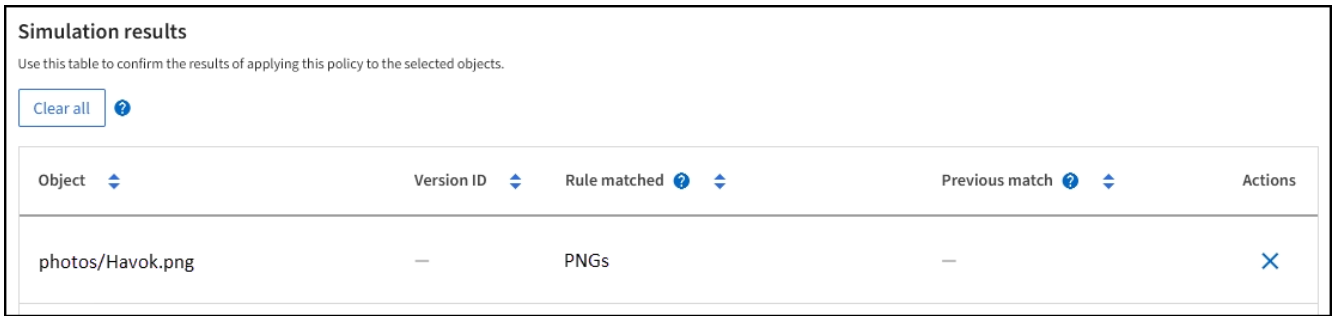
In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie, die zum Auffinden von Objekten mit den Benutzermetadaten „series=x-men“ dient, umfasst die folgenden drei Regeln:

- Die erste Regel, **PNGs**, filtert nach Schlüsselnamen, die auf enden `.png`.
- Die zweite Regel, **X-men**, gilt nur für Objekte für Mieter A und filtert nach `series=x-men` Benutzermetadaten.
- Die letzte Regel, **Zwei Kopien, zwei Rechenzentren**, ist die Standardregel, die auf alle Objekte zutrifft, die nicht den ersten beiden Regeln entsprechen.

Schritte

1. Nachdem Sie die Regeln hinzugefügt und die Richtlinie gespeichert haben, wählen Sie **Simulieren**.
2. Geben Sie im Feld **Objekt** den S3-Bucket/Objektschlüssel für ein Testobjekt ein und wählen Sie **Simulieren** aus.

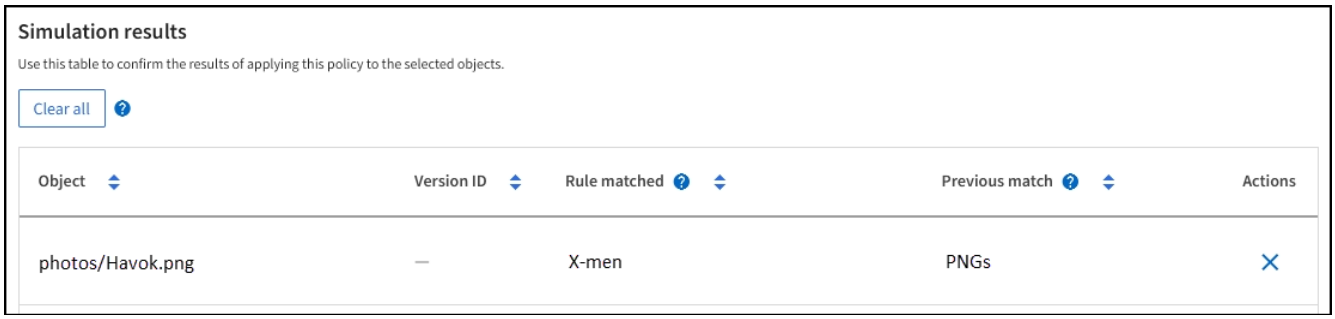
   Die Simulationsergebnisse werden angezeigt und zeigen, dass die `Havok.png` Das Objekt wurde mit der **PNGs**-Regel abgeglichen.

   Jedoch, `Havok.png` sollte die **X-Men**-Regel testen.

3. Um das Problem zu beheben, ordnen Sie die Regeln neu an.
   a. Wählen Sie **Fertig**, um das Fenster „ILM-Richtlinie simulieren“ zu schließen.
   b. Wählen Sie **Bearbeiten**, um die Richtlinie zu bearbeiten.
   c. Ziehen Sie die **X-Men**-Regel an den Anfang der Liste.
   d. Wählen Sie **Speichern**.
4. Wählen Sie **Simulieren**.

Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie erneut ausgewertet und die neuen Simulationsergebnisse werden angezeigt. Im Beispiel zeigt die Spalte Regelübereinstimmung, dass die `Havok.png` Das Objekt entspricht jetzt wie erwartet der X-Men-Metadatenregel. Die Spalte „Vorherige Übereinstimmung“ zeigt, dass die PNG-Regel mit dem Objekt in der vorherigen Simulation übereinstimmte.



Beispiel 3: Korrigieren einer Regel beim Simulieren einer ILM-Richtlinie

Dieses Beispiel zeigt, wie Sie eine Richtlinie simulieren, eine Regel in der Richtlinie korrigieren und die Simulation fortsetzen.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Mit dieser Richtlinie sollen Objekte gefunden werden, die `series=x-men` Benutzermetadaten. Allerdings kam es zu unerwarteten Ergebnissen bei der Simulation dieser Politik gegenüber der `Beast.jpg` Objekt. Anstatt der X-Men-Metadatenregel zu entsprechen, entsprach das Objekt der Standardregel „Zwei Kopien, zwei Rechenzentren“.

Wenn ein Testobjekt nicht mit der erwarteten Regel in der Richtlinie übereinstimmt, müssen Sie jede Regel in der Richtlinie prüfen und etwaige Fehler beheben.

Schritte

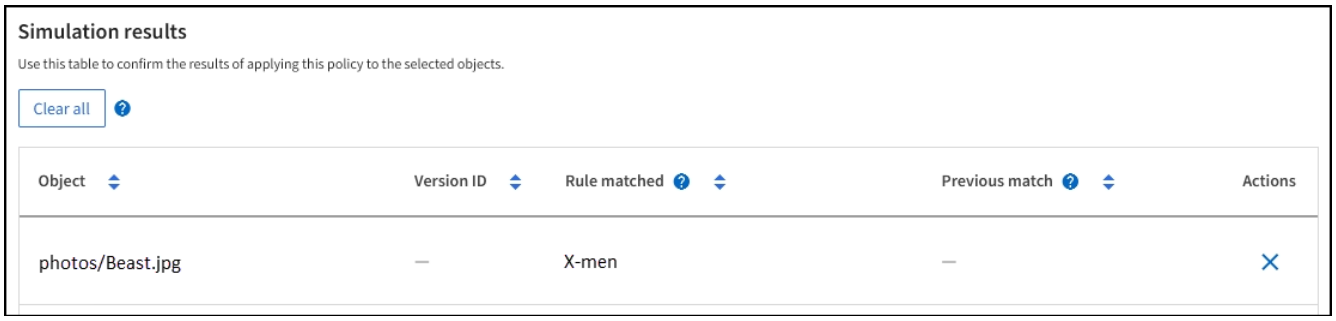
1. Wählen Sie **Fertig**, um das Dialogfeld „Richtlinie simulieren“ zu schließen. Wählen Sie auf der Detailseite der Richtlinie **Aufbewahrungsdiagramm** aus. Wählen Sie dann je nach Bedarf für jede Regel **Alle erweitern** oder **Details anzeigen** aus.
2. Überprüfen Sie das Mandantenkonto, die Referenzzeit und die Filterkriterien der Regel.

   Nehmen wir beispielsweise an, dass die Metadaten für die X-Men-Regel als „x-men01“ statt als „x-men“ eingegeben wurden.

3. Um den Fehler zu beheben, korrigieren Sie die Regel wie folgt:
   - Wenn die Regel Teil der Richtlinie ist, können Sie die Regel entweder klonen oder aus der Richtlinie entfernen und dann bearbeiten.
   - Wenn die Regel Teil der aktiven Richtlinie ist, müssen Sie die Regel klonen. Sie können eine Regel aus der aktiven Richtlinie weder bearbeiten noch entfernen.

4. Führen Sie die Simulation erneut durch.

   In diesem Beispiel entspricht die korrigierte X-Men-Regel nun der `Beast.jpg` Objekt basierend auf dem `series=x-men` Benutzermetadaten, wie erwartet.



Verwalten von ILM-Richtlinientags

Sie können Details zu ILM-Richtlinien-Tags anzeigen, ein Tag bearbeiten oder ein Tag entfernen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Anzeigen von ILM-Richtlinientagdetails

So zeigen Sie die Details für ein Tag an:

1. Wählen Sie **ILM** > **Richtlinien-Tags**.
2. Wählen Sie den Namen der Richtlinie aus der Tabelle aus. Die Detailseite für das Tag wird angezeigt.
3. Zeigen Sie auf der Detailseite den bisherigen Verlauf der zugewiesenen Richtlinien an.
4. Zeigen Sie eine Richtlinie an, indem Sie sie auswählen.

ILM-Richtlinientag bearbeiten

> Tag-Namen und -Beschreibungen sind für Mieter sichtbar. Wählen Sie Werte aus, die den Mandanten dabei helfen, eine fundierte Entscheidung zu treffen, wenn sie Richtlinien-Tags auswählen, die sie ihren Buckets zuweisen möchten. Wenn die zugewiesene Richtlinie beispielsweise das Löschen von Objekten nach einer bestimmten Zeit vorsieht, können Sie dies in der Beschreibung mitteilen. Geben Sie in diese Felder keine vertraulichen Informationen ein.

So bearbeiten Sie die Beschreibung für ein vorhandenes Tag:

1. Wählen Sie **ILM** > **Richtlinien-Tags**.
2. Aktivieren Sie das Kontrollkästchen für das Tag und wählen Sie dann **Bearbeiten**.

   Alternativ können Sie den Namen des Tags auswählen. Die Detailseite für das Tag wird angezeigt und Sie können auf dieser Seite **Bearbeiten** auswählen.

3. Ändern Sie die Tag-Beschreibung nach Bedarf

4. Wählen Sie **Speichern**.

ILM-Richtlinientag entfernen

Wenn Sie ein Richtlinien-Tag entfernen, wird auf alle Buckets, denen dieses Tag zugewiesen ist, die Standardrichtlinie angewendet.

So entfernen Sie ein Tag:

1. Wählen Sie **ILM** > **Richtlinien-Tags**.
2. Aktivieren Sie das Kontrollkästchen für das Tag und wählen Sie dann **Entfernen**. Ein Bestätigungsdialogfeld wird angezeigt.

   Alternativ können Sie den Namen des Tags auswählen. Die Detailseite für das Tag wird angezeigt und Sie können auf dieser Seite **Entfernen** auswählen.

3. Wählen Sie **Ja**, um das Tag zu löschen.

Überprüfen einer ILM-Richtlinie mit der Objektmetadatensuche

Nachdem Sie eine ILM-Richtlinie aktiviert haben, nehmen Sie repräsentative Testobjekte in das StorageGRID -System auf und führen Sie dann eine Objektmetadatensuche durch, um zu bestätigen, dass Kopien wie beabsichtigt erstellt und an den richtigen Speicherorten abgelegt werden.

Bevor Sie beginnen

Sie haben eine Objektkennung, die eine der folgenden sein kann: * **UUID**: Die universell eindeutige Kennung des Objekts. * **CBID**: Die eindeutige Kennung des Objekts innerhalb von StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in Großbuchstaben ein. * **S3-Bucket und Objektschlüssel**: Wenn ein Objekt über die S3-Schnittstelle aufgenommen wird, verwendet die Clientanwendung eine Kombination aus Bucket und Objektschlüssel, um das Objekt zu speichern und zu identifizieren. Wenn der S3-Bucket versioniert ist und Sie mithilfe des Bucket- und Objektschlüssels eine bestimmte Version eines S3-Objekts nachschlagen möchten, verfügen Sie über die **Versions-ID**.

Schritte

1. Nehmen Sie das Objekt auf.
2. Wählen Sie **ILM** > **Objektmetadatensuche**.
3. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein. Sie können eine UUID, CBID oder einen S3-Bucket/Objektschlüssel eingeben.
4. Geben Sie optional eine Versions-ID für das Objekt ein (nur S3).
5. Wählen Sie **Nachschlagen**.

   Die Ergebnisse der Objektmetadatensuche werden angezeigt. Auf dieser Seite sind die folgenden Arten von Informationen aufgeführt:

   - Systemmetadaten, wie Objekt-ID (UUID), Ergebnistyp (Objekt, Löschmarkierung, S3-Bucket) und logische Größe des Objekts. Weitere Einzelheiten finden Sie im Beispiel-Screenshot unten.
   - 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 eine Liste von Objektsegmenten einschließlich Segmentkennungen und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objektmetadaten im unverarbeiteten, internen Speicherformat. Diese Rohmetadaten umfassen interne Systemmetadaten, deren Beibehaltung von Version zu Version nicht garantiert ist.

6. Bestätigen Sie, dass das Objekt am richtigen Ort bzw. an den richtigen Orten gespeichert ist und dass es sich um den richtigen Kopietyp handelt.

   Wenn die Audit-Option aktiviert ist, können Sie das Audit-Protokoll auch auf die Meldung „ORLM-Objektregeln erfüllt“ überwachen. Die ORLM-Auditnachricht kann Ihnen weitere Informationen zum Status des ILM-Bewertungsprozesses liefern, sie kann Ihnen jedoch keine Informationen zur Richtigkeit der Platzierung der Objektdaten oder zur Vollständigkeit der ILM-Richtlinie geben. Dies müssen Sie selbst bewerten. Weitere Informationen finden Sie unter "Überprüfen der Überwachungsprotokolle" .

Das folgende Beispiel zeigt die Ergebnisse der Objektmetadatensuche für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

> Der folgende Screenshot ist ein Beispiel. Ihre Ergebnisse variieren je nach Ihrer StorageGRID Version.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Ähnliche Informationen

"Verwenden Sie die S3 REST-API"

Arbeiten mit ILM-Richtlinien und ILM-Regeln

Wenn sich Ihre Speicheranforderungen ändern, müssen Sie möglicherweise zusätzliche Richtlinien implementieren oder die mit einer Richtlinie verknüpften ILM-Regeln ändern. Sie können ILM-Metriken anzeigen, um die Systemleistung zu bestimmen.

Bevor Sie beginnen

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

ILM-Richtlinien anzeigen

So zeigen Sie aktive und inaktive ILM-Richtlinien und den Richtlinienaktivierungsverlauf an:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Wählen Sie **Richtlinien** aus, um eine Liste der aktiven und inaktiven Richtlinien anzuzeigen. In der Tabelle sind der Name jeder Richtlinie, die Tags, denen die Richtlinie zugewiesen ist, und die Angabe aufgeführt, ob die Richtlinie aktiv oder inaktiv ist.
3. Wählen Sie **Aktivierungsverlauf** aus, um eine Liste mit den Start- und Enddaten der Aktivierung für Richtlinien anzuzeigen.
4. Wählen Sie einen Richtliniennamen aus, um die Details der Richtlinie anzuzeigen.

> Wenn Sie die Details einer Richtlinie mit dem Status „Bearbeitet“ oder „Gelöscht“ anzeigen, wird eine Meldung angezeigt, die darauf hinweist, dass Sie die Version der Richtlinie anzeigen, die für den angegebenen Zeitraum aktiv war und seitdem bearbeitet oder gelöscht wurde.

Bearbeiten einer ILM-Richtlinie

Sie können nur eine inaktive Richtlinie bearbeiten. Wenn Sie eine aktive Richtlinie bearbeiten möchten, deaktivieren Sie sie oder erstellen Sie einen Klon und bearbeiten Sie den Klon.

So bearbeiten Sie eine Richtlinie:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Aktivieren Sie das Kontrollkästchen für die Richtlinie, die Sie bearbeiten möchten, und wählen Sie dann **Bearbeiten** aus.
3. Bearbeiten Sie die Richtlinie, indem Sie den Anweisungen in"Erstellen von ILM-Richtlinien" .
4. Simulieren Sie die Richtlinie, bevor Sie sie erneut aktivieren.

> Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Klonen einer ILM-Richtlinie

So klonen Sie eine ILM-Richtlinie:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Aktivieren Sie das Kontrollkästchen für die Richtlinie, die Sie klonen möchten, und wählen Sie dann **Klonen** aus.
3. Erstellen Sie eine neue Richtlinie, beginnend mit der Richtlinie, die Sie geklont haben, indem Sie den Anweisungen in"Erstellen von ILM-Richtlinien" .

> Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Entfernen einer ILM-Richtlinie

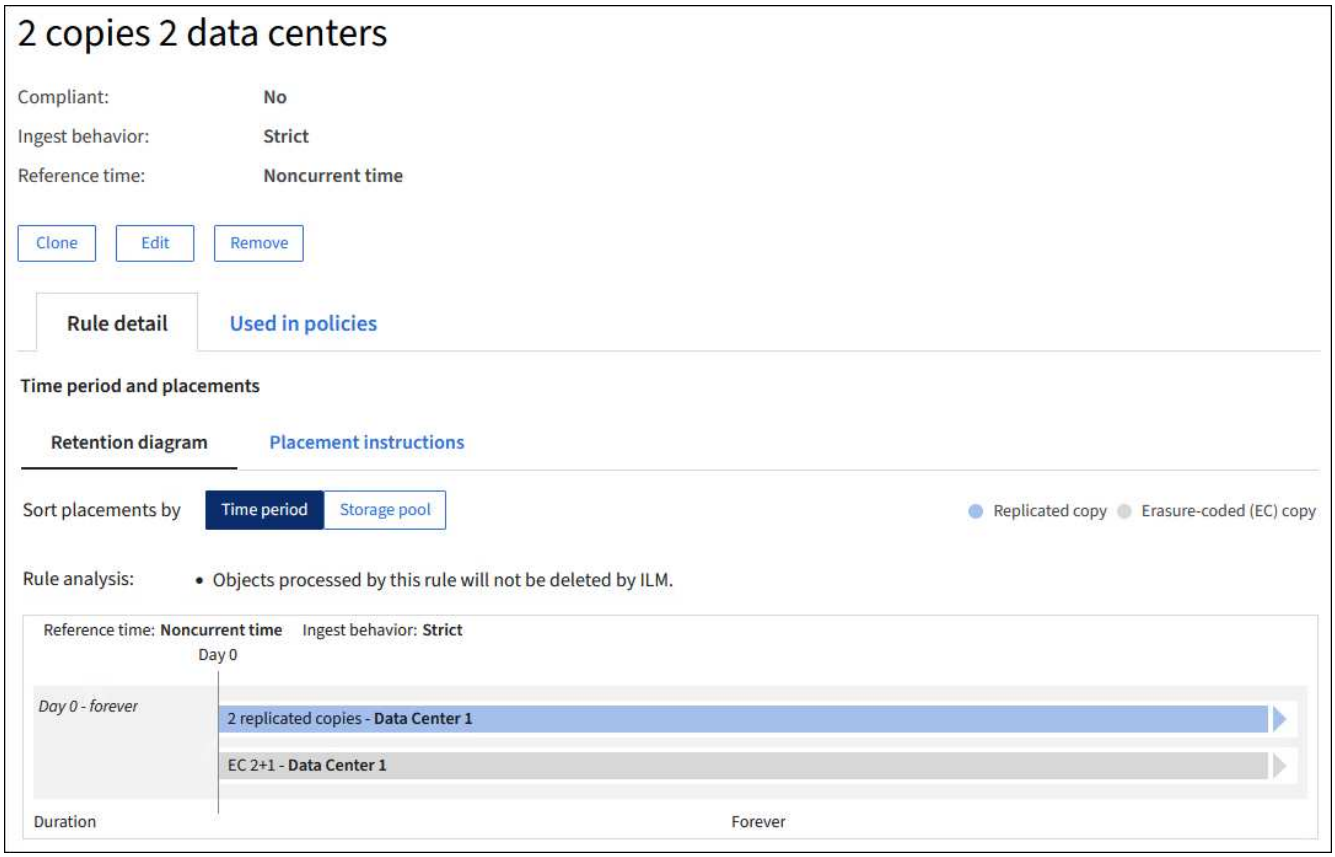
Sie können eine ILM-Richtlinie nur entfernen, wenn sie inaktiv ist. So entfernen Sie eine Richtlinie:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Aktivieren Sie das Kontrollkästchen für die inaktive Richtlinie, die Sie entfernen möchten.
3. Wählen Sie **Entfernen**.

Anzeigen von ILM-Regeldetails

So zeigen Sie die Details einer ILM-Regel an, einschließlich des Aufbewahrungsdiagramms und der Platzierungsanweisungen für die Regel:

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie den Namen der Regel aus, deren Details Sie anzeigen möchten. Beispiel:



Darüber hinaus können Sie auf der Detailseite eine Regel klonen, bearbeiten oder entfernen. Sie können eine Regel nicht bearbeiten oder entfernen, wenn sie in einer Richtlinie verwendet wird.

Klonen einer ILM-Regel

Sie können eine vorhandene Regel klonen, wenn Sie eine neue Regel erstellen möchten, die einige der Einstellungen der vorhandenen Regel verwendet. Wenn Sie eine Regel bearbeiten müssen, die in einer Richtlinie verwendet wird, klonen Sie stattdessen die Regel und nehmen Änderungen am Klon vor. Nachdem Sie Änderungen am Klon vorgenommen haben, können Sie die ursprüngliche Regel aus der Richtlinie entfernen und sie nach Bedarf durch die geänderte Version ersetzen.

Sie können eine ILM-Regel nicht klonen, wenn sie mit StorageGRID Version 10.2 oder früher erstellt wurde.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Aktivieren Sie das Kontrollkästchen für die Regel, die Sie klonen möchten, und wählen Sie dann **Klonen**. Alternativ können Sie den Regelnamen auswählen und dann auf der Seite mit den Regeldetails die Option **Klonen** auswählen.
3. Aktualisieren Sie die geklonte Regel, indem Sie die Schritte fürBearbeiten einer ILM-Regel Und"Verwenden erweiterter Filter in ILM-Regeln" .

   Beim Klonen einer ILM-Regel müssen Sie einen neuen Namen eingeben.

Bearbeiten einer ILM-Regel

Möglicherweise müssen Sie eine ILM-Regel bearbeiten, um einen Filter oder eine Platzierungsanweisung zu ändern.

Sie können eine Regel nicht bearbeiten, wenn sie in einer ILM-Richtlinie verwendet wird. Stattdessen können SieKlonen Sie die Regel und nehmen Sie alle erforderlichen Änderungen an der geklonten Kopie vor.

Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Vergewissern Sie sich, dass die Regel, die Sie bearbeiten möchten, in keiner ILM-Richtlinie verwendet wird.
3. Wenn die Regel, die Sie bearbeiten möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen für die Regel und wählen Sie **Aktionen** > **Bearbeiten**. Alternativ können Sie den Namen der Regel auswählen und dann auf der Seite mit den Regeldetails „Bearbeiten“ wählen.
4. Führen Sie die Schritte des Assistenten „ILM-Regel bearbeiten“ aus. Befolgen Sie bei Bedarf die Schritte für"Erstellen einer ILM-Regel" Und"Verwenden erweiterter Filter in ILM-Regeln" .

   Beim Bearbeiten einer ILM-Regel können Sie ihren Namen nicht ändern.

Entfernen einer ILM-Regel

Um die Liste der aktuellen ILM-Regeln übersichtlich zu halten, entfernen Sie alle ILM-Regeln, die Sie wahrscheinlich nicht verwenden werden.

Schritte

So entfernen Sie eine ILM-Regel, die derzeit in einer aktiven Richtlinie verwendet wird:

1. Klonen Sie die Richtlinie.
2. Entfernen Sie die ILM-Regel aus dem Richtlinienklon.

3. Speichern, simulieren und aktivieren Sie die neue Richtlinie, um sicherzustellen, dass Objekte wie erwartet geschützt sind.
4. Fahren Sie mit den Schritten zum Entfernen einer ILM-Regel fort, die derzeit in einer inaktiven Richtlinie verwendet wird.

So entfernen Sie eine ILM-Regel, die derzeit in einer inaktiven Richtlinie verwendet wird:

1. Wählen Sie die inaktive Richtlinie aus.
2. Entfernen Sie die ILM-Regel aus der Richtlinie oderEntfernen Sie die Richtlinie .
3. Fahren Sie mit den Schritten zum Entfernen einer ILM-Regel fort, die derzeit nicht verwendet wird.

So entfernen Sie eine ILM-Regel, die derzeit nicht verwendet wird:

1. Wählen Sie **ILM** > **Regeln**.
2. Bestätigen Sie, dass die Regel, die Sie entfernen möchten, in keiner Richtlinie verwendet wird.
3. Wenn die Regel, die Sie entfernen möchten, nicht verwendet wird, wählen Sie die Regel aus und wählen Sie **Aktionen** > **Entfernen**. Sie können mehrere Regeln auswählen und alle gleichzeitig entfernen.
4. Wählen Sie **Ja**, um zu bestätigen, dass Sie die ILM-Regel entfernen möchten.

Anzeigen von ILM-Metriken

Sie können Kennzahlen für ILM anzeigen, beispielsweise die Anzahl der Objekte in der Warteschlange und die Auswertungsrate. Sie können diese Metriken überwachen, um die Systemleistung zu bestimmen. Eine große Warteschlange oder Auswertungsrate kann darauf hinweisen, dass das System mit der Aufnahmerate nicht Schritt halten kann, die Belastung durch die Clientanwendungen zu hoch ist oder ein anormaler Zustand vorliegt.

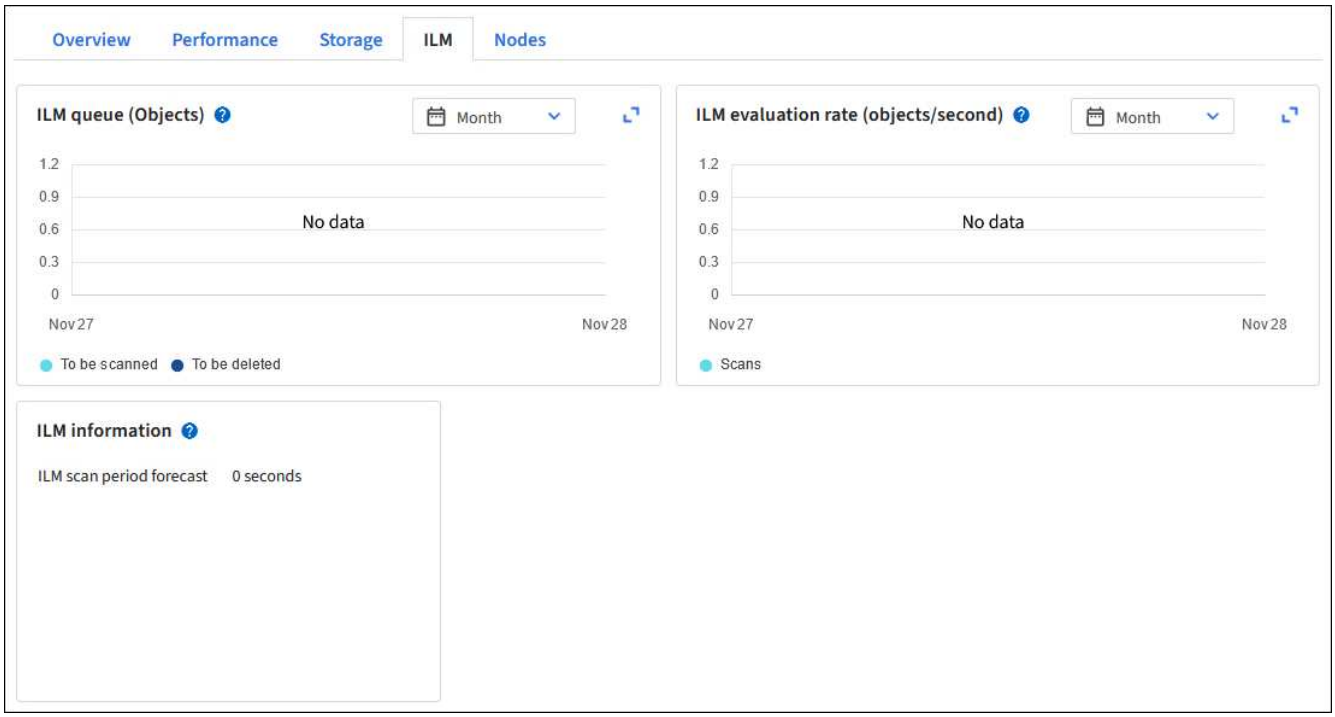
Schritte

1. Wählen Sie **Dashboard** > **ILM**.

   Da das Dashboard angepasst werden kann, ist die Registerkarte „ILM“ möglicherweise nicht verfügbar.

2. Überwachen Sie die Metriken auf der Registerkarte „ILM“.

   Sie können das Fragezeichen auswählen , um eine Beschreibung der Elemente auf der Registerkarte ILM anzuzeigen.



S3-Objektsperre verwenden

Verwalten von Objekten mit S3 Object Lock

Als Grid-Administrator können Sie S3 Object Lock für Ihr StorageGRID System aktivieren und eine konforme ILM-Richtlinie implementieren, um sicherzustellen, dass Objekte in bestimmten S3-Buckets für einen bestimmten Zeitraum nicht gelöscht oder überschrieben werden.

Was ist S3 Object Lock?

Die StorageGRID S3 Object Lock-Funktion ist eine Objektschutzlösung, die S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

Wenn die globale S3-Objektsperre-Einstellung für ein StorageGRID -System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn für einen Bucket die S3-Objektsperre aktiviert ist, ist eine Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Ein Bucket ohne S3-Objektsperre kann nur Objekte ohne angegebene Aufbewahrungseinstellungen enthalten. Für aufgenommene Objekte werden keine Aufbewahrungseinstellungen festgelegt.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen enthalten, die von S3-Clientanwendungen angegeben werden. Für einige aufgenommene Objekte gelten Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann hochgeladene Objekte mit angegebenen Aufbewahrungseinstellungen und neue Objekte ohne Aufbewahrungseinstellungen enthalten. Die neuen Objekte verwenden die Standardeinstellung, da die Aufbewahrungseinstellung nicht auf Objektebene konfiguriert wurde.

Tatsächlich verfügen alle neu aufgenommenen Objekte über Aufbewahrungseinstellungen, wenn die Standardaufbewahrung konfiguriert ist. Vorhandene Objekte ohne Objektaufbewahrungseinstellungen bleiben

davon unberührt.

Aufbewahrungsmodi

Die StorageGRID S3 Object Lock-Funktion unterstützt zwei Aufbewahrungsmodi, um unterschiedliche Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Aufbewahrungsmodi von Amazon S3.

- Im Compliance-Modus:
  - Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
  - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
  - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
  - Benutzer mit Sonderberechtigung können in Anfragen einen Bypass-Header verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
  - Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.
  - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mit der S3-Clientanwendung optional die folgenden Aufbewahrungseinstellungen für jedes dem Bucket hinzugefügte Objekt angeben:

- **Aufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Aufbewahrungsdatum**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Rechtliche Sperre**: Durch Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise müssen Sie möglicherweise ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht, rechtlich sperren. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie ausdrücklich aufgehoben wird. Rechtliche Sperren sind unabhängig vom Aufbewahrungsdatum.

  > Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

  Details zu den Objekteinstellungen finden Sie unter"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .

Standardaufbewahrungseinstellung für Buckets

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Standardaufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Standardaufbewahrungszeitraum**: Wie lange neue Objektversionen, die diesem Bucket hinzugefügt werden, ab dem Tag ihrer Hinzufügung aufbewahrt werden sollen.

Die Standard-Bucket-Einstellungen gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Vorhandene Bucket-Objekte sind nicht betroffen, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

Sehen"Erstellen eines S3-Buckets" Und"Standardaufbewahrung für S3 Object Lock aktualisieren" .

Vergleich von S3 Object Lock mit herkömmlicher Compliance

Die S3-Objektsperre ersetzt die Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war. Da die S3 Object Lock-Funktion den Anforderungen von Amazon S3 entspricht, wird die proprietäre StorageGRID Compliance-Funktion, die jetzt als „Legacy Compliance“ bezeichnet wird, dadurch verworfen.

> ⓘ Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung „S3 Object Lock“ automatisch aktiviert. Sie können StorageGRID weiterhin verwenden, um die Einstellungen vorhandener konformer Buckets zu verwalten. Sie können jedoch keine neuen konformen Buckets erstellen. Weitere Einzelheiten finden Sie unter "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5" .

Wenn Sie die alte Compliance-Funktion in einer früheren Version von StorageGRID verwendet haben, können Sie in der folgenden Tabelle nachlesen, wie sie im Vergleich zur S3 Object Lock-Funktion in StorageGRID abschneidet.

	S3-Objektsperre	**Compliance (alt)**
Wie wird die Funktion global aktiviert?	Wählen Sie im Grid Manager **KONFIGURATION** > **System** > **S3-Objektsperre**.	Wird nicht mehr unterstützt.
Wie wird die Funktion für einen Bucket aktiviert?	Benutzer müssen S3 Object Lock aktivieren, wenn sie mit dem Tenant Manager, der Tenant Management API oder der S3 REST API einen neuen Bucket erstellen.	Wird nicht mehr unterstützt.
Wird Bucket-Versionierung unterstützt?	Ja. Bucket-Versionierung ist erforderlich und wird automatisch aktiviert, wenn S3 Object Lock für den Bucket aktiviert ist.	NEIN.
Wie wird die Objektaufbewahrung eingestellt?	Benutzer können für jede Objektversion ein Aufbewahrungsdatum oder für jeden Bucket eine Standardaufbewahrungsdauer festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Die Aufbewahrungsfrist gilt für alle Objekte im Bucket.

	S3-Objektsperre	Compliance (alt)
Kann die Aufbewahrungsdauer geändert werden?	• Im Compliance-Modus kann das Aufbewahrungsdatum für eine Objektversion erhöht, aber nie verringert werden. • Im Governance-Modus können Benutzer mit Sonderberechtigungen die Aufbewahrungseinstellungen eines Objekts verringern oder sogar entfernen.	Die Aufbewahrungsdauer eines Buckets kann verlängert, aber niemals verkürzt werden.
Wo wird die rechtliche Aufbewahrung kontrolliert?	Benutzer können für jede Objektversion im Bucket eine rechtliche Sperre festlegen oder aufheben.	Für den Bucket wird eine rechtliche Sperre verhängt, die sich auf alle Objekte im Bucket auswirkt.
Wann können Objekte gelöscht werden?	• Im Compliance-Modus kann eine Objektversion nach Erreichen des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt unterliegt keiner rechtlichen Sperre. • Im Governance-Modus können Benutzer mit Sonderberechtigungen ein Objekt löschen, bevor das Aufbewahrungsdatum erreicht ist, vorausgesetzt, das Objekt unterliegt keiner rechtlichen Sperre.	Ein Objekt kann nach Ablauf der Aufbewahrungsfrist gelöscht werden, vorausgesetzt, der Bucket unterliegt keiner rechtlichen Sperre. Objekte können automatisch oder manuell gelöscht werden.
Wird die Bucket-Lebenszykluskonfiguration unterstützt?	Ja	Nein

S3 Object Lock-Aufgaben

Als Grid-Administrator müssen Sie sich eng mit den Mandantenbenutzern abstimmen, um sicherzustellen, dass die Objekte auf eine Weise geschützt werden, die ihren Aufbewahrungsanforderungen entspricht.

Das Anwenden von Mandanteneinstellungen im gesamten Grid kann je nach Netzwerkkonnektivität, Knotenstatus und Cassandra-Vorgängen 15 Minuten oder länger dauern.

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die allgemeinen Aufgaben zur Verwendung der S3 Object Lock-Funktion.

Grid-Administrator

- Aktivieren Sie die globale S3-Objektsperreinstellung für das gesamte StorageGRID System.
- Stellen Sie sicher, dass die Richtlinien für das Information Lifecycle Management (ILM) *konform* sind; das heißt, sie erfüllen die"Anforderungen an Buckets mit aktivierter S3-Objektsperre" .
- Erlauben Sie einem Mandanten bei Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungsdauer für einen Mandanten fest.

Mandantenbenutzer

- Überprüfen Sie die Überlegungen zu Buckets und Objekten mit S3 Object Lock.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3-Objektsperreinstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen Sie Buckets mit aktivierter S3-Objektsperre.
- Konfigurieren Sie optional die Standardaufbewahrungseinstellungen für einen Bucket:
  - Standardaufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Standardaufbewahrungszeitraum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.
- Verwenden Sie die S3-Clientanwendung, um Objekte hinzuzufügen und optional eine objektspezifische Aufbewahrung festzulegen:
  - Aufbewahrungsmodus. Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Aufbewahrungsdatum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.

Anforderungen für S3 Object Lock

Sie müssen die Anforderungen zum Aktivieren der globalen S3 Object Lock-Einstellung, die Anforderungen zum Erstellen konformer ILM-Regeln und ILM-Richtlinien sowie die Einschränkungen überprüfen, die StorageGRID für Buckets und Objekte auferlegt, die S3 Object Lock verwenden.

Voraussetzungen für die Verwendung der globalen S3 Object Lock-Einstellung

- Sie müssen die globale S3-Objektsperreinstellung mithilfe des Grid Managers oder der Grid Management API aktivieren, bevor ein S3-Mandant einen Bucket mit aktivierter S3-Objektsperre erstellen kann.
- Durch Aktivieren der globalen S3-Objektsperre können alle S3-Mandantenkonten Buckets mit aktivierter S3-Objektsperre erstellen.
- Nachdem Sie die globale S3-Objektsperreinstellung aktiviert haben, können Sie die Einstellung nicht mehr deaktivieren.
- Sie können die globale S3-Objektsperre nur aktivieren, wenn die Standardregel in allen aktiven ILM-Richtlinien *konform* ist (d. h., die Standardregel muss den Anforderungen von Buckets mit aktivierter S3-Objektsperre entsprechen).
- Wenn die globale Einstellung „S3-Objektsperre“ aktiviert ist, können Sie keine neue ILM-Richtlinie erstellen oder eine vorhandene ILM-Richtlinie aktivieren, es sei denn, die Standardregel in der Richtlinie ist konform. Nachdem die globale S3-Objektsperreinstellung aktiviert wurde, zeigen die Seiten mit den ILM-Regeln und ILM-Richtlinien an, welche ILM-Regeln konform sind.

Anforderungen an konforme ILM-Regeln

Wenn Sie die globale S3-Objektsperreinstellung aktivieren möchten, müssen Sie sicherstellen, dass die Standardregel in allen aktiven ILM-Richtlinien konform ist. Eine konforme Regel erfüllt die Anforderungen sowohl von Buckets mit aktivierter S3-Objektsperre als auch von allen vorhandenen Buckets mit aktivierter Legacy-Compliance:

- Es müssen mindestens zwei replizierte Objektkopien oder eine Erasure-Coded-Kopie erstellt werden.
- Diese Kopien müssen für die gesamte Dauer jeder Zeile in den Platzierungsanweisungen auf den Speicherknoten vorhanden sein.
- Objektkopien können nicht in einem Cloud-Speicherpool gespeichert werden.
- Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei **Aufnahmezeit** als Referenzzeit verwendet wird.
- Mindestens eine Zeile der Platzierungsanweisungen muss „für immer“ lauten.

Anforderungen für ILM-Richtlinien

Wenn die globale S3-Objektsperreinstellung aktiviert ist, können aktive und inaktive ILM-Richtlinien sowohl konforme als auch nicht konforme Regeln enthalten.

- Die Standardregel in einer aktiven oder inaktiven ILM-Richtlinie muss konform sein.
- Nicht konforme Regeln gelten nur für Objekte in Buckets, für die S3 Object Lock oder die alte Compliance-Funktion nicht aktiviert ist.
- Konforme Regeln können auf Objekte in jedem Bucket angewendet werden; S3 Object Lock oder Legacy Compliance müssen für den Bucket nicht aktiviert werden.

"Beispiel einer konformen ILM-Richtlinie für S3 Object Lock"

Anforderungen für Buckets mit aktivierter S3-Objektsperre

- Wenn die globale S3-Objektsperre-Einstellung für das StorageGRID -System aktiviert ist, können Sie den Tenant Manager, die Tenant Management API oder die S3 REST API verwenden, um Buckets mit aktivierter S3-Objektsperre zu erstellen.
- Wenn Sie S3 Object Lock verwenden möchten, müssen Sie S3 Object Lock beim Erstellen des Buckets aktivieren. Sie können S3 Object Lock nicht für einen vorhandenen Bucket aktivieren.
- Wenn S3 Object Lock für einen Bucket aktiviert ist, aktiviert StorageGRID automatisch die Versionierung für diesen Bucket. Sie können die S3-Objektsperre nicht deaktivieren oder die Versionsverwaltung für den Bucket aussetzen.
- Optional können Sie mithilfe des Tenant Managers, der Tenant Management API oder der S3 REST API einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer für jeden Bucket angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt werden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen überschreiben, indem Sie beim Hochladen für jede Objektversion einen Aufbewahrungsmodus und ein Aufbewahrungsdatum angeben.
- Die Bucket-Lebenszykluskonfiguration wird für Buckets mit aktivierter S3-Objektsperre unterstützt.
- Die CloudMirror-Replikation wird für Buckets mit aktivierter S3-Objektsperre nicht unterstützt.

Anforderungen für Objekte in Buckets mit aktivierter S3-Objektsperre

- Um eine Objektversion zu schützen, können Sie Standardaufbewahrungseinstellungen für den Bucket oder

Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mithilfe der S3-Clientanwendung oder der S3-REST-API angegeben werden.

- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl über eine Aufbewahrungsfrist als auch über eine gesetzliche Aufbewahrungsfrist verfügen, über eine der beiden Einstellungen, aber nicht über die andere, oder über keine von beiden. Durch die Angabe eines Aufbewahrungsdatums oder einer Einstellung für die rechtliche Aufbewahrung eines Objekts wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets mit aktivierter S3-Objektsperre

Jedes Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft die folgenden Phasen:

1. **Objektaufnahme**

   Wenn eine Objektversion zu einem Bucket hinzugefügt wird, für den die S3-Objektsperre aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

   - Wenn für das Objekt Aufbewahrungseinstellungen angegeben sind, werden die Einstellungen auf Objektebene angewendet. Alle Standard-Bucket-Einstellungen werden ignoriert.
   - Wenn für das Objekt keine Aufbewahrungseinstellungen angegeben sind, werden die Standard-Bucket-Einstellungen angewendet, sofern diese vorhanden sind.
   - Wenn für das Objekt oder den Bucket keine Aufbewahrungseinstellungen angegeben sind, ist das Objekt nicht durch S3 Object Lock geschützt.

   Wenn Aufbewahrungseinstellungen angewendet werden, sind sowohl das Objekt als auch alle benutzerdefinierten S3-Metadaten geschützt.

2. **Objektaufbewahrung und -löschung**

   Von jedem geschützten Objekt werden von StorageGRID mehrere Kopien für den angegebenen Aufbewahrungszeitraum gespeichert. Die genaue Anzahl und Art der Objektkopien sowie die Speicherorte werden durch die konformen Regeln in den aktiven ILM-Richtlinien bestimmt. Ob ein geschütztes Objekt vor Erreichen seines Aufbewahrungsdatums gelöscht werden kann, hängt von seinem Aufbewahrungsmodus ab.

   - Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

Ähnliche Informationen

- "Erstellen eines S3-Buckets"
- "Standardaufbewahrung für S3 Object Lock aktualisieren"
- "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
- "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

S3 Object Lock global aktivieren

Wenn ein S3-Mandantenkonto beim Speichern von Objektdaten gesetzliche Anforderungen erfüllen muss, müssen Sie S3 Object Lock für Ihr gesamtes StorageGRID System aktivieren. Durch Aktivieren der globalen S3 Object Lock-Einstellung kann jeder S3-Mandantenbenutzer Buckets und Objekte mit S3 Object Lock erstellen und verwalten.

Bevor Sie beginnen

- Sie haben die"Root-Zugriffsberechtigung" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben den S3 Object Lock-Workflow überprüft und verstehen die Überlegungen.
- Sie haben bestätigt, dass die Standardregel in der aktiven ILM-Richtlinie konform ist. Sehen"Erstellen einer ILM-Standardregel" für Details.

Informationen zu diesem Vorgang

Ein Grid-Administrator muss die globale S3-Objektsperreinstellung aktivieren, damit Mandantenbenutzer neue Buckets erstellen können, bei denen S3-Objektsperrung aktiviert ist. Nachdem diese Einstellung aktiviert wurde, kann sie nicht mehr deaktiviert werden.

Überprüfen Sie die Compliance-Einstellungen vorhandener Mandanten, nachdem Sie die globale S3-Objektsperreinstellung aktiviert haben. Wenn Sie diese Einstellung aktivieren, hängen die S3 Object Lock-Einstellungen pro Mandant von der StorageGRID Version zum Zeitpunkt der Mandantenerstellung ab.

> ⓘ Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung „S3 Object Lock“ automatisch aktiviert. Sie können StorageGRID weiterhin verwenden, um die Einstellungen vorhandener konformer Buckets zu verwalten. Sie können jedoch keine neuen konformen Buckets erstellen. Weitere Einzelheiten finden Sie unter "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5" .

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **S3-Objektsperre**.

   Die Seite „S3-Objektsperreinstellungen“ wird angezeigt.

2. Wählen Sie **S3-Objektsperre aktivieren**.
3. Wählen Sie **Übernehmen**.

   Ein Bestätigungsdialogfeld wird angezeigt und erinnert Sie daran, dass Sie S3 Object Lock nach der Aktivierung nicht mehr deaktivieren können.

4. Wenn Sie sicher sind, dass Sie S3 Object Lock dauerhaft für Ihr gesamtes System aktivieren möchten, wählen Sie **OK**.

   Wenn Sie **OK** auswählen:

   - Wenn die Standardregel in der aktiven ILM-Richtlinie konform ist, ist S3 Object Lock jetzt für das gesamte Grid aktiviert und kann nicht deaktiviert werden.
   - Wenn die Standardregel nicht konform ist, wird ein Fehler angezeigt. Sie müssen eine neue ILM-Richtlinie erstellen und aktivieren, die eine konforme Regel als Standardregel enthält. Wählen Sie **OK**. Erstellen Sie dann eine neue Richtlinie, simulieren Sie sie und aktivieren Sie sie. Sehen"ILM-Richtlinie erstellen" Anweisungen hierzu finden Sie unter.

Beheben Sie Konsistenzfehler beim Aktualisieren der S3 Object Lock- oder Legacy-Compliance-Konfiguration

Wenn ein Rechenzentrumsstandort oder mehrere Speicherknoten an einem Standort nicht mehr verfügbar sind, müssen Sie den S3-Tenant-Benutzern möglicherweise dabei

helfen, Änderungen an der S3-Objektsperre oder der alten Compliance-Konfiguration vorzunehmen.

Mandantenbenutzer, die Buckets mit aktivierter S3-Objektsperre (oder Legacy-Compliance) haben, können bestimmte Einstellungen ändern. Beispielsweise muss ein Mandantenbenutzer, der S3 Object Lock verwendet, möglicherweise eine Objektversion unter rechtliche Sperre stellen.

Wenn ein Mandantenbenutzer die Einstellungen für einen S3-Bucket oder eine Objektversion aktualisiert, versucht StorageGRID , die Bucket- oder Objektmetadaten im gesamten Grid sofort zu aktualisieren. Wenn das System die Metadaten nicht aktualisieren kann, weil ein Rechenzentrumsstandort oder mehrere Speicherknoten nicht verfügbar sind, gibt es einen Fehler zurück:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Um diesen Fehler zu beheben, führen Sie die folgenden Schritte aus:

1. Versuchen Sie, alle Speicherknoten oder Sites so schnell wie möglich wieder verfügbar zu machen.
2. Wenn Sie nicht in der Lage sind, an jedem Standort genügend Speicherknoten verfügbar zu machen, wenden Sie sich an den technischen Support. Dieser kann Ihnen bei der Wiederherstellung der Knoten helfen und sicherstellen, dass Änderungen im gesamten Grid konsistent angewendet werden.
3. Sobald das zugrunde liegende Problem behoben wurde, erinnern Sie den Mandantenbenutzer daran, seine Konfigurationsänderungen erneut zu versuchen.

Ähnliche Informationen

- "Verwenden eines Mandantenkontos"
- "Verwenden Sie die S3 REST-API"
- "Wiederherstellen und pflegen"

Beispiele für ILM-Regeln und -Richtlinien

Beispiel 1: ILM-Regeln und -Richtlinien für Objektspeicher

Sie können die folgenden Beispielregeln und -richtlinien als Ausgangspunkt verwenden, wenn Sie eine ILM-Richtlinie definieren, um Ihre Anforderungen an den Objektschutz und die Objektaufbewahrung zu erfüllen.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

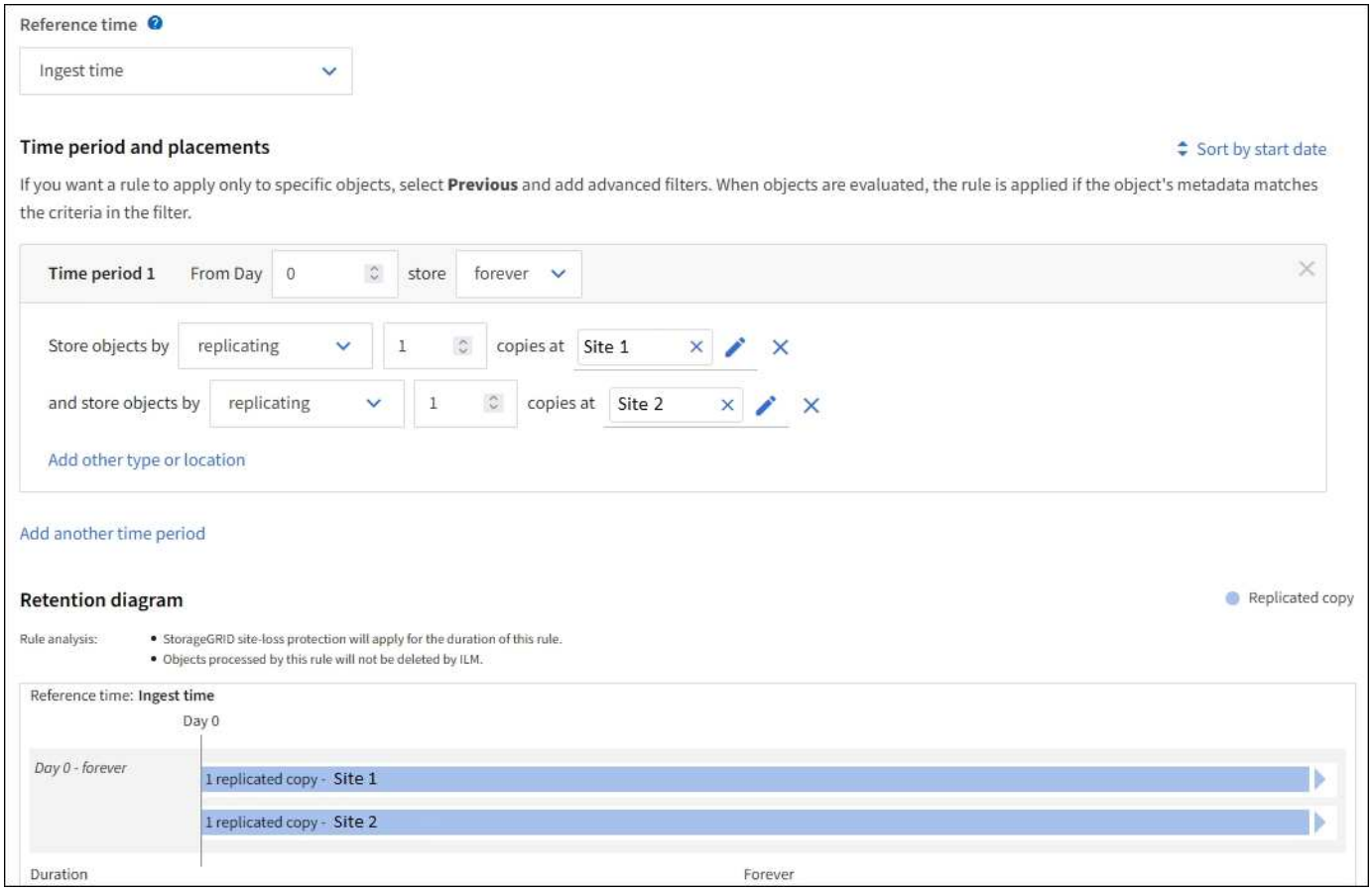
ILM-Regel 1 für Beispiel 1: Objektdaten auf zwei Sites kopieren

Diese beispielhafte ILM-Regel kopiert Objektdaten in Speicherpools an zwei Standorten.

Regeldefinition	Beispielwert
Speicherpools an einem Standort	Zwei Speicherpools, die jeweils unterschiedliche Sites enthalten, mit den Namen Site 1 und Site 2.
Regelname	Zwei Kopien, zwei Standorte
Referenzzeit	Aufnahmezeit
Platzierungen	Behalten Sie vom Tag 0 bis in alle Ewigkeit eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2.

Im Abschnitt „Regelanalyse“ des Retention-Diagramms heißt es:

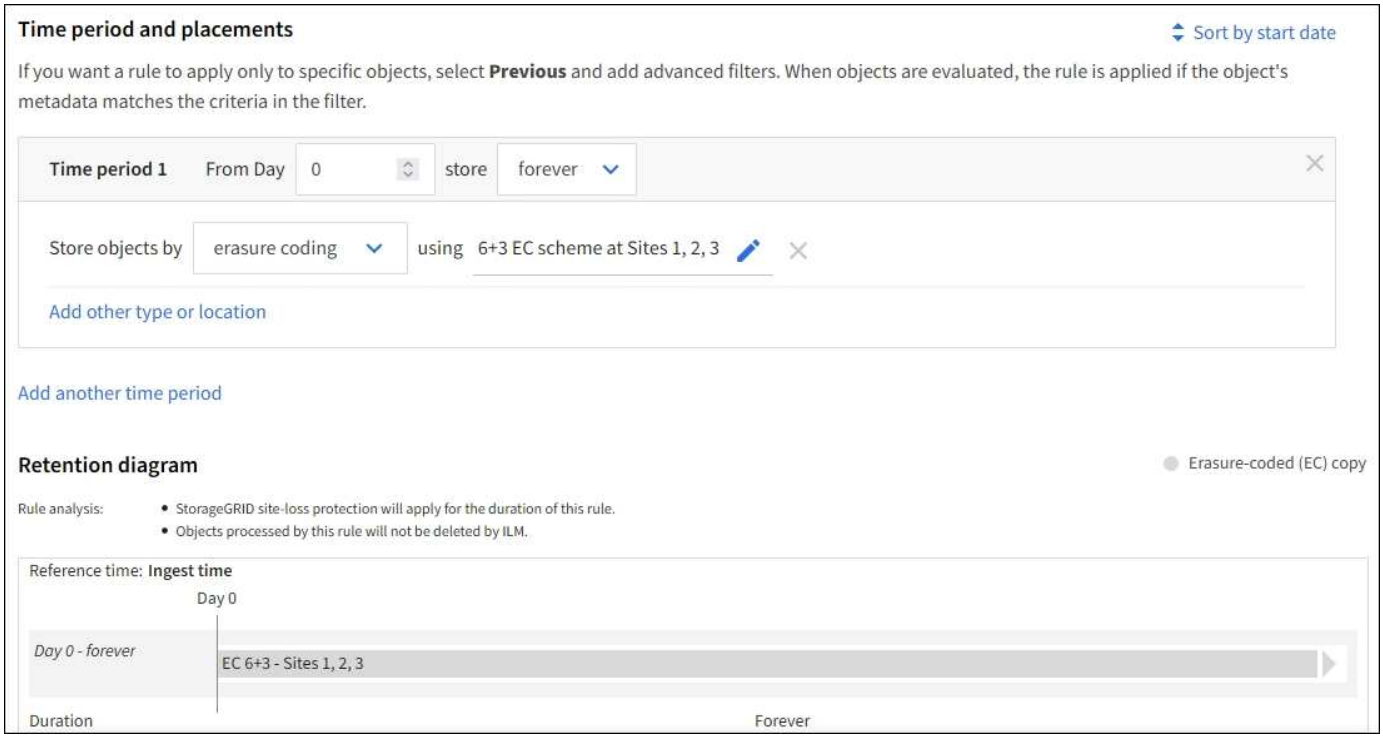
- Für die Dauer dieser Regelung gilt der Site-Loss-Schutz von StorageGRID .
- Von dieser Regel verarbeitete Objekte werden von ILM nicht gelöscht.



ILM-Regel 2 für Beispiel 1: Erasure-Coding-Profil mit Bucket-Matching

Dieses Beispiel einer ILM-Regel verwendet ein Erasure-Coding-Profil und einen S3-Bucket, um zu bestimmen, wo und wie lange das Objekt gespeichert wird.

Regeldefinition	Beispielwert
Speicherpool mit mehreren Standorten	• Ein Speicherpool an drei Standorten (Standorte 1, 2, 3) • Verwenden Sie das 6+3-Löschcodierungsschema
Regelname	S3 Bucket Finanzaufzeichnungen
Referenzzeit	Aufnahmezeit
Platzierungen	Erstellen Sie für Objekte im S3-Bucket mit dem Namen „finance-records“ eine Erasure-Coding-Kopie im Pool, der durch das Erasure-Coding-Profil angegeben ist. Bewahren Sie diese Kopie für immer auf.

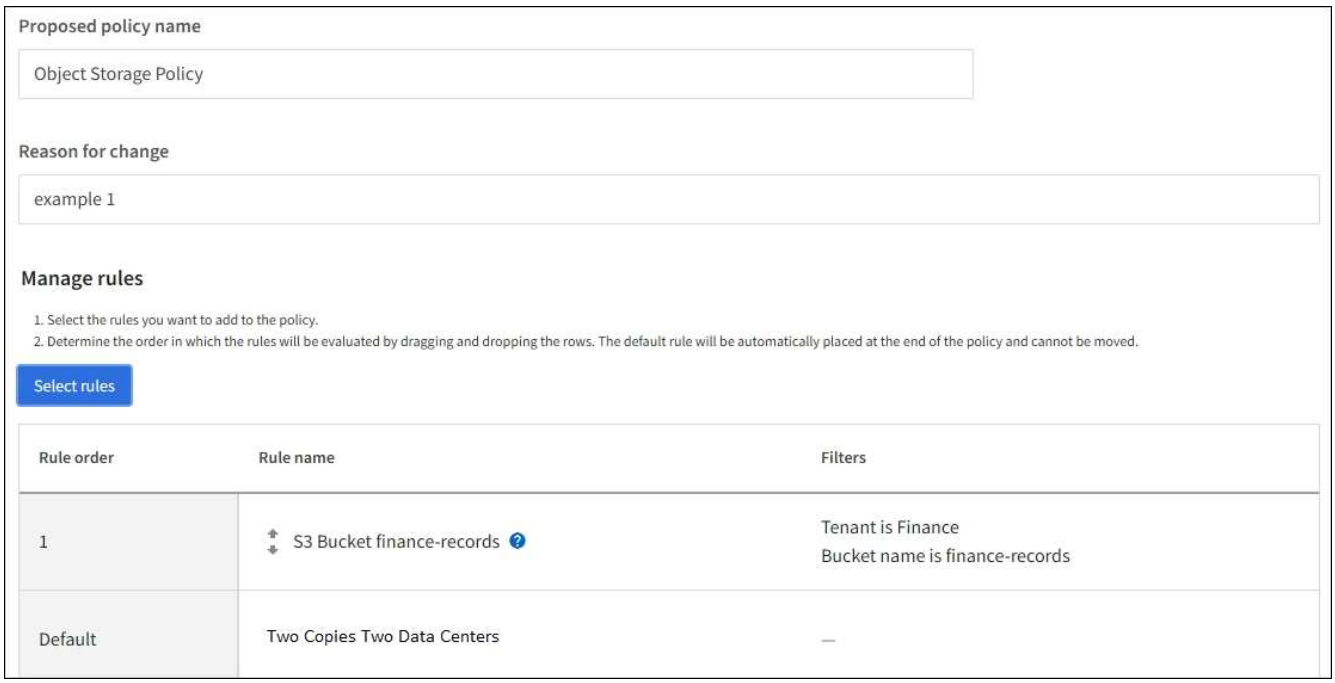


ILM-Richtlinie für Beispiel 1

In der Praxis sind die meisten ILM-Richtlinien einfach, obwohl das StorageGRID -System die Entwicklung anspruchsvoller und komplexer ILM-Richtlinien ermöglicht.

Eine typische ILM-Richtlinie für ein Grid mit mehreren Standorten könnte ILM-Regeln wie die folgenden enthalten:

- Speichern Sie beim Ingest alle Objekte, die zum S3-Bucket mit dem Namen gehören `finance-records` in einem Speicherpool, der drei Standorte enthält. Verwenden Sie 6+3-Löschcodierung.
- Wenn ein Objekt nicht der ersten ILM-Regel entspricht, verwenden Sie die ILM-Standardregel der Richtlinie „Zwei Kopien, zwei Rechenzentren“, um eine Kopie dieses Objekts an Standort 1 und eine Kopie an Standort 2 zu speichern.



Ähnliche Informationen

- "Verwenden von ILM-Richtlinien"
- "Erstellen von ILM-Richtlinien"

Beispiel 2: ILM-Regeln und -Richtlinien für die EC-Objektgrößenfilterung

Sie können die folgenden Beispielregeln und -richtlinien als Ausgangspunkt verwenden, um eine ILM-Richtlinie zu definieren, die nach Objektgröße filtert, um die empfohlenen EC-Anforderungen zu erfüllen.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

ILM-Regel 1 für Beispiel 2: Verwenden Sie EC für Objekte größer als 1 MB

Dieses Beispiel einer ILM-Regel löscht Codes für Objekte, die größer als 1 MB sind.

> Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

Regeldefinition	Beispielwert
Regelname	Nur EC-Objekte > 1 MB
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB

Regeldefinition	Beispielwert
Platzierungen	Erstellen Sie eine 2+1-Löschcodierte Kopie mit drei Standorten

ILM-Regel 2 für Beispiel 2: Zwei replizierte Kopien

Diese beispielhafte ILM-Regel erstellt zwei replizierte Kopien und filtert nicht nach Objektgröße. Diese Regel ist die Standardregel für die Richtlinie. Da die erste Regel alle Objekte herausfiltert, die größer als 1 MB sind, gilt diese Regel nur für Objekte, die 1 MB oder kleiner sind.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Keine
Platzierungen	Behalten Sie vom Tag 0 bis in alle Ewigkeit eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2.

ILM-Richtlinie für Beispiel 2: Verwenden Sie EC für Objekte größer als 1 MB

Dieses Beispiel einer ILM-Richtlinie enthält zwei ILM-Regeln:

- Die erste Regel löscht alle Objekte, die größer als 1 MB sind.
- Die zweite (Standard-)ILM-Regel erstellt zwei replizierte Kopien. Da Objekte, die größer als 1 MB sind, durch Regel 1 herausgefiltert wurden, gilt Regel 2 nur für Objekte, die 1 MB oder kleiner sind.

Beispiel 3: ILM-Regeln und -Richtlinien für besseren Schutz von Bilddateien

Mithilfe der folgenden Beispielregeln und -richtlinien können Sie sicherstellen, dass Bilder, die größer als 1 MB sind, mit einem Löschcode versehen werden und dass von kleineren Bildern zwei Kopien erstellt werden.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

ILM-Regel 1 für Beispiel 3: Verwenden Sie EC für Bilddateien größer als 1 MB

Dieses Beispiel einer ILM-Regel verwendet erweiterte Filterung, um den Code aller Bilddateien, die größer als 1 MB sind, zu löschen.

Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

Regeldefinition	Beispielwert
Regelname	EC-Bilddateien > 1 MB
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Erstellen Sie eine 2+1-Löschcodierte Kopie mit drei Standorten

Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Platzierungsanweisung für die Löschcodierung nur für JPG- und PNG-Dateien, die größer als 1 MB sind.

ILM-Regel 2 für Beispiel 3: Erstellen Sie 2 replizierte Kopien für alle verbleibenden Bilddateien

Dieses Beispiel einer ILM-Regel verwendet erweiterte Filterung, um anzugeben, dass kleinere Bilddateien repliziert werden. Da die erste Regel in der Richtlinie bereits Bilddateien mit einer Größe von über 1 MB zugeordnet hat, gilt diese Regel für Bilddateien mit einer Größe von 1 MB oder weniger.

Regeldefinition	Beispielwert
Regelname	2 Kopien für Bilddateien
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Erstellen Sie 2 replizierte Kopien in zwei Speicherpools

ILM-Richtlinie für Beispiel 3: Besserer Schutz für Bilddateien

Dieses Beispiel einer ILM-Richtlinie umfasst drei Regeln:

- Die erste Regel löscht alle Bilddateien, die größer als 1 MB sind.
- Die zweite Regel erstellt zwei Kopien aller verbleibenden Bilddateien (d. h. Bilder mit einer Größe von 1 MB oder weniger).
- Die Standardregel gilt für alle verbleibenden Objekte (d. h. alle Nicht-Bilddateien).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Beispiel 4: ILM-Regeln und -Richtlinien für versionierte S3-Objekte

Wenn Sie über einen S3-Bucket mit aktivierter Versionierung verfügen, können Sie die nicht aktuellen Objektversionen verwalten, indem Sie Regeln in Ihre ILM-Richtlinie aufnehmen, die „Nicht aktuelle Zeit“ als Referenzzeit verwenden.

> Wenn Sie für Objekte eine begrenzte Aufbewahrungsdauer angeben, werden diese Objekte nach Ablauf der Zeitspanne dauerhaft gelöscht. Stellen Sie sicher, dass Sie wissen, wie lange die Objekte aufbewahrt werden.

Wie dieses Beispiel zeigt, können Sie die von versionierten Objekten verwendete Speichermenge steuern, indem Sie für nicht aktuelle Objektversionen unterschiedliche Platzierungsanweisungen verwenden.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

Um eine ILM-Richtliniensimulation für eine nicht aktuelle Version eines Objekts durchzuführen, müssen Sie die UUID oder CBID der Objektversion kennen. Um die UUID und CBID zu finden, verwenden Sie"Objektmetadatensuche" solange das Objekt noch aktuell ist.

Ähnliche Informationen

"So werden Objekte gelöscht"

ILM-Regel 1 für Beispiel 4: Drei Kopien 10 Jahre lang aufbewahren

Diese beispielhafte ILM-Regel speichert eine Kopie jedes Objekts 10 Jahre lang an drei Standorten.

Diese Regel gilt für alle Objekte, unabhängig davon, ob sie versioniert sind oder nicht.

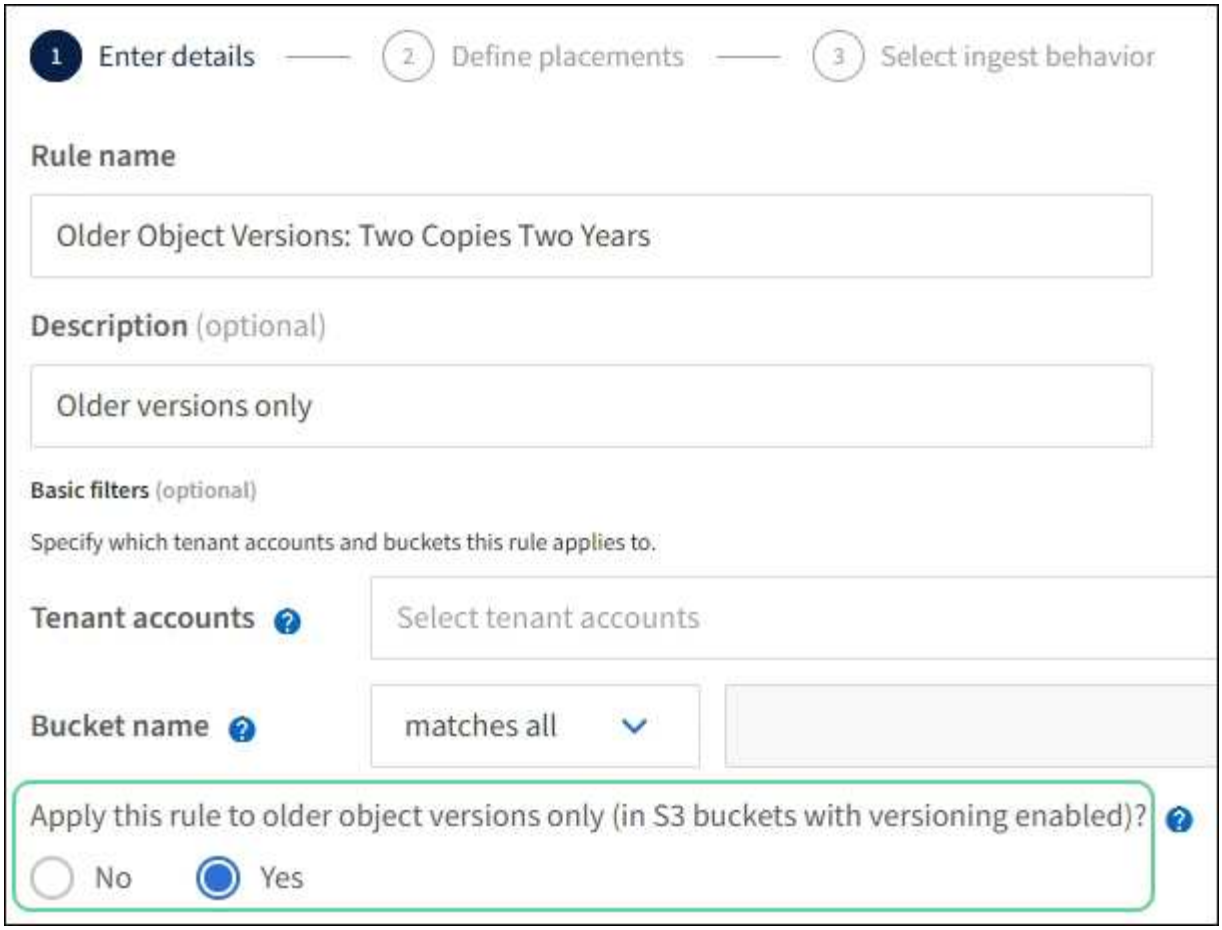
Regeldefinition	Beispielwert
Speicherpools	Drei Speicherpools, die jeweils aus unterschiedlichen Rechenzentren bestehen und als Site 1, Site 2 und Site 3 bezeichnet werden.
Regelname	Drei Kopien, zehn Jahre
Referenzzeit	Aufnahmezeit
Platzierungen	Bewahren Sie am Tag 0 drei replizierte Kopien 10 Jahre lang (3.652 Tage) auf, eine an Standort 1, eine an Standort 2 und eine an Standort 3. Löschen Sie nach 10 Jahren alle Kopien des Objekts.

ILM-Regel 2 für Beispiel 4: Zwei Kopien nicht aktueller Versionen für 2 Jahre aufbewahren

Dieses Beispiel einer ILM-Regel speichert zwei Kopien der nicht aktuellen Versionen eines versionierten S3-Objekts für zwei Jahre.

Da ILM-Regel 1 für alle Versionen des Objekts gilt, müssen Sie eine weitere Regel erstellen, um alle nicht aktuellen Versionen herauszufiltern.

Um eine Regel zu erstellen, die „Nicht aktuelle Zeit“ als Referenzzeit verwendet, wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ in Schritt 1 (Details eingeben) des Assistenten „ILM-Regel erstellen“. Wenn Sie **Ja** auswählen, wird automatisch *Nicht aktuelle Zeit* als Referenzzeit ausgewählt und Sie können keine andere Referenzzeit auswählen.



In diesem Beispiel werden nur zwei Kopien der nicht aktuellen Versionen gespeichert, und diese Kopien werden zwei Jahre lang gespeichert.

Regeldefinition	Beispielwert
Speicherpools	Zwei Speicherpools, jeweils in unterschiedlichen Rechenzentren, Standort 1 und Standort 2.
Regelname	Nicht aktuelle Versionen: Zwei Kopien, zwei Jahre
Referenzzeit	Nicht aktuelle Zeit Wird automatisch ausgewählt, wenn Sie im Assistenten „ILM-Regel erstellen“ bei der Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ **Ja** auswählen.
Platzierungen	Bewahren Sie am Tag 0 relativ zur nicht aktuellen Zeit (d. h. ab dem Tag, an dem die Objektversion zur nicht aktuellen Version wird) zwei replizierte Kopien der nicht aktuellen Objektversionen 2 Jahre (730 Tage) lang auf, eine an Standort 1 und eine an Standort 2. Löschen Sie nach zwei Jahren die nicht aktuellen Versionen.

ILM-Richtlinie für Beispiel 4: S3-versionierte Objekte

Wenn Sie ältere Versionen eines Objekts anders verwalten möchten als die aktuelle Version, müssen Regeln, die als Referenzzeit „Nicht aktuelle Zeit“ verwenden, in der ILM-Richtlinie vor Regeln erscheinen, die für die aktuelle Objektversion gelten.

Eine ILM-Richtlinie für versionierte S3-Objekte kann ILM-Regeln wie die folgenden enthalten:

- Bewahren Sie alle älteren (nicht aktuellen) Versionen jedes Objekts 2 Jahre lang auf, beginnend mit dem Tag, an dem die Version nicht mehr aktuell war.

> Die Regeln für „nicht aktuelle Zeit“ müssen in der Richtlinie vor den Regeln erscheinen, die für die aktuelle Objektversion gelten. Andernfalls werden die nicht aktuellen Objektversionen nie mit der Regel „Nicht aktuelle Zeit“ abgeglichen.

- Erstellen Sie beim Einlesen drei replizierte Kopien und speichern Sie an jedem der drei Standorte eine Kopie. Bewahren Sie Kopien der aktuellen Objektversion 10 Jahre lang auf.

Wenn Sie die Beispielrichtlinie simulieren, würden Sie erwarten, dass Testobjekte wie folgt ausgewertet werden:

- Alle nicht aktuellen Objektversionen würden mit der ersten Regel abgeglichen. Wenn eine nicht aktuelle Objektversion älter als 2 Jahre ist, wird sie von ILM dauerhaft gelöscht (alle Kopien der nicht aktuellen Version werden aus dem Grid entfernt).
- Die zweite Regel würde mit der aktuellen Objektversion übereinstimmen. Wenn die aktuelle Objektversion 10 Jahre lang gespeichert wurde, fügt der ILM-Prozess eine Löschmarkierung als aktuelle Version des Objekts hinzu und macht die vorherige Objektversion zu „nicht aktuell“. Bei der nächsten ILM-Auswertung wird diese nicht aktuelle Version mit der ersten Regel abgeglichen. Infolgedessen wird die Kopie an Standort 3 gelöscht und die beiden Kopien an Standort 1 und Standort 2 werden für weitere zwei Jahre gespeichert.

Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten

Sie können einen Standortfilter und das strikte Aufnahmeverhalten in einer Regel verwenden, um zu verhindern, dass Objekte an einem bestimmten Rechenzentrumsstandort gespeichert werden.

In diesem Beispiel möchte ein in Paris ansässiger Mieter einige Objekte aus rechtlichen Gründen nicht außerhalb der EU lagern. Andere Objekte, einschließlich aller Objekte aus anderen Mandantenkonten, können entweder im Pariser Rechenzentrum oder im US-Rechenzentrum gespeichert werden.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

Ähnliche Informationen

- "Aufnahmeoptionen"
- "ILM-Regel erstellen: Aufnahmeverhalten auswählen"

ILM-Regel 1 für Beispiel 5: Strikte Aufnahme zur Gewährleistung des Pariser Rechenzentrums

Dieses Beispiel einer ILM-Regel verwendet das strikte Aufnahmeverhalten, um zu gewährleisten, dass

Objekte, die von einem in Paris ansässigen Mandanten in S3-Buckets mit der auf die Region „eu-west-3“ (Paris) eingestellten Region gespeichert werden, niemals im US-Rechenzentrum gespeichert werden.

Diese Regel gilt für Objekte, die zum Pariser Mandanten gehören und deren S3-Bucket-Region auf eu-west-3 (Paris) eingestellt ist.

Regeldefinition	Beispielwert
Mieterkonto	Pariser Mieter
Erweiterter Filter	Standortbeschränkung entspricht eu-west-3
Speicherpools	Standort 1 (Paris)
Regelname	Strenge Aufnahme zur Gewährleistung des Pariser Rechenzentrums
Referenzzeit	Aufnahmezeit
Platzierungen	Behalten Sie am Tag 0 zwei replizierte Kopien für immer an Standort 1 (Paris).
Aufnahmeverhalten	Strikt. Verwenden Sie beim Aufnehmen immer die Platzierungen dieser Regel. Die Aufnahme schlägt fehl, wenn es nicht möglich ist, zwei Kopien des Objekts im Pariser Rechenzentrum zu speichern.

ILM-Regel 2 für Beispiel 5: Ausgewogene Aufnahme für andere Objekte

Dieses Beispiel einer ILM-Regel verwendet das ausgewogene Aufnahmeverhalten, um optimale ILM-Effizienz für alle Objekte bereitzustellen, die nicht der ersten Regel entsprechen. Von allen Objekten, die dieser Regel entsprechen, werden zwei Kopien gespeichert – eine im US-Rechenzentrum und eine im Pariser Rechenzentrum. Kann die Regel nicht sofort erfüllt werden, werden Zwischenkopien an einem beliebigen verfügbaren Ort gespeichert.

Diese Regel gilt für Objekte, die zu einem beliebigen Mandanten und einer beliebigen Region gehören.

Regeldefinition	Beispielwert
Mieterkonto	Ignorieren
Erweiterter Filter	*Nicht angegeben*
Speicherpools	Standort 1 (Paris) und Standort 2 (USA)
Regelname	2 Kopien 2 Rechenzentren
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Bewahren Sie am Tag 0 zwei replizierte Kopien für immer in zwei Rechenzentren auf
Aufnahmeverhalten	Ausgewogen. Objekte, die dieser Regel entsprechen, werden nach Möglichkeit entsprechend den Platzierungsanweisungen der Regel platziert. Andernfalls werden Zwischenkopien an jedem verfügbaren Ort erstellt.

ILM-Richtlinie für Beispiel 5: Kombinieren von Aufnahmeverhalten

Die beispielhafte ILM-Richtlinie umfasst zwei Regeln mit unterschiedlichem Aufnahmeverhalten.

Eine ILM-Richtlinie, die zwei verschiedene Aufnahmeverhalten verwendet, kann ILM-Regeln wie die folgenden enthalten:

- Speichern Sie Objekte, die zum Pariser Mandanten gehören und deren S3-Bucket-Region auf eu-west-3 (Paris) eingestellt ist, nur im Pariser Rechenzentrum. Die Aufnahme schlägt fehl, wenn das Pariser Rechenzentrum nicht verfügbar ist.
- Speichern Sie alle anderen Objekte (einschließlich derjenigen, die zum Pariser Mandanten gehören, aber eine andere Bucket-Region haben) sowohl im US-Rechenzentrum als auch im Pariser Rechenzentrum. Erstellen Sie Zwischenkopien an einem beliebigen verfügbaren Ort, wenn die Platzierungsanweisung nicht erfüllt werden kann.

Wenn Sie die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt ausgewertet werden:

- Alle Objekte, die zum Pariser Mandanten gehören und deren S3-Bucket-Region auf „eu-west-3“ eingestellt ist, werden mit der ersten Regel abgeglichen und im Pariser Rechenzentrum gespeichert. Da die erste Regel die strikte Aufnahme verwendet, werden diese Objekte nie im US-Rechenzentrum gespeichert. Wenn die Speicherknoten im Pariser Rechenzentrum nicht verfügbar sind, schlägt die Aufnahme fehl.
- Alle anderen Objekte werden mit der zweiten Regel abgeglichen, einschließlich der Objekte, die zum Paris-Mandanten gehören und bei denen die S3-Bucket-Region nicht auf „eu-west-3“ eingestellt ist. In jedem Rechenzentrum wird eine Kopie jedes Objekts gespeichert. Da die zweite Regel jedoch eine ausgewogene Aufnahme verwendet, werden bei Nichtverfügbarkeit eines Rechenzentrums zwei Zwischenkopien an einem beliebigen verfügbaren Standort gespeichert.

Beispiel 6: Ändern einer ILM-Richtlinie

Wenn Ihr Datenschutz geändert werden muss oder Sie neue Sites hinzufügen, können Sie eine neue ILM-Richtlinie erstellen und aktivieren.

Bevor Sie eine Richtlinie ändern, müssen Sie verstehen, wie sich Änderungen an ILM-Platzierungen vorübergehend auf die Gesamtleistung eines StorageGRID Systems auswirken können.

In diesem Beispiel wurde im Rahmen einer Erweiterung ein neuer StorageGRID Standort hinzugefügt und es muss eine neue aktive ILM-Richtlinie implementiert werden, um Daten am neuen Standort zu speichern. Um eine neue aktive Richtlinie zu implementieren, müssen Sie zunächst"Erstellen einer Richtlinie" . Anschließend müssen Sie"simulieren" und dann"aktivieren" die neue Richtlinie.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

Auswirkungen der Änderung einer ILM-Richtlinie auf die Leistung

Wenn Sie eine neue ILM-Richtlinie aktivieren, kann die Leistung Ihres StorageGRID -Systems vorübergehend beeinträchtigt werden, insbesondere wenn die Platzierungsanweisungen in der neuen Richtlinie erfordern, dass viele vorhandene Objekte an neue Speicherorte verschoben werden.

Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese zum Verwalten aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Überprüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und löschcodierter Objekte. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Um sicherzustellen, dass eine neue ILM-Richtlinie keinen Einfluss auf die Platzierung vorhandener replizierter und erasure-coded Objekte hat, können Sie"Erstellen Sie eine ILM-Regel mit einem Aufnahmezeitfilter" . Beispiel: **Aufnahmezeit *ist am oder nach <Datum und Uhrzeit>***, sodass die neue Regel nur für Objekte gilt, die am oder nach dem angegebenen Datum und der angegebenen Uhrzeit aufgenommen wurden.

Zu den Arten von ILM-Richtlinienänderungen, die die Leistung von StorageGRID vorübergehend beeinträchtigen können, gehören die folgenden:

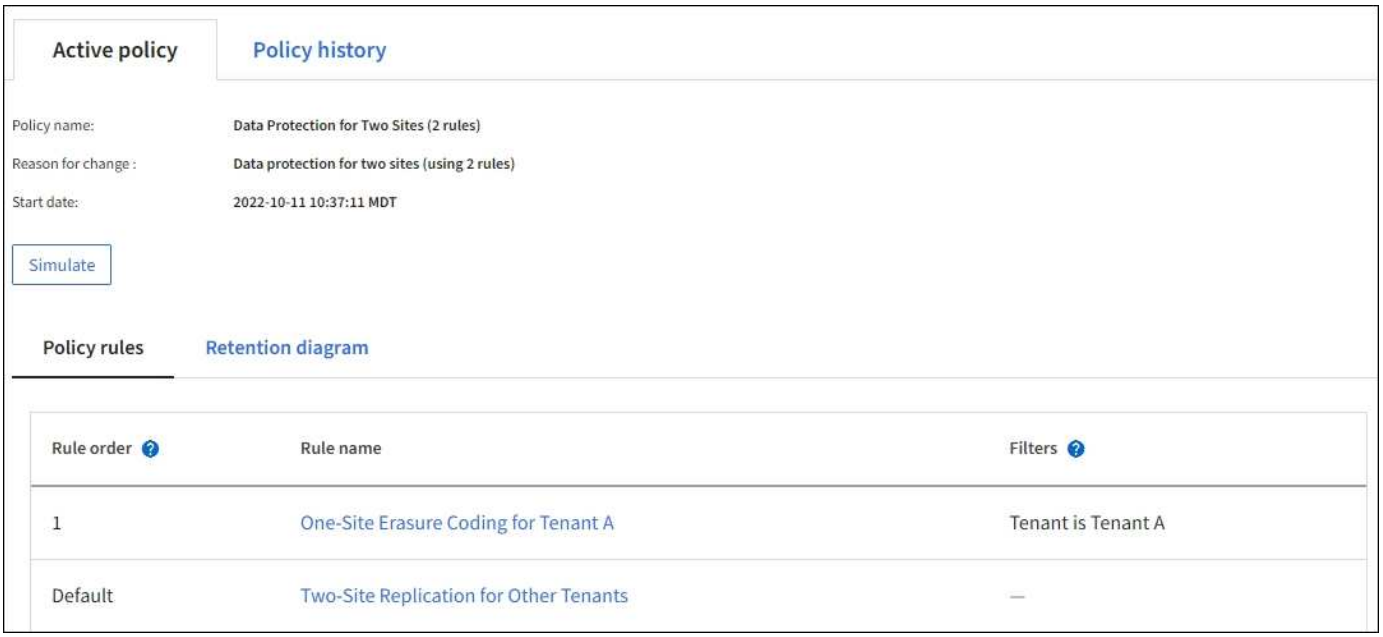
- Anwenden eines anderen Erasure-Coding-Profils auf vorhandene Erasure-Coding-Objekte.

  StorageGRID betrachtet jedes Erasure-Coding-Profil als einzigartig und verwendet Erasure-Coding-Fragmente nicht erneut, wenn ein neues Profil verwendet wird.

- Ändern des Typs der Kopien, die für vorhandene Objekte erforderlich sind. Beispielsweise das Konvertieren eines großen Prozentsatzes replizierter Objekte in Erasure-Coded-Objekte.
- Verschieben von Kopien vorhandener Objekte an einen völlig anderen Ort; beispielsweise das Verschieben einer großen Anzahl von Objekten in oder aus einem Cloud-Speicherpool oder zu oder von einem Remote-Standort.

Aktive ILM-Richtlinie für Beispiel 6: Datenschutz an zwei Standorten

In diesem Beispiel wurde die aktive ILM-Richtlinie ursprünglich für ein StorageGRID -System mit zwei Standorten entwickelt und verwendet zwei ILM-Regeln.



In dieser ILM-Richtlinie werden Objekte des Mandanten A durch 2+1-Löschcodierung an einem einzelnen Standort geschützt, während Objekte aller anderen Mandanten über zwei Standorte hinweg durch 2-Kopien-Replikation geschützt werden.

Regel 1: One-Site-Erasure-Coding für Mandant A

Regeldefinition	Beispielwert
Regelname	One-Site Erasure Coding für Mieter A
Mandantenkonto	Mieter A
Speicherpool	Standort 1
Platzierungen	2+1 Erasure Coding in Site 1 von Tag 0 bis für immer

Regel 2: Zwei-Site-Replikation für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Zwei-Site-Replikation für andere Mandanten
Mandantenkonto	Ignorieren
Speicherpools	Standort 1 und Standort 2
Platzierungen	Zwei replizierte Kopien vom Tag 0 bis in alle Ewigkeit: eine Kopie an Standort 1 und eine Kopie an Standort 2.

ILM-Richtlinie für Beispiel 6: Datenschutz an drei Standorten

In diesem Beispiel wird die ILM-Richtlinie durch eine neue Richtlinie für ein StorageGRID System mit drei Standorten ersetzt.

Nachdem der Grid-Administrator eine Erweiterung zum Hinzufügen der neuen Site durchgeführt hatte, erstellte er zwei neue Speicherpools: einen Speicherpool für Site 3 und einen Speicherpool, der alle drei Sites enthält (nicht derselbe wie der Standardspeicherpool „Alle Speicherknoten“). Anschließend erstellte der Administrator zwei neue ILM-Regeln und eine neue ILM-Richtlinie, die dem Schutz der Daten an allen drei Standorten dienen soll.

Wenn diese neue ILM-Richtlinie aktiviert wird, werden Objekte von Mandant A durch 2+1-Löschcodierung an drei Standorten geschützt, während Objekte anderer Mandanten (und kleinere Objekte von Mandant A) an drei Standorten durch 3-Kopien-Replikation geschützt werden.

Regel 1: Drei-Site-Löschcodierung für Mandant A

Regeldefinition	Beispielwert
Regelname	Drei-Site-Erasure-Coding für Mieter A
Mandantenkonto	Mieter A
Speicherpool	Alle 3 Standorte (einschließlich Standort 1, Standort 2 und Standort 3)
Platzierungen	2+1 Erasure Coding an allen 3 Standorten vom Tag 0 bis für immer

Regel 2: Drei-Standort-Replikation für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Drei-Site-Replikation für andere Mandanten
Mandantenkonto	Ignorieren
Speicherpools	Standort 1, Standort 2 und Standort 3
Platzierungen	Drei replizierte Kopien vom Tag 0 bis in alle Ewigkeit: eine Kopie an Standort 1, eine Kopie an Standort 2 und eine Kopie an Standort 3.

Aktivieren der ILM-Richtlinie für Beispiel 6

Wenn Sie eine neue ILM-Richtlinie aktivieren, werden vorhandene Objekte möglicherweise an neue Speicherorte verschoben oder es werden neue Objektkopien für vorhandene Objekte erstellt, basierend auf den Platzierungsanweisungen in neuen oder aktualisierten Regeln.

> Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbarem Datenverlust führen. Überprüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert.

Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese zum Verwalten aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Überprüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und löschcodierter Objekte. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Was passiert, wenn sich die Anweisungen zur Erasure-Codierung ändern?

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte des Mandanten A mithilfe von 2+1-Löschcodierung an Standort 1 geschützt. In der neuen ILM-Richtlinie werden Objekte des Mandanten A mithilfe von 2+1-Löschcodierung an den Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert wird, werden die folgenden ILM-Vorgänge ausgeführt:

- Neue, von Mandant A aufgenommene Objekte werden in zwei Datenfragmente aufgeteilt und ein Paritätsfragment wird hinzugefügt. Anschließend wird jedes der drei Fragmente an einem anderen Ort gespeichert.
- Die vorhandenen Objekte des Mandanten A werden während des laufenden ILM-Scan-Prozesses neu ausgewertet. Da die ILM-Platzierungsanweisungen ein neues Erasure-Coding-Profil verwenden, werden völlig neue Erasure-Coding-Fragmente erstellt und an die drei Standorte verteilt.

Die vorhandenen 2+1-Fragmente an Standort 1 werden nicht wiederverwendet. StorageGRID betrachtet jedes Erasure-Coding-Profil als einzigartig und verwendet Erasure-Coding-Fragmente nicht erneut, wenn ein neues Profil verwendet wird.

Was passiert, wenn sich Replikationsanweisungen ändern?

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte anderer Mandanten mithilfe von zwei replizierten Kopien in Speicherpools an den Standorten 1 und 2 geschützt. In der neuen ILM-Richtlinie werden Objekte anderer Mandanten mithilfe von drei replizierten Kopien in Speicherpools an den Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert wird, werden die folgenden ILM-Vorgänge ausgeführt:

- Wenn ein anderer Mandant als Mandant A ein neues Objekt aufnimmt, erstellt StorageGRID drei Kopien und speichert an jedem Standort eine Kopie.
- Vorhandene Objekte dieser anderen Mandanten werden während des laufenden ILM-Scanvorgangs neu bewertet. Da die vorhandenen Objektkopien an Standort 1 und Standort 2 weiterhin die Replikationsanforderungen der neuen ILM-Regel erfüllen, muss StorageGRID nur eine neue Kopie des Objekts für Standort 3 erstellen.

Auswirkungen der Aktivierung dieser Richtlinie auf die Leistung

Wenn die ILM-Richtlinie in diesem Beispiel aktiviert wird, wird die Gesamtleistung dieses StorageGRID Systems vorübergehend beeinträchtigt. Es werden mehr Grid-Ressourcen als üblich benötigt, um neue Erasure-Code-Fragmente für die vorhandenen Objekte von Mandant A und neue replizierte Kopien an Standort 3 für die vorhandenen Objekte anderer Mandanten zu erstellen.

Aufgrund der Änderung der ILM-Richtlinie kann es bei Lese- und Schreibanforderungen des Clients vorübergehend zu höheren Latenzen als normal kommen. Die Latenzen werden wieder auf ein normales Niveau zurückkehren, nachdem die Platzierungsanweisungen im gesamten Raster vollständig implementiert

wurden.

Um Ressourcenprobleme beim Aktivieren einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter „Aufnahmezeit“ in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie die Aufnahmezeit so fest, dass sie größer oder gleich der ungefähren Zeit ist, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.

> Wenden Sie sich an den technischen Support, wenn Sie die Geschwindigkeit, mit der Objekte nach einer Änderung der ILM-Richtlinie verarbeitet werden, verlangsamen oder erhöhen müssen.

Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock

Sie können den S3-Bucket, die ILM-Regeln und die ILM-Richtlinie in diesem Beispiel als Ausgangspunkt verwenden, wenn Sie eine ILM-Richtlinie definieren, um die Objektschutz- und Aufbewahrungsanforderungen für Objekte in Buckets mit aktivierter S3-Objektsperre zu erfüllen.

> Wenn Sie die alte Compliance-Funktion in früheren StorageGRID Versionen verwendet haben, können Sie dieses Beispiel auch zur Verwaltung aller vorhandenen Buckets verwenden, bei denen die alte Compliance-Funktion aktiviert ist.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

Ähnliche Informationen

- "Verwalten von Objekten mit S3 Object Lock"
- "Erstellen einer ILM-Richtlinie"

Bucket und Objekte für S3 Object Lock-Beispiel

In diesem Beispiel hat ein S3-Mandantenkonto mit dem Namen Bank of ABC den Mandantenmanager verwendet, um einen Bucket mit aktivierter S3-Objektsperre zum Speichern wichtiger Bankdaten zu erstellen.

Bucket-Definition	Beispielwert
Mandantenkontoname	Bank von ABC
Bucket-Name	Bankunterlagen
Bucket-Region	us-east-1 (Standard)

Jedes Objekt und jede Objektversion, die zum Bucket „Bankunterlagen“ hinzugefügt wird, verwendet die folgenden Werte für `retain-until-date` Und `legal hold` Einstellungen.

Einstellung für jedes Objekt	Beispielwert
`retain-until-date`	"2030-12-30T23:59:59Z" (30. Dezember 2030) Jede Objektversion hat ihre eigene `retain-until-date` Einstellung. Diese Einstellung kann erhöht, aber nicht verringert werden.
`legal hold`	„AUS“ (Nicht wirksam) Eine rechtliche Sperre kann für jede Objektversion jederzeit während der Aufbewahrungsfrist verhängt oder aufgehoben werden. Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann das Objekt nicht gelöscht werden, auch wenn `retain-until-date` erreicht ist.

ILM-Regel 1 für S3 Object Lock-Beispiel: Erasure-Coding-Profil mit Bucket-Matching

Diese beispielhafte ILM-Regel gilt nur für das S3-Mandantenkonto mit dem Namen Bank of ABC. Es passt zu jedem Objekt in der `bank-records` Bucket und verwendet dann Erasure Coding, um das Objekt auf Speicherknoten an drei Rechenzentrumsstandorten unter Verwendung eines 6+3-Erasure-Coding-Profils zu speichern. Diese Regel erfüllt die Anforderungen von Buckets mit aktivierter S3-Objektsperre: Eine Kopie wird vom Tag 0 bis in alle Ewigkeit auf den Speicherknoten aufbewahrt, wobei die Aufnahmezeit als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte im Bankaufzeichnungs-Bucket – Bank of ABC
Mandantenkonto	Bank von ABC
Bucket-Name	`bank-records`
Erweiterter Filter	Objektgröße (MB) größer als 1 **Hinweis:** Dieser Filter stellt sicher, dass Erasure Coding nicht für Objekte mit 1 MB oder weniger verwendet wird.

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Ab Tag 0 für immer speichern
Erasure-Coding-Profil	• Erstellen Sie eine Löschcodierte Kopie auf Speicherknoten an drei Rechenzentrumsstandorten • Verwendet das 6+3-Erasure-Coding-Schema

ILM-Regel 2 für S3 Object Lock-Beispiel: Nicht konforme Regel

Diese beispielhafte ILM-Regel speichert zunächst zwei replizierte Objektkopien auf Speicherknoten. Nach einem Jahr wird eine Kopie dauerhaft in einem Cloud-Speicherpool gespeichert. Da diese Regel einen Cloud-Speicherpool verwendet, ist sie nicht konform und gilt nicht für Objekte in Buckets mit aktivierter S3-Objektsperre.

Regeldefinition	Beispielwert
Regelname	Nicht konforme Regel: Cloud-Speicherpool verwenden
Mandantenkonten	Nicht angegeben
Bucket-Name	Nicht angegeben, gilt aber nur für Buckets, bei denen S3 Object Lock (oder die alte Compliance-Funktion) nicht aktiviert ist.
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	• Bewahren Sie am Tag 0 zwei replizierte Kopien auf Speicherknoten in Rechenzentrum 1 und Rechenzentrum 2 für 365 Tage auf • Behalten Sie nach einem Jahr eine replizierte Kopie für immer in einem Cloud-Speicherpool

ILM-Regel 3 für S3 Object Lock-Beispiel: Standardregel

Diese beispielhafte ILM-Regel kopiert Objektdaten in Speicherpools in zwei Rechenzentren. Diese konforme Regel ist als Standardregel in der ILM-Richtlinie konzipiert. Es enthält keine Filter, verwendet nicht die nicht aktuelle Referenzzeit und erfüllt die Anforderungen von Buckets mit aktivierter S3-Objektsperre: Zwei Objektkopien werden von Tag 0 bis auf unbestimmte Zeit auf Speicherknoten aufbewahrt, wobei Ingest als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Standardkonforme Regel: Zwei Kopien, zwei Rechenzentren
Mieterkonto	Nicht angegeben
Bucket-Name	Nicht angegeben
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Bewahren Sie von Tag 0 bis in alle Ewigkeit zwei replizierte Kopien auf – eine auf Speicherknoten in Rechenzentrum 1 und eine auf Speicherknoten in Rechenzentrum 2.

Konforme ILM-Richtlinie für S3 Object Lock-Beispiel

Um eine ILM-Richtlinie zu erstellen, die alle Objekte in Ihrem System wirksam schützt, einschließlich der Objekte in Buckets mit aktivierter S3-Objektsperre, müssen Sie ILM-Regeln auswählen, die die Speicheranforderungen für alle Objekte erfüllen. Anschließend müssen Sie die Richtlinie simulieren und aktivieren.

Regeln zur Richtlinie hinzufügen

In diesem Beispiel enthält die ILM-Richtlinie drei ILM-Regeln in der folgenden Reihenfolge:

1. Eine konforme Regel, die Erasure Coding verwendet, um Objekte mit mehr als 1 MB in einem bestimmten Bucket mit aktivierter S3-Objektsperre zu schützen. Die Objekte werden vom Tag 0 bis in alle Ewigkeit auf Speicherknoten gespeichert.
2. Eine nicht konforme Regel, die ein Jahr lang zwei replizierte Objektkopien auf Speicherknoten erstellt und dann eine Objektkopie dauerhaft in einen Cloud-Speicherpool verschiebt. Diese Regel gilt nicht für Buckets mit aktivierter S3-Objektsperre, da diese einen Cloud-Speicherpool verwenden.
3. Die standardmäßige konforme Regel, die vom Tag 0 bis in alle Ewigkeit zwei replizierte Objektkopien auf Speicherknoten erstellt.

Simulieren Sie die Richtlinie

Nachdem Sie Ihrer Richtlinie Regeln hinzugefügt, eine standardmäßige konforme Regel ausgewählt und die anderen Regeln angeordnet haben, sollten Sie die Richtlinie simulieren, indem Sie Objekte aus dem Bucket mit aktivierter S3-Objektsperre und aus anderen Buckets testen. Wenn Sie beispielsweise die Beispielrichtlinie simulieren, würden Sie erwarten, dass Testobjekte wie folgt ausgewertet werden:

- Die erste Regel stimmt nur mit Testobjekten überein, die im Bucket „Bankdatensätze“ für den Mandanten der Bank of ABC größer als 1 MB sind.
- Die zweite Regel gleicht alle Objekte in allen nicht konformen Buckets für alle anderen Mandantenkonten ab.
- Die Standardregel trifft auf diese Objekte zu:
  - Objekte mit 1 MB oder weniger im Bucket „Bankunterlagen“ für den Mandanten der Bank of ABC.
  - Objekte in jedem anderen Bucket, für den S3 Object Lock für alle anderen Mandantenkonten aktiviert ist.

Aktivieren der Richtlinie

Wenn Sie vollständig davon überzeugt sind, dass die neue Richtlinie die Objektdaten wie erwartet schützt, können Sie sie aktivieren.

Beispiel 8: Prioritäten für den S3-Bucket-Lebenszyklus und die ILM-Richtlinie

Abhängig von Ihrer Lebenszykluskonfiguration folgen Objekte entweder den

Aufbewahrungseinstellungen des S3-Bucket-Lebenszyklus oder einer ILM-Richtlinie.

Beispiel für den Bucket-Lebenszyklus, der Vorrang vor der ILM-Richtlinie hat

ILM-Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien 20 Tage lang aufbewahren
- Regel basierend auf der Aufnahmezeitreferenz (Standard): Am Tag 0 X Kopien 50 Tage lang aufbewahren

Bucket-Lebenszyklus

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Ergebnis

- Ein Objekt mit dem Namen „docs/text“ wird aufgenommen. Es entspricht dem Bucket-Lebenszyklusfilter des Präfixes „docs/“.
  - Nach 100 Tagen wird eine Löschmarkierung erstellt und „docs/text“ wird nicht mehr aktuell.
  - Nach 5 Tagen, insgesamt 105 Tage seit der Aufnahme, wird „docs/text“ gelöscht.
  - Nach 95 Tagen, also insgesamt 200 Tagen seit der Aufnahme und 100 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.
- Ein Objekt mit dem Namen „Video/Film“ wird aufgenommen. Es entspricht nicht dem Filter und verwendet die ILM-Aufbewahrungsrichtlinie.
  - Nach 50 Tagen wird eine Löschmarkierung erstellt und „Video/Film“ wird nicht mehr aktuell.
  - Nach 20 Tagen, also insgesamt 70 Tagen seit der Aufnahme, wird „Video/Film“ gelöscht.
  - Nach 30 Tagen, also insgesamt 100 Tagen seit der Aufnahme und 50 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.

Beispiel für den Bucket-Lebenszyklus mit impliziter ewiger Aufbewahrung

ILM-Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien 20 Tage lang aufbewahren
- Regel basierend auf der Aufnahmezeitreferenz (Standard): Am Tag 0 X Kopien 50 Tage lang aufbewahren

Bucket-Lebenszyklus

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Ergebnis

- Ein Objekt mit dem Namen „docs/text“ wird aufgenommen. Es entspricht dem Bucket-Lebenszyklusfilter des Präfixes „docs/“.

  Der `Expiration` Die Aktion gilt nur für abgelaufene Löschmarkierungen, was bedeutet, dass alles andere (beginnend mit „docs/“) für immer erhalten bleibt.

  Löschmarkierungen, die mit „docs/“ beginnen, werden entfernt, wenn sie ablaufen.

- Ein Objekt mit dem Namen „Video/Film“ wird aufgenommen. Es entspricht nicht dem Filter und verwendet die ILM-Aufbewahrungsrichtlinie.

- Nach 50 Tagen wird eine Löschmarkierung erstellt und „Video/Film“ wird nicht mehr aktuell.
- Nach 20 Tagen, also insgesamt 70 Tagen seit der Aufnahme, wird „Video/Film“ gelöscht.
- Nach 30 Tagen, also insgesamt 100 Tagen seit der Aufnahme und 50 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.

Beispiel für die Verwendung des Bucket-Lebenszyklus zum Duplizieren von ILM und Bereinigen abgelaufener Löschmarkierungen

ILM-Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien 20 Tage lang aufbewahren
- Regel basierend auf der Aufnahmezeitreferenz (Standard): Am Tag 0 X Kopien für immer behalten

Bucket-Lebenszyklus

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Ergebnis

- Die ILM-Richtlinie wird im Bucket-Lebenszyklus dupliziert.
  - Die „Für immer“-Regel der ILM-Richtlinie ist darauf ausgelegt, Objekte manuell zu entfernen und nicht aktuelle Versionen nach 20 Tagen zu bereinigen. Folglich behält die Aufnahmezeitregel abgelaufene Löschmarkierungen für immer bei.
  - Der Bucket-Lebenszyklus dupliziert das Verhalten der ILM-Richtlinie und fügt hinzu `"ExpiredObjectDeleteMarker": true` , wodurch Löschmarkierungen entfernt werden, sobald sie abgelaufen sind
- Ein Gegenstand wird verschluckt. Kein Filter bedeutet, dass der Bucket-Lebenszyklus für alle Objekte gilt und die ILM-Aufbewahrungseinstellungen überschreibt.
  - Wenn ein Mandant eine Anforderung zum Löschen eines Objekts ausgibt, wird eine Löschmarkierung erstellt und das Objekt wird nicht mehr aktuell.
  - Nach 20 Tagen wird das nicht aktuelle Objekt gelöscht und die Löschmarkierung läuft ab.
  - Kurz darauf wird der abgelaufene Löschmarker gelöscht.

Systemhärtung

Allgemeine Überlegungen zur Systemhärtung

Unter Systemhärtung versteht man den Prozess, möglichst viele Sicherheitsrisiken aus einem StorageGRID -System zu eliminieren.

Verwenden Sie beim Installieren und Konfigurieren von StorageGRID diese Richtlinien, um alle vorgeschriebenen Sicherheitsziele hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu erreichen.

Sie sollten bereits branchenübliche Best Practices zur Systemhärtung verwenden. Verwenden Sie beispielsweise sichere Passwörter für StorageGRID, verwenden Sie HTTPS statt HTTP und aktivieren Sie die zertifikatsbasierte Authentifizierung, sofern verfügbar.

StorageGRID folgt dem "NetApp -Richtlinie zur Handhabung von Sicherheitslücken" . Gemeldete Schwachstellen werden überprüft und gemäß dem Reaktionsprozess für Produktsicherheitsvorfälle behoben.

Beachten Sie beim Härten eines StorageGRID -Systems Folgendes:

- **Welches der drei StorageGRID Netzwerke** haben Sie implementiert? Alle StorageGRID -Systeme müssen das Grid-Netzwerk verwenden, Sie können jedoch auch das Admin-Netzwerk, das Client-Netzwerk oder beide verwenden. Für jedes Netzwerk gelten andere Sicherheitsaspekte.
- **Die Art der Plattformen**, die Sie für die einzelnen Knoten in Ihrem StorageGRID -System verwenden. StorageGRID -Knoten können auf virtuellen VMware-Maschinen, innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Geräte bereitgestellt werden. Jeder Plattformtyp verfügt über einen eigenen Satz bewährter Verfahren zur Härtung.
- **Wie vertrauenswürdig die Mieterkonten sind**. Wenn Sie ein Dienstanbieter mit nicht vertrauenswürdigen Mandantenkonten sind, haben Sie andere Sicherheitsbedenken, als wenn Sie nur vertrauenswürdige, interne Mandanten verwenden.
- **Welche Sicherheitsanforderungen und Konventionen** Ihre Organisation befolgt. Möglicherweise müssen Sie bestimmte gesetzliche oder unternehmensbezogene Anforderungen erfüllen.

Härtungsrichtlinien für Software-Upgrades

Sie müssen Ihr StorageGRID -System und die zugehörigen Dienste auf dem neuesten Stand halten, um sich vor Angriffen zu schützen.

Upgrades der StorageGRID -Software

Wenn möglich, sollten Sie die StorageGRID -Software auf die neueste Hauptversion oder auf die vorherige Hauptversion aktualisieren. Durch die Aktualisierung von StorageGRID lässt sich die Zeit verkürzen, in der bekannte Schwachstellen aktiv sind, und die gesamte Angriffsfläche wird verringert. Darüber hinaus enthalten die neuesten Versionen von StorageGRID häufig Funktionen zur Sicherheitshärtung, die in früheren Versionen nicht enthalten waren.

Konsultieren Sie die "NetApp Interoperabilitätsmatrix-Tool" (IMT), um zu bestimmen, welche Version der StorageGRID -Software Sie verwenden sollten. Wenn ein Hotfix erforderlich ist, legt NetApp Wert darauf, Updates für die aktuellsten Versionen zu erstellen. Einige Patches sind möglicherweise nicht mit früheren Versionen kompatibel.

- Um die neuesten StorageGRID Versionen und Hotfixes herunterzuladen, gehen Sie zu "NetApp Downloads: StorageGRID" .
- Informationen zum Upgrade der StorageGRID -Software finden Sie im"Upgrade-Anweisungen" .
- Informationen zum Anwenden eines Hotfixes finden Sie im"StorageGRID Hotfix-Verfahren" .

Upgrades auf externe Dienste

Externe Dienste können Schwachstellen aufweisen, die StorageGRID indirekt betreffen. Sie sollten sicherstellen, dass die Dienste, von denen StorageGRID abhängt, auf dem neuesten Stand gehalten werden. Zu diesen Diensten gehören LDAP, KMS (oder KMIP-Server), DNS und NTP.

Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Upgrades auf Hypervisoren

Wenn Ihre StorageGRID -Knoten auf VMware oder einem anderen Hypervisor ausgeführt werden, müssen Sie sicherstellen, dass die Software und Firmware des Hypervisors auf dem neuesten Stand sind.

Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Upgrades auf Linux-Knoten

Wenn Ihre StorageGRID -Knoten Linux-Hostplattformen verwenden, müssen Sie sicherstellen, dass Sicherheitsupdates und Kernelupdates auf das Hostbetriebssystem angewendet werden. Darüber hinaus müssen Sie Firmware-Updates auf anfällige Hardware anwenden, sobald diese Updates verfügbar sind.

Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Härtungsrichtlinien für StorageGRID -Netzwerke

Das StorageGRID -System unterstützt bis zu drei Netzwerkschnittstellen pro Grid-Knoten, sodass Sie die Vernetzung für jeden einzelnen Grid-Knoten entsprechend Ihren Sicherheits- und Zugriffsanforderungen konfigurieren können.

Ausführliche Informationen zu StorageGRID -Netzwerken finden Sie im"StorageGRID -Netzwerktypen" .

Richtlinien für das Grid-Netzwerk

Sie müssen für den gesamten internen StorageGRID Verkehr ein Grid-Netzwerk konfigurieren. Alle Grid-Knoten befinden sich im Grid-Netzwerk und müssen mit allen anderen Knoten kommunizieren können.

Befolgen Sie beim Konfigurieren des Grid-Netzwerks die folgenden Richtlinien:

- Stellen Sie sicher, dass das Netzwerk vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt ist.
- Verwenden Sie das Grid-Netzwerk nach Möglichkeit ausschließlich für den internen Verkehr. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk unterliegen zusätzlichen Firewall-Einschränkungen, die den externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Verkehr wird unterstützt, diese Verwendung bietet jedoch weniger Schutzebenen.
- Wenn sich die StorageGRID -Bereitstellung über mehrere Rechenzentren erstreckt, verwenden Sie ein virtuelles privates Netzwerk (VPN) oder ein gleichwertiges Netzwerk im Grid-Netzwerk, um zusätzlichen Schutz für den internen Datenverkehr zu bieten.
- Einige Wartungsverfahren erfordern einen Secure Shell-Zugriff (SSH) auf Port 22 zwischen dem primären Admin-Knoten und allen anderen Grid-Knoten. Verwenden Sie eine externe Firewall, um den SSH-Zugriff auf vertrauenswürdige Clients zu beschränken.

Richtlinien für das Admin-Netzwerk

Das Admin-Netzwerk wird normalerweise für Verwaltungsaufgaben (vertrauenswürdige Mitarbeiter, die den Grid Manager oder SSH verwenden) und für die Kommunikation mit anderen vertrauenswürdigen Diensten wie LDAP, DNS, NTP oder KMS (oder KMIP-Server) verwendet. StorageGRID erzwingt diese Verwendung jedoch nicht intern.

Wenn Sie das Admin-Netzwerk verwenden, befolgen Sie diese Richtlinien:

- Blockieren Sie alle internen Datenverkehrsports im Admin-Netzwerk. Siehe die"Liste der internen Ports" .
- Wenn nicht vertrauenswürdige Clients auf das Admin-Netzwerk zugreifen können, blockieren Sie den Zugriff auf StorageGRID im Admin-Netzwerk mit einer externen Firewall.

Richtlinien für das Client-Netzwerk

Das Client-Netzwerk wird normalerweise für Mandanten und zur Kommunikation mit externen Diensten

verwendet, beispielsweise dem CloudMirror-Replikationsdienst oder einem anderen Plattformdienst. StorageGRID erzwingt diese Verwendung jedoch nicht intern.

Wenn Sie das Client-Netzwerk verwenden, befolgen Sie diese Richtlinien:

- Blockieren Sie alle internen Datenverkehrsports im Client-Netzwerk. Siehe die"Liste der internen Ports" .
- Akzeptieren Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Endpunkten. Informationen zu"Verwalten von Firewall-Kontrollen" .

Härtungsrichtlinien für StorageGRID Knoten

StorageGRID -Knoten können auf virtuellen VMware-Maschinen, innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Geräte bereitgestellt werden. Jeder Plattformtyp und jeder Knotentyp verfügt über einen eigenen Satz bewährter Verfahren zur Härtung.

Steuern Sie den Remote-IPMI-Zugriff auf BMC

Sie können den Remote-IPMI-Zugriff für alle Appliances mit einem BMC aktivieren oder deaktivieren. Die Remote-IPMI-Schnittstelle ermöglicht jedem mit einem BMC -Konto und Kennwort den Low-Level-Hardwarezugriff auf Ihre StorageGRID -Geräte. Wenn Sie keinen Remote-IPMI-Zugriff auf den BMC benötigen, deaktivieren Sie diese Option.

- Um den Remote-IPMI-Zugriff auf den BMC im Grid Manager zu steuern, gehen Sie zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** > **Geräte**:
  - Deaktivieren Sie das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren**, um den IPMI-Zugriff auf den BMC zu deaktivieren.
  - Aktivieren Sie das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren**, um den IPMI-Zugriff auf den BMC zu aktivieren.

Firewall-Konfiguration

Im Rahmen der Systemhärtung müssen Sie die Konfigurationen externer Firewalls überprüfen und so ändern, dass Datenverkehr nur von den IP-Adressen und Ports akzeptiert wird, von denen er unbedingt benötigt wird.

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. Du solltest"Verwalten Sie interne Firewall-Kontrollen" um den Netzwerkzugriff auf allen Ports außer denen zu verhindern, die für Ihre spezifische Grid-Bereitstellung erforderlich sind. Die Konfigurationsänderungen, die Sie auf der Firewall-Steuerungsseite vornehmen, werden auf jedem Knoten bereitgestellt.

Insbesondere können Sie diese Bereiche verwalten:

- **Privilegierte Adressen**: Sie können ausgewählten IP-Adressen oder Subnetzen den Zugriff auf Ports erlauben, die durch Einstellungen auf der Registerkarte „Externen Zugriff verwalten“ geschlossen sind.
- **Externen Zugriff verwalten**: Sie können standardmäßig geöffnete Ports schließen oder zuvor geschlossene Ports wieder öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk**: Sie können angeben, ob ein Knoten eingehendem Datenverkehr vom Client-Netzwerk vertraut, sowie die zusätzlichen Ports, die geöffnet werden sollen, wenn ein nicht vertrauenswürdiges Client-Netzwerk konfiguriert ist.

Diese interne Firewall bietet zwar eine zusätzliche Schutzebene gegen einige gängige Bedrohungen, macht jedoch eine externe Firewall nicht überflüssig.

Eine Liste aller von StorageGRID verwendeten internen und externen Ports finden Sie unter"Netzwerkportreferenz" .

Deaktivieren Sie nicht verwendete Dienste

Für alle StorageGRID -Knoten sollten Sie den Zugriff auf nicht verwendete Dienste deaktivieren oder blockieren. Wenn Sie beispielsweise DHCP nicht verwenden möchten, schließen Sie Port 68 mit dem Grid Manager. Wählen Sie **KONFIGURATION** > **Firewall-Steuerung** > **Externen Zugriff verwalten**. Ändern Sie dann den Statusschalter für Port 68 von **Offen** auf **Geschlossen**.

Virtualisierung, Container und gemeinsam genutzte Hardware

Vermeiden Sie bei allen StorageGRID -Knoten, StorageGRID auf derselben physischen Hardware wie nicht vertrauenswürdige Software auszuführen. Gehen Sie nicht davon aus, dass der Hypervisor-Schutz Schadsoftware daran hindert, auf durch StorageGRID geschützte Daten zuzugreifen, wenn sich sowohl StorageGRID als auch die Schadsoftware auf derselben physischen Hardware befinden. Beispielsweise nutzen die Meltdown- und Spectre-Angriffe kritische Schwachstellen in modernen Prozessoren aus und ermöglichen es Programmen, Daten im Speicher desselben Computers zu stehlen.

Schützen Sie Knoten während der Installation

Erlauben Sie nicht vertrauenswürdigen Benutzern nicht, über das Netzwerk auf StorageGRID -Knoten zuzugreifen, wenn die Knoten installiert werden. Knoten sind erst dann vollständig sicher, wenn sie dem Netz beigetreten sind.

Richtlinien für Admin-Knoten

Admin-Knoten bieten Verwaltungsdienste wie Systemkonfiguration, Überwachung und Protokollierung. Wenn Sie sich beim Grid Manager oder Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her.

Befolgen Sie diese Richtlinien, um die Admin-Knoten in Ihrem StorageGRID -System zu sichern:

- Schützen Sie alle Admin-Knoten vor nicht vertrauenswürdigen Clients, beispielsweise solchen im offenen Internet. Stellen Sie sicher, dass kein nicht vertrauenswürdiger Client auf einen Admin-Knoten im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk zugreifen kann.
- StorageGRID -Gruppen steuern den Zugriff auf die Funktionen Grid Manager und Tenant Manager. Gewähren Sie jeder Benutzergruppe die für ihre Rolle erforderlichen Mindestberechtigungen und verwenden Sie den schreibgeschützten Zugriffsmodus, um zu verhindern, dass Benutzer die Konfiguration ändern.
- Wenn Sie StorageGRID Load Balancer-Endpunkte verwenden, verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr Gateway-Knoten anstelle von Admin-Knoten.
- Wenn Sie nicht vertrauenswürdige Mandanten haben, gewähren Sie ihnen keinen direkten Zugriff auf den Mandanten-Manager oder die Mandantenverwaltungs-API. Lassen Sie stattdessen nicht vertrauenswürdige Mandanten ein Mandantenportal oder ein externes Mandantenverwaltungssystem verwenden, das mit der Mandantenverwaltungs-API interagiert.
- Verwenden Sie optional einen Admin-Proxy, um mehr Kontrolle über die AutoSupport -Kommunikation von Admin-Knoten zum NetApp Support zu haben. Sehen Sie sich die Schritte für"Erstellen eines Admin-Proxys" .

- Verwenden Sie optional die eingeschränkten Ports 8443 und 9443, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen. Blockieren Sie den freigegebenen Port 443 und beschränken Sie die Mieteranfragen auf Port 9443 für zusätzlichen Schutz.
- Verwenden Sie optional separate Admin-Knoten für Grid-Administratoren und Mandantenbenutzer.

Weitere Informationen finden Sie in der Anleitung für"StorageGRID verwalten" .

Richtlinien für Speicherknoten

Speicherknoten verwalten und speichern Objektdaten und Metadaten. Befolgen Sie diese Richtlinien, um die Speicherknoten in Ihrem StorageGRID -System zu sichern.

- Erlauben Sie nicht vertrauenswürdigen Clients nicht, eine direkte Verbindung zu Speicherknoten herzustellen. Verwenden Sie einen Load Balancer-Endpunkt, der von einem Gateway-Knoten oder einem Load Balancer eines Drittanbieters bedient wird.
- Aktivieren Sie keine ausgehenden Dienste für nicht vertrauenswürdige Mandanten. Wenn Sie beispielsweise das Konto für einen nicht vertrauenswürdigen Mandanten erstellen, erlauben Sie dem Mandanten nicht, seine eigene Identitätsquelle zu verwenden, und erlauben Sie nicht die Verwendung von Plattformdiensten. Sehen Sie sich die Schritte für"Erstellen eines Mieterkontos" .
- Verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr einen Load Balancer eines Drittanbieters. Der Lastenausgleich durch Drittanbieter bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe.
- Verwenden Sie optional einen Speicherproxy für mehr Kontrolle über Cloud-Speicherpools und die Kommunikation der Plattformdienste von Speicherknoten zu externen Diensten. Sehen Sie sich die Schritte für"Erstellen eines Speicherproxys" .
- Optional können Sie über das Client-Netzwerk eine Verbindung zu externen Diensten herstellen. Wählen Sie dann **KONFIGURATION** > **Sicherheit** > **Firewall-Steuerung** > **Nicht vertrauenswürdige Client-Netzwerke** und geben Sie an, dass das Client-Netzwerk auf dem Speicherknoten nicht vertrauenswürdig ist. Der Speicherknoten akzeptiert keinen eingehenden Datenverkehr mehr im Client-Netzwerk, lässt jedoch weiterhin ausgehende Anfragen für Plattformdienste zu.

Richtlinien für Gateway-Knoten

Gateway-Knoten bieten eine optionale Lastausgleichsschnittstelle, die Clientanwendungen zur Verbindung mit StorageGRID verwenden können. Befolgen Sie diese Richtlinien, um alle Gateway-Knoten in Ihrem StorageGRID System zu sichern:

- Konfigurieren und verwenden Sie Load Balancer-Endpunkte. Sehen "Überlegungen zum Lastenausgleich" .
- Verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr einen Load Balancer eines Drittanbieters zwischen dem Client und dem Gateway-Knoten oder den Speicherknoten. Der Lastenausgleich durch Drittanbieter bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe. Wenn Sie einen Load Balancer eines Drittanbieters verwenden, kann der Netzwerkverkehr optional weiterhin so konfiguriert werden, dass er über einen internen Load Balancer-Endpunkt läuft oder direkt an Speicherknoten gesendet wird.
- Wenn Sie Load Balancer-Endpunkte verwenden, können Sie Clients optional über das Client-Netzwerk verbinden. Wählen Sie dann **KONFIGURATION** > **Sicherheit** > **Firewall-Steuerung** > **Nicht vertrauenswürdige Client-Netzwerke** und geben Sie an, dass das Client-Netzwerk auf dem Gateway-Knoten nicht vertrauenswürdig ist. Der Gateway-Knoten akzeptiert eingehenden Datenverkehr nur auf den Ports, die explizit als Endpunkte des Lastenausgleichs konfiguriert sind.

Richtlinien für Hardware-Appliance-Knoten

StorageGRID Hardwaregeräte sind speziell für die Verwendung in einem StorageGRID -System konzipiert. Einige Geräte können als Speicherknoten verwendet werden. Andere Appliances können als Admin-Knoten oder Gateway-Knoten verwendet werden. Sie können Appliance-Knoten mit softwarebasierten Knoten kombinieren oder vollständig entwickelte Grids mit ausschließlich Appliances bereitstellen.

Befolgen Sie diese Richtlinien, um alle Hardware-Appliance-Knoten in Ihrem StorageGRID System zu sichern:

- Wenn das Gerät SANtricity System Manager zur Verwaltung des Speichercontrollers verwendet, verhindern Sie, dass nicht vertrauenswürdige Clients über das Netzwerk auf SANtricity System Manager zugreifen.
- Wenn das Gerät über einen Baseboard Management Controller (BMC) verfügt, beachten Sie, dass der BMC Verwaltungsport einen Low-Level-Hardwarezugriff ermöglicht. Verbinden Sie den BMC Verwaltungsport nur mit einem sicheren, vertrauenswürdigen internen Verwaltungsnetzwerk. Wenn kein solches Netzwerk verfügbar ist, lassen Sie den BMC Verwaltungsport unverbunden oder blockiert, es sei denn, der technische Support fordert eine BMC -Verbindung an.
- Wenn die Appliance die Remoteverwaltung der Controller-Hardware über Ethernet mithilfe des IPMI-Standards (Intelligent Platform Management Interface) unterstützt, blockieren Sie nicht vertrauenswürdigen Datenverkehr auf Port 623.

> ⓘ Sie können den Remote-IPMI-Zugriff für alle Appliances mit einem BMC aktivieren oder deaktivieren. Die Remote-IPMI-Schnittstelle ermöglicht jedem mit einem BMC -Konto und Kennwort den Low-Level-Hardwarezugriff auf Ihre StorageGRID -Geräte. Wenn Sie keinen Remote-IPMI-Zugriff auf den BMC benötigen, deaktivieren Sie diese Option mit einer der folgenden Methoden: + Gehen Sie im Grid Manager zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** > **Geräte** und deaktivieren Sie das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren**. + Verwenden Sie in der Grid-Management-API den privaten Endpunkt: `PUT /private/bmc` .

- Für Appliance-Modelle mit SED-, FDE- oder FIPS NL-SAS-Laufwerken, die Sie mit SANtricity System Manager verwalten, "Aktivieren und Konfigurieren von SANtricity Drive Security" .
- Für Appliance-Modelle mit SED- oder FIPS-NVMe-SSDs, die Sie mit dem StorageGRID Appliance Installer und Grid Manager verwalten, "Aktivieren und Konfigurieren der StorageGRID -Laufwerkverschlüsselung" .
- Aktivieren und konfigurieren Sie für Appliances ohne SED-, FDE- oder FIPS-Laufwerke die StorageGRID Softwareknotenverschlüsselung "mithilfe eines Key Management Servers (KMS)" .

Härtungsrichtlinien für TLS und SSH

Sie sollten die während der Installation erstellten Standardzertifikate ersetzen und die entsprechende Sicherheitsrichtlinie für TLS- und SSH-Verbindungen auswählen.

Härtungsrichtlinien für Zertifikate

Sie sollten die während der Installation erstellten Standardzertifikate durch Ihre eigenen benutzerdefinierten Zertifikate ersetzen.

Bei vielen Organisationen entspricht das selbstsignierte digitale Zertifikat für den StorageGRID Webzugriff nicht ihren Informationssicherheitsrichtlinien. Auf Produktionssystemen sollten Sie ein von einer Zertifizierungsstelle signiertes digitales Zertifikat zur Authentifizierung von StorageGRID installieren.

Insbesondere sollten Sie benutzerdefinierte Serverzertifikate anstelle dieser Standardzertifikate verwenden:

- **Management-Schnittstellenzertifikat**: Wird verwendet, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern.
- **S3-API-Zertifikat**: Wird verwendet, um den Zugriff auf Speicherknoten und Gateway-Knoten zu sichern, die von S3-Clientanwendungen zum Hoch- und Herunterladen von Objektdaten verwendet werden.

Sehen"Sicherheitszertifikate verwalten" für Details und Anweisungen.

> StorageGRID verwaltet die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie unter"Konfigurieren von Load Balancer-Endpunkten" .

Beachten Sie bei der Verwendung benutzerdefinierter Serverzertifikate die folgenden Richtlinien:

- Zertifikate sollten eine `subjectAltName` das mit den DNS-Einträgen für StorageGRID übereinstimmt. Weitere Einzelheiten finden Sie in Abschnitt 4.2.1.6, „Alternativer Betreffname“, in "RFC 5280: PKIX-Zertifikat und CRL-Profil" .
- Vermeiden Sie nach Möglichkeit die Verwendung von Platzhalterzertifikaten. Eine Ausnahme von dieser Richtlinie ist das Zertifikat für einen virtuell gehosteten S3-Endpunkt, bei dem die Verwendung eines Platzhalters erforderlich ist, wenn die Bucket-Namen nicht im Voraus bekannt sind.
- Wenn Sie in Zertifikaten Platzhalter verwenden müssen, sollten Sie zusätzliche Schritte unternehmen, um die Risiken zu verringern. Verwenden Sie ein Platzhaltermuster wie `*.s3.example.com` und verwenden Sie nicht die `s3.example.com` Suffix für andere Anwendungen. Dieses Muster funktioniert auch mit S3-Zugriff im Pfadstil, wie z. B. `dc1-s1.s3.example.com/mybucket` .
- Legen Sie kurze Ablaufzeiten für Zertifikate fest (z. B. 2 Monate) und verwenden Sie die Grid Management API, um die Zertifikatrotation zu automatisieren. Dies ist besonders wichtig für Wildcard-Zertifikate.

Darüber hinaus sollten Clients bei der Kommunikation mit StorageGRID eine strenge Hostnamenprüfung durchführen.

Härtungsrichtlinien für TLS- und SSH-Richtlinien

Sie können eine Sicherheitsrichtlinie auswählen, um zu bestimmen, welche Protokolle und Verschlüsselungen 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. Als bewährte Methode sollten Sie Verschlüsselungsoptionen deaktivieren, die für die Anwendungskompatibilität nicht erforderlich sind. Verwenden Sie die standardmäßige moderne Richtlinie, es sei denn, Ihr System muss Common Criteria-kompatibel sein oder Sie müssen andere Chiffren verwenden.

Sehen"Verwalten der TLS- und SSH-Richtlinie" für Details und Anweisungen.

Weitere Härtungsrichtlinien

Zusätzlich zur Befolgung der Härtungsrichtlinien für StorageGRID -Netzwerke und -Knoten sollten Sie die Härtungsrichtlinien für andere Bereiche des StorageGRID Systems befolgen.

Temporäres Installationskennwort

Um das StorageGRID -System während der Installation zu sichern, legen Sie auf der Seite mit dem

temporären Installationskennwort in der StorageGRID Installationsbenutzeroberfläche oder in der Installations-API ein Kennwort fest. Wenn dieses Passwort festgelegt ist, gilt es für alle Methoden zur Installation von StorageGRID, einschließlich der Benutzeroberfläche, der Installations-API und `configure-storagegrid.py` Skript.

Weitere Informationen finden Sie unter:

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"
- "Installieren Sie das StorageGRID -Gerät"

Protokolle und Prüfmeldungen

Schützen Sie StorageGRID -Protokolle und die Ausgabe von Prüfnachrichten stets auf sichere Weise. StorageGRID -Protokolle und Prüfmeldungen liefern aus Sicht des Supports und der Systemverfügbarkeit wertvolle Informationen. Darüber hinaus sind die in den Protokollen und Prüfnachrichten von StorageGRID enthaltenen Informationen und Details im Allgemeinen vertraulicher Natur.

Konfigurieren Sie StorageGRID so, dass Sicherheitsereignisse an einen externen Syslog-Server gesendet werden. Wenn Sie den Syslog-Export verwenden, wählen Sie TLS und RELP/TLS als Transportprotokolle aus.

Siehe die"Referenz zu Protokolldateien" Weitere Informationen zu StorageGRID Protokollen. Sehen"Prüfmeldungen" Weitere Informationen zu StorageGRID -Auditmeldungen finden Sie unter.

NetApp AutoSupport

Mit der AutoSupport Funktion von StorageGRID können Sie den Zustand Ihres Systems proaktiv überwachen und automatisch Pakete an die NetApp -Support-Site, das interne Support-Team Ihres Unternehmens oder einen Support-Partner senden. Standardmäßig ist das Senden von AutoSupport Paketen an NetApp aktiviert, wenn StorageGRID zum ersten Mal konfiguriert wird.

Die AutoSupport Funktion kann deaktiviert werden. NetApp empfiehlt jedoch, es zu aktivieren, da AutoSupport die Problemidentifizierung und -lösung beschleunigt, falls auf Ihrem StorageGRID -System ein Problem auftritt.

AutoSupport unterstützt HTTPS, HTTP und SMTP als Transportprotokolle. Aufgrund der sensiblen Natur von AutoSupport Paketen empfiehlt NetApp dringend, HTTPS als Standardtransportprotokoll zum Senden von AutoSupport Paketen an NetApp zu verwenden.

Cross-Origin-Ressourcenfreigabe (CORS)

Sie können Cross-Origin Resource Sharing (CORS) für einen S3-Bucket konfigurieren, wenn dieser Bucket und die darin enthaltenen Objekte für Webanwendungen in anderen Domänen zugänglich sein sollen. Aktivieren Sie CORS grundsätzlich nur, wenn es erforderlich ist. Wenn CORS erforderlich ist, beschränken Sie es auf vertrauenswürdige Ursprünge.

Sehen Sie sich die Schritte für"Konfigurieren der Cross-Origin-Ressourcenfreigabe (CORS)" .

Externe Sicherheitsgeräte

Eine vollständige Härtungslösung muss Sicherheitsmechanismen außerhalb von StorageGRID berücksichtigen. Die Verwendung zusätzlicher Infrastrukturgeräte zum Filtern und Beschränken des Zugriffs auf StorageGRID ist eine effektive Möglichkeit, eine strenge Sicherheitslage zu etablieren und

aufrechtzuerhalten. Zu diesen externen Sicherheitsgeräten gehören Firewalls, Intrusion Prevention Systems (IPS) und andere Sicherheitsgeräte.

Für nicht vertrauenswürdigen Client-Datenverkehr wird ein Load Balancer eines Drittanbieters empfohlen. Der Lastenausgleich durch Drittanbieter bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe.

Ransomware-Minderung

Schützen Sie Ihre Objektdaten vor Ransomware-Angriffen, indem Sie die Empfehlungen in "Ransomware-Abwehr mit StorageGRID" .

Konfigurieren von StorageGRID für FabricPool

Konfigurieren von StorageGRID für FabricPool

Wenn Sie die NetApp ONTAP -Software verwenden, können Sie mit NetApp FabricPool inaktive Daten auf ein NetApp StorageGRID -Objektspeichersystem verschieben.

Verwenden Sie diese Anweisungen, um:

- Informieren Sie sich über die Überlegungen und Best Practices zur Konfiguration von StorageGRID für eine FabricPool -Workload.
- Erfahren Sie, wie Sie ein StorageGRID Objektspeichersystem für die Verwendung mit FabricPool konfigurieren.
- Erfahren Sie, wie Sie ONTAP die erforderlichen Werte bereitstellen, wenn Sie StorageGRID als FabricPool Cloud-Tier anhängen.

Schnellstart zur Konfiguration von StorageGRID für FabricPool

1 **Planen Sie Ihre Konfiguration**

- Entscheiden Sie, welche FabricPool Volume-Tiering-Richtlinie Sie verwenden möchten, um inaktive ONTAP Daten in StorageGRID zu verschieben.
- Planen und installieren Sie ein StorageGRID -System, um Ihren Anforderungen an Speicherkapazität und Leistung gerecht zu werden.
- Machen Sie sich mit der StorageGRID -Systemsoftware vertraut, einschließlich der"Grid-Manager" und die"Mietermanager" .
- Lesen Sie die Best Practices für FabricPool für"HA-Gruppen" ,"Lastausgleich" ,"ILM" , Und"mehr" .
- Sehen Sie sich diese zusätzlichen Ressourcen an, die Details zur Verwendung und Konfiguration von ONTAP und FabricPool enthalten:

  "TR-4598: FabricPool Best Practices in ONTAP"

  "ONTAP -Dokumentation für FabricPool"

2 **Ausführen der erforderlichen Aufgaben**

Erhalten Sie die"Informationen, die zum Anhängen von StorageGRID als Cloud-Ebene erforderlich sind" ,

einschließlich:

- IP-Adressen
- Domänennamen
- SSL-Zertifikat

Optional konfigurieren"Identitätsföderation" Und"Einmaliges Anmelden" .

3 Konfigurieren der StorageGRID -Einstellungen

Verwenden Sie StorageGRID , um die Werte abzurufen, die ONTAP für die Verbindung mit dem Grid benötigt.

Verwenden des"FabricPool -Setup-Assistent" ist die empfohlene und schnellste Möglichkeit, alle Elemente zu konfigurieren. Sie können jedoch bei Bedarf auch jede Entität manuell konfigurieren.

4 Konfigurieren Sie ONTAP und DNS

Nutzen Sie ONTAP für"eine Cloud-Ebene hinzufügen" das die StorageGRID -Werte verwendet. Dann,"DNS-Einträge konfigurieren" um IP-Adressen mit allen Domänennamen zu verknüpfen, die Sie verwenden möchten.

5 Überwachen und verwalten

Wenn Ihr System betriebsbereit ist, führen Sie laufende Aufgaben in ONTAP und StorageGRID aus, um die FabricPool Datenschichtung im Laufe der Zeit zu verwalten und zu überwachen.

Was ist FabricPool?

FabricPool ist eine hybride ONTAP Speicherlösung, die ein leistungsstarkes Flash-Aggregat als Leistungsebene und einen Objektspeicher als Cloud-Ebene verwendet. Durch die Verwendung von FabricPool-fähigen Aggregaten können Sie die Speicherkosten senken, ohne die Leistung, Effizienz oder Sicherheit zu beeinträchtigen.

FabricPool verknüpft eine Cloud-Ebene (einen externen Objektspeicher wie StorageGRID) mit einer lokalen Ebene (einem ONTAP -Speicheraggregat), um eine zusammengesetzte Sammlung von Datenträgern zu erstellen. Volumes innerhalb des FabricPool können dann die Vorteile der Tiering-Funktion nutzen, indem sie aktive (heiße) Daten auf einem Hochleistungsspeicher (der lokalen Ebene) behalten und inaktive (kalte) Daten in den externen Objektspeicher (die Cloud-Ebene) verschieben.

Es sind keine Änderungen an der Architektur erforderlich und Sie können Ihre Daten- und Anwendungsumgebung weiterhin vom zentralen ONTAP Speichersystem aus verwalten.

Was ist StorageGRID?

NetApp StorageGRID ist eine Speicherarchitektur, die Daten als Objekte verwaltet, im Gegensatz zu anderen Speicherarchitekturen wie Datei- oder Blockspeicher. Objekte werden in einem einzelnen Container (z. B. einem Bucket) aufbewahrt und nicht als Dateien in einem Verzeichnis innerhalb anderer Verzeichnisse verschachtelt. Obwohl Objektspeicher im Allgemeinen eine geringere Leistung als Datei- oder Blockspeicher bieten, sind sie deutlich skalierbarer. StorageGRID Buckets können Petabyte an Daten und Milliarden von Objekten enthalten.

Warum StorageGRID als FabricPool Cloud-Ebene verwenden?

FabricPool kann ONTAP Daten auf eine Reihe von Objektspeicheranbietern verteilen, darunter StorageGRID. Im Gegensatz zu öffentlichen Clouds, die möglicherweise eine maximale Anzahl unterstützter Eingabe-/Ausgabevorgänge pro Sekunde (IOPS) auf Bucket- oder Containerebene festlegen, skaliert die Leistung von StorageGRID mit der Anzahl der Knoten in einem System. Durch die Verwendung von StorageGRID als FabricPool -Cloud-Ebene können Sie Ihre kalten Daten in Ihrer eigenen privaten Cloud aufbewahren, um höchste Leistung und vollständige Kontrolle über Ihre Daten zu erzielen.

Darüber hinaus ist keine FabricPool -Lizenz erforderlich, wenn Sie StorageGRID als Cloud-Ebene verwenden.

Erforderliche Informationen zum Anhängen von StorageGRID als Cloud-Ebene

Bevor Sie StorageGRID als Cloud-Tier für FabricPool anhängen können, müssen Sie Konfigurationsschritte in StorageGRID durchführen und bestimmte Werte zur Verwendung in ONTAP abrufen.

Welche Werte benötige ich?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen, und wie diese Werte von ONTAP und dem DNS-Server verwendet werden.

Wert	Wo der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Hafen	StorageGRID > Load Balancer-Endpunkt	ONTAP System Manager > Cloud-Tier hinzufügen
SSL-Zertifikat	StorageGRID > Load Balancer-Endpunkt	ONTAP System Manager > Cloud-Tier hinzufügen
Servername (FQDN)	StorageGRID > Load Balancer-Endpunkt	DNS-Eintrag
Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	ONTAP System Manager > Cloud-Tier hinzufügen
Bucket-/Containername	StorageGRID > Mandant und Bucket	ONTAP System Manager > Cloud-Tier hinzufügen

Wie komme ich an diese Werte?

Je nach Ihren Anforderungen können Sie die benötigten Informationen auf folgende Weise abrufen:

- Verwenden Sie die"FabricPool -Setup-Assistent" . Der FabricPool -Setup-Assistent unterstützt Sie bei der schnellen Konfiguration der erforderlichen Werte in StorageGRID und gibt eine Datei aus, mit der Sie ONTAP System Manager konfigurieren können. Der Assistent führt Sie durch die erforderlichen Schritte und hilft sicherzustellen, dass Ihre Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.

- Konfigurieren Sie jedes Element manuell. Geben Sie dann die Werte in den ONTAP System Manager oder die ONTAP CLI ein. Gehen Sie folgendermaßen vor:
  a. "Konfigurieren einer Hochverfügbarkeitsgruppe (HA) für FabricPool" .
  b. "Erstellen Sie einen Load Balancer-Endpunkt für FabricPool" .
  c. "Erstellen Sie ein Mandantenkonto für FabricPool" .
  d. Sign in beim Mandantenkonto an und"Erstellen Sie den Bucket und die Zugriffsschlüssel für den Root-Benutzer" .
  e. Erstellen Sie eine ILM-Regel für FabricPool -Daten und fügen Sie sie Ihren aktiven ILM-Richtlinien hinzu. Sehen "Konfigurieren von ILM für FabricPool -Daten" .
  f. Optional:"Erstellen Sie eine Datenverkehrsklassifizierungsrichtlinie für FabricPool" .

Verwenden des FabricPool -Setup-Assistenten

Verwenden des FabricPool -Setup-Assistenten: Überlegungen und Anforderungen

Sie können den FabricPool -Setup-Assistenten verwenden, um StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Ebene zu konfigurieren. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie die erforderlichen Details in ONTAP System Manager eingeben.

Wann Sie den FabricPool -Setup-Assistenten verwenden sollten

Der FabricPool -Setup-Assistent führt Sie durch jeden Schritt der Konfiguration von StorageGRID für die Verwendung mit FabricPool und konfiguriert automatisch bestimmte Entitäten für Sie, z. B. die ILM- und Verkehrsklassifizierungsrichtlinien. Beim Abschließen des Assistenten laden Sie eine Datei herunter, mit der Sie Werte in ONTAP System Manager eingeben können. Verwenden Sie den Assistenten, um Ihr System schneller zu konfigurieren und sicherzustellen, dass Ihre Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.

Vorausgesetzt, Sie verfügen über Root-Zugriffsberechtigungen, können Sie den FabricPool -Setup-Assistenten abschließen, wenn Sie mit der Verwendung des StorageGRID Grid Manager beginnen, oder Sie können zu einem späteren Zeitpunkt auf den Assistenten zugreifen und ihn abschließen. Abhängig von Ihren Anforderungen können Sie einige oder alle erforderlichen Elemente auch manuell konfigurieren und dann mithilfe des Assistenten die von ONTAP benötigten Werte in einer einzigen Datei zusammenstellen.

Verwenden Sie den FabricPool -Setup-Assistenten, es sei denn, Sie wissen, dass Sie besondere Anforderungen haben oder Ihre Implementierung erhebliche Anpassungen erfordert.

Vor der Verwendung des Assistenten

Bestätigen Sie, dass Sie diese erforderlichen Schritte abgeschlossen haben.

Überprüfen Sie die bewährten Methoden

- Sie verfügen über ein allgemeines Verständnis der"Informationen, die zum Anhängen von StorageGRID als Cloud-Ebene erforderlich sind" .
- Sie haben die Best Practices von FabricPool für Folgendes überprüft:
  - "Hochverfügbarkeitsgruppen (HA)"

- "Lastenausgleich"
- "ILM-Regeln und -Richtlinien"

Beziehen Sie IP-Adressen und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine HA-Gruppe konfigurieren, wissen Sie, mit welchen Knoten ONTAP 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 zur Trennung des FabricPool -Verkehrs verwenden möchten, 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 von ONTAP verwendete Mandantenkonto haben sollte. 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. Sehen "DNS-Server konfigurieren" .
- Wenn Sie virtuelle S3-Hosting-Anfragen verwenden möchten, müssen Sie"konfigurierte S3-Endpunktdomänennamen" . ONTAP verwendet standardmäßig URLs im Pfadstil, es wird jedoch die Verwendung von Anfragen im virtuellen gehosteten Stil empfohlen.

Überprüfen Sie die Anforderungen für Load Balancer und Sicherheitszertifikate

Wenn Sie den StorageGRID Load Balancer verwenden möchten, haben Sie die allgemeinen"Überlegungen zum Lastenausgleich" . 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.

Bestätigen Sie die Konfiguration des ILM-Speicherpools

Wenn Sie StorageGRID 11.6 oder früher ursprünglich installiert haben, haben Sie den zu verwendenden Speicherpool konfiguriert. Im Allgemeinen sollten Sie für jede StorageGRID -Site, die Sie zum Speichern von ONTAP -Daten verwenden, einen Speicherpool erstellen.

> Diese Voraussetzung gilt nicht, wenn Sie StorageGRID 11.7 oder 11.8 ursprünglich installiert haben. Wenn Sie eine dieser Versionen zum ersten Mal installieren, werden für jeden Standort automatisch Speicherpools erstellt.

Beziehung zwischen ONTAP und der StorageGRID Cloud-Ebene

Der FabricPool Assistent führt Sie durch den Prozess der Erstellung einer einzelnen StorageGRID Cloud-Ebene, die einen StorageGRID Mandanten, einen Satz Zugriffsschlüssel und einen StorageGRID Bucket umfasst. Sie können diese StorageGRID Cloud-Ebene an eine oder mehrere lokale ONTAP Ebenen anhängen.

Das Anhängen einer einzelnen Cloud-Ebene an mehrere lokale Ebenen in einem Cluster ist die allgemeine Best Practice. Abhängig von Ihren Anforderungen möchten Sie möglicherweise jedoch mehr als einen Bucket oder sogar mehr als einen StorageGRID Mandanten für die lokalen Ebenen in einem einzelnen Cluster verwenden. Durch die Verwendung unterschiedlicher Buckets und Mandanten können Sie Daten und Datenzugriff zwischen lokalen ONTAP Ebenen isolieren, die Konfiguration und Verwaltung ist jedoch etwas komplexer.

NetApp empfiehlt nicht, eine einzelne Cloud-Ebene an lokale Ebenen in mehreren Clustern anzuhängen.

> Die Best Practices für die Verwendung von StorageGRID mit NetApp MetroCluster™ und FabricPool Mirror finden Sie unter "TR-4598: FabricPool Best Practices in ONTAP" .

Optional: Verwenden Sie für jede lokale Ebene einen anderen Bucket

Um mehr als einen Bucket für die lokalen Tiers in einem ONTAP Cluster zu verwenden, fügen Sie mehr als ein StorageGRID Cloud-Tier in ONTAP hinzu. Jede Cloud-Ebene teilt sich dieselbe HA-Gruppe, denselben Load Balancer-Endpunkt, denselben Mandanten und dieselben Zugriffsschlüssel, verwendet jedoch einen anderen Container (StorageGRID Bucket). Befolgen Sie diese allgemeinen Schritte:

1. Schließen Sie im StorageGRID Grid Manager den FabricPool -Setup-Assistenten für die erste Cloud-Ebene ab.
2. Fügen Sie im ONTAP System Manager eine Cloud-Ebene hinzu und verwenden Sie die von StorageGRID heruntergeladene Datei, um die erforderlichen Werte bereitzustellen.
3. Melden Sie sich im StorageGRID Tenant Manager bei dem vom Assistenten erstellten Mandanten an und erstellen Sie einen zweiten Bucket.
4. Schließen Sie den FabricPool Assistenten erneut ab. Wählen Sie die vorhandene HA-Gruppe, den Load Balancer-Endpunkt und den Mandanten aus. Wählen Sie dann den neuen Bucket aus, den Sie manuell erstellt haben. Erstellen Sie eine neue ILM-Regel für den neuen Bucket und aktivieren Sie eine ILM-Richtlinie, um diese Regel einzuschließen.
5. Fügen Sie von ONTAP aus eine zweite Cloud-Ebene hinzu, geben Sie jedoch den neuen Bucket-Namen an.

Optional: Verwenden Sie für jede lokale Ebene einen anderen Mandanten und Bucket

Um mehr als einen Mandanten und verschiedene Zugriffsschlüsselsätze für die lokalen Ebenen in einem ONTAP Cluster zu verwenden, fügen Sie mehr als eine StorageGRID Cloud-Ebene in ONTAP hinzu. Jede Cloud-Ebene teilt sich dieselbe HA-Gruppe und denselben Load Balancer-Endpunkt, verwendet jedoch einen anderen Mandanten, andere Zugriffsschlüssel und einen anderen Container (StorageGRID Bucket). Befolgen Sie diese allgemeinen Schritte:

1. Schließen Sie im StorageGRID Grid Manager den FabricPool -Setup-Assistenten für die erste Cloud-Ebene ab.
2. Fügen Sie im ONTAP System Manager eine Cloud-Ebene hinzu und verwenden Sie die von StorageGRID heruntergeladene Datei, um die erforderlichen Werte bereitzustellen.
3. Schließen Sie den FabricPool Assistenten erneut ab. Wählen Sie die vorhandene HA-Gruppe und den Load Balancer-Endpunkt aus. Erstellen Sie einen neuen Mandanten und Bucket. Erstellen Sie eine neue ILM-Regel für den neuen Bucket und aktivieren Sie eine ILM-Richtlinie, um diese Regel einzuschließen.
4. Fügen Sie von ONTAP aus eine zweite Cloud-Ebene hinzu, geben Sie jedoch den neuen Zugriffsschlüssel, den geheimen Schlüssel und den Bucket-Namen an.

Greifen Sie auf den FabricPool -Setup-Assistenten zu und schließen Sie ihn ab

Sie können den FabricPool -Setup-Assistenten verwenden, um StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Ebene zu konfigurieren.

Bevor Sie beginnen

- Sie haben die"Überlegungen und Anforderungen" zur Verwendung des FabricPool -Setup-Assistenten.

> Wenn Sie StorageGRID für die Verwendung mit einer anderen S3-Clientanwendung konfigurieren möchten, gehen Sie zu"Verwenden Sie den S3-Setup-Assistenten" .

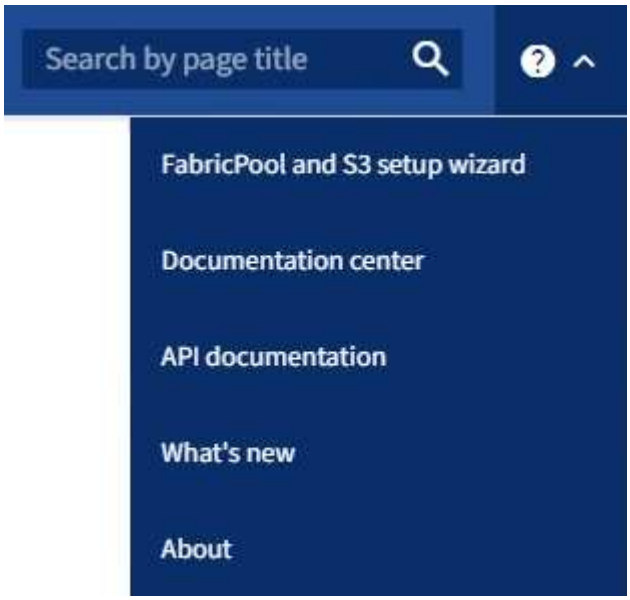
- Sie haben die"Root-Zugriffsberechtigung" .

Zugriff auf den Assistenten

Sie können den FabricPool -Setup-Assistenten abschließen, wenn Sie mit der Verwendung des StorageGRID Grid Manager beginnen, oder Sie können zu einem späteren Zeitpunkt auf den Assistenten zugreifen und ihn abschließen.

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 FabricPool der Seite des FabricPool und S3-Setup-Assistenten die Option **Jetzt konfigurieren** aus.

   Schritt 1 von 9: HA-Gruppe konfigurieren wird angezeigt.

Schritt 1 von 9: HA-Gruppe konfigurieren

Eine Hochverfügbarkeitsgruppe (HA) 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 von FabricPool Datenverbindungen aufrechtzuerhalten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Dienst bereitzustellen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast mit geringen Auswirkungen auf den FabricPool -Betrieb verwalten.

Einzelheiten zu dieser Aufgabe finden Sie unter"Verwalten von Hochverfügbarkeitsgruppen" Und"Best Practices für 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 9: Load Balancer-Endpunkt konfigurieren .
2. Um den StorageGRID Load Balancer zu verwenden, erstellen Sie eine neue HA-Gruppe oder verwenden Sie eine vorhandene HA-Gruppe.

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 zurückversetzt.

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)	Optional. Wenn sich die für den Zugriff auf StorageGRID verwendeten ONTAP -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 und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein. 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 FabricPool 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 Dropdown-Liste **HA-Gruppe auswählen** aus.

b. Wählen Sie **Weiter**, um zum Schritt „Lastenausgleich“ zu gelangen.

Schritt 2 von 9: Load Balancer-Endpunkt konfigurieren

StorageGRID verwendet einen Load Balancer, um die Arbeitslast von Clientanwendungen wie FabricPool 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 in den allgemeinen"Überlegungen zum Lastenausgleich" und die"Best Practices für den Lastenausgleich für FabricPool" .

Schritte

1. Wählen oder erstellen Sie einen StorageGRID Load Balancer-Endpunkt oder verwenden Sie einen externen Load Balancer.

Endpunkt erstellen

a. Wählen Sie **Endpunkt erstellen**.

b. Füllen Sie für den Schritt **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.

c. 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.

d. 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. **Alle Mandanten zulassen** ist fast immer die geeignete Option für den für FabricPool verwendeten Load Balancer-Endpunkt. Sie müssen diese Option auswählen, wenn Sie den FabricPool -Setup -Assistenten für ein neues StorageGRID -System verwenden und noch keine Mandantenkonten erstellt haben.
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.

e. 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	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID -Zertifikats hochgeladen oder generiert haben. Sehen"Konfigurieren von S3-API-Zertifikaten" für Details.

f. Wählen Sie **Fertig**, um zum FabricPool -Setup-Assistenten zurückzukehren.

g. 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

a. Wählen Sie den Namen eines vorhandenen Endpunkts aus der Dropdown-Liste **Wählen Sie einen Load Balancer-Endpunkt** aus.

b. Wählen Sie **Weiter**, um zum Schritt „Mandant und Bucket“ zu gelangen.

Externen Load Balancer verwenden

a. Füllen Sie die folgenden Felder für den externen Lastenausgleich aus.

Feld	Beschreibung
FQDN	Der vollqualifizierte Domänenname (FQDN) des externen Load Balancers.
Hafen	Die Portnummer, die FabricPool für die Verbindung mit dem externen Lastenausgleich verwendet.
Zertifikat	Kopieren Sie das Serverzertifikat für den externen Load Balancer und fügen Sie es in dieses Feld ein.

b. Wählen Sie **Weiter**, um zum Schritt „Mandant und Bucket“ zu gelangen.

Schritt 3 von 9: Mieter und Bucket

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. Sie müssen einen StorageGRID Mandanten erstellen, bevor Sie den Bucket erstellen können, den FabricPool verwenden wird.

Ein Bucket ist ein Container zum Speichern der Objekte und Objektmetadaten eines Mandanten. Obwohl einige Mandanten möglicherweise über viele Buckets verfügen, können Sie mit dem Assistenten jeweils nur einen Mandanten und einen Bucket erstellen oder auswählen. Sie können den Tenant Manager später verwenden, um alle weiteren benötigten Buckets hinzuzufügen.

Sie können einen neuen Mandanten und Bucket für die Verwendung von FabricPool erstellen oder einen vorhandenen Mandanten und Bucket auswählen. Wenn Sie einen neuen Mandanten erstellen, erstellt das System automatisch die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer des Mandanten.

Einzelheiten zu dieser Aufgabe finden Sie unter"Erstellen Sie ein Mandantenkonto für FabricPool" Und"Erstellen Sie einen S3-Bucket und erhalten Sie einen Zugriffsschlüssel" .

Schritte

Erstellen Sie einen neuen Mandanten und Bucket oder wählen Sie einen vorhandenen Mandanten aus.

Neuer Mieter und Eimer

1. Um einen neuen Mandanten und Bucket zu erstellen, geben Sie einen **Mandantennamen** ein. Beispiel: `FabricPool tenant` .
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.
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.

3. Geben Sie für **Bucket-Name** den Namen des Buckets ein, den FabricPool zum Speichern von ONTAP Daten verwenden wird. Beispiel: `fabricpool-bucket` .

   Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht mehr ändern.

4. 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**, um den Mandanten und den Bucket zu erstellen und zum Schritt „Daten herunterladen“ zu gelangen.

Wählen Sie Mandanten und Bucket aus

Das vorhandene Mandantenkonto muss mindestens einen Bucket haben, für den die Versionierung nicht aktiviert ist. Sie können kein vorhandenes Mandantenkonto auswählen, wenn für diesen Mandanten kein Bucket vorhanden ist.

1. Wählen Sie den vorhandenen Mandanten aus der Dropdown-Liste **Mandantenname** aus.
2. Wählen Sie den vorhandenen Bucket aus der Dropdown-Liste **Bucket-Name** aus.

   FabricPool unterstützt keine Objektversionierung, daher werden Buckets mit aktivierter Versionierung nicht angezeigt.

   Wählen Sie keinen Bucket aus, bei dem S3 Object Lock für die Verwendung mit FabricPool aktiviert ist.

3. Wählen Sie **Weiter**, um zum Schritt „Daten herunterladen“ zu gelangen.

Schritt 4 von 9: ONTAP -Einstellungen herunterladen

In diesem Schritt laden Sie eine Datei herunter, mit der Sie Werte in ONTAP System Manager eingeben können.

Schritte

1. Wählen Sie optional das Kopiersymbol ( ), um sowohl die Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.

   Diese Werte sind in der Download-Datei enthalten, Sie möchten sie jedoch möglicherweise separat speichern.

2. Wählen Sie * ONTAP -Einstellungen herunterladen*, um eine Textdatei herunterzuladen, die die bisher eingegebenen Werte enthält.

   Der `ONTAP_FabricPool_settings_bucketname.txt` Die Datei enthält die Informationen, die Sie zum Konfigurieren von StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Ebene benötigen, darunter:

   - Verbindungsdetails des Load Balancers, einschließlich Servername (FQDN), Port und Zertifikat
   - Bucket-Name
   - Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel für den Root-Benutzer des Mandantenkontos

3. Speichern Sie die kopierten Schlüssel und die heruntergeladene Datei an einem sicheren Ort.

   Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert, die ONTAP Einstellungen heruntergeladen oder beides getan 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 das Kontrollkästchen, um zu bestätigen, dass Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter**, um zum Schritt „ILM-Speicherpool“ zu gelangen.

Schritt 5 von 9: Speicherpool auswählen

Ein Speicherpool ist eine Gruppe von Speicherknoten. Wenn Sie einen Speicherpool auswählen, legen Sie fest, welche Knoten StorageGRID zum Speichern der von ONTAP abgestuften Daten verwenden wird.

Einzelheiten zu diesem Schritt finden Sie unter"Erstellen eines Speicherpools" .

Schritte

1. Wählen Sie aus der Dropdown-Liste **Site** die StorageGRID -Site aus, die Sie für die von ONTAP abgestuften Daten verwenden möchten.
2. Wählen Sie aus der Dropdown-Liste **Speicherpool** den Speicherpool für diese Site aus.

   Der Speicherpool für einen Standort umfasst alle Speicherknoten an diesem Standort.

3. Wählen Sie **Weiter**, um zum ILM-Regelschritt zu gelangen.

Schritt 6 von 9: ILM-Regel für FabricPool überprüfen

Regeln für das Information Lifecycle Management (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System.

Der FabricPool -Setup-Assistent erstellt automatisch die empfohlene ILM-Regel für die Verwendung von FabricPool . Diese Regel gilt nur für den von Ihnen angegebenen Bucket. Es verwendet 2+1-Erasure-Coding an einem einzigen Standort, um die von ONTAP abgestuften Daten zu speichern.

Einzelheiten zu diesem Schritt finden Sie unter"ILM-Regel erstellen" Und"Best Practices für die Verwendung von ILM mit FabricPool -Daten" .

Schritte

1. Überprüfen Sie die Regeldetails.

Feld	Beschreibung
Regelname	Automatisch generiert und kann nicht geändert werden
Beschreibung	Automatisch generiert und kann nicht geändert werden
Filter	Der Bucket-Name Diese Regel gilt nur für Objekte, die in dem von Ihnen angegebenen Bucket gespeichert sind.
Referenzzeit	Aufnahmezeit Die Platzierungsanweisung beginnt, wenn Objekte erstmals im Bucket gespeichert werden.
Platzierungsanweisung	Verwenden Sie 2+1 Erasure Coding

2. Sortieren Sie das Aufbewahrungsdiagramm nach **Zeitraum** und **Speicherpool**, um die Platzierungsanweisung zu bestätigen.
   - Der **Zeitraum** für die Regel ist **Tag 0 – für immer**. **Tag 0** bedeutet, dass die Regel angewendet wird, wenn Daten von ONTAP abgestuft werden. **Für immer** bedeutet, dass StorageGRID ILM keine Daten löscht, die von ONTAP abgestuft wurden.
   - Der **Speicherpool** für die Regel ist der von Ihnen ausgewählte Speicherpool. **EC 2+1** bedeutet, dass die Daten mit 2+1-Löschcodierung gespeichert werden. Jedes Objekt wird als zwei Datenfragmente und ein Paritätsfragment gespeichert. Die drei Fragmente für jedes Objekt werden auf verschiedenen Speicherknoten an einem einzigen Standort gespeichert.
3. Wählen Sie **Erstellen und fortfahren** aus, um diese Regel zu erstellen und zum ILM-Richtlinienschritt zu gelangen.

Schritt 7 von 9: ILM-Richtlinie prüfen und aktivieren

Nachdem der FabricPool -Setup-Assistent die ILM-Regel für die FabricPool Verwendung erstellt hat, erstellt er eine ILM-Richtlinie. Sie müssen diese Richtlinie sorgfältig simulieren und überprüfen, bevor Sie sie aktivieren.

Einzelheiten zu diesem Schritt finden Sie unter"ILM-Richtlinie erstellen" Und"Best Practices für die

Verwendung von ILM mit FabricPool -Daten" .

> Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese Richtlinie, um die Platzierung, Dauer und den Datenschutz aller Objekte im Grid zu verwalten, einschließlich vorhandener und neu aufgenommener Objekte. In einigen Fällen kann die Aktivierung einer neuen Richtlinie dazu führen, dass vorhandene Objekte an neue Speicherorte verschoben werden.

> Um Datenverlust zu vermeiden, verwenden Sie keine ILM-Regel, die FabricPool Cloud-Tier-Daten ablaufen lässt oder löscht. Legen Sie die Aufbewahrungsdauer auf **für immer** fest, um sicherzustellen, dass FabricPool Objekte nicht von StorageGRID ILM gelöscht werden.

Schritte

1. Aktualisieren Sie optional den vom System generierten **Richtliniennamen**. Standardmäßig hängt das System „+ FabricPool“ an den Namen Ihrer aktiven oder inaktiven Richtlinie an, Sie können jedoch auch Ihren eigenen Namen angeben.
2. Überprüfen Sie die Liste der Regeln in der inaktiven Richtlinie.
   - Wenn Ihr Grid keine inaktive ILM-Richtlinie hat, erstellt der Assistent eine inaktive Richtlinie, indem er Ihre aktive Richtlinie klont und die neue Regel oben hinzufügt.
   - Wenn Ihr Grid bereits über eine inaktive ILM-Richtlinie verfügt und diese Richtlinie dieselben Regeln und dieselbe Reihenfolge wie die aktive ILM-Richtlinie verwendet, fügt der Assistent die neue Regel oben in der inaktiven Richtlinie hinzu.
   - Wenn Ihre inaktive Richtlinie andere Regeln oder eine andere Reihenfolge als die aktive Richtlinie enthält, erstellt der Assistent eine neue inaktive Richtlinie, indem er Ihre aktive Richtlinie klont und die neue Regel oben hinzufügt.
3. Überprüfen Sie die Reihenfolge der Regeln in der neuen inaktiven Richtlinie.

   Da die FabricPool Regel die erste Regel ist, werden alle Objekte im FabricPool Bucket platziert, bevor die anderen Regeln in der Richtlinie ausgewertet werden. Objekte in anderen Buckets werden durch nachfolgende Regeln in der Richtlinie platziert.
4. Sehen Sie sich das Aufbewahrungsdiagramm an, um zu erfahren, wie verschiedene Objekte aufbewahrt werden.
   a. Wählen Sie **Alle erweitern** aus, um ein Aufbewahrungsdiagramm für jede Regel in der inaktiven Richtlinie anzuzeigen.
   b. Wählen Sie **Zeitraum** und **Speicherpool** aus, um das Aufbewahrungsdiagramm zu überprüfen. Bestätigen Sie, dass alle Regeln, die für den FabricPool Bucket oder -Mandanten gelten, Objekte **für immer** aufbewahren.
5. Wenn Sie die inaktive Richtlinie überprüft haben, wählen Sie **Aktivieren und fortfahren**, um die Richtlinie zu aktivieren und mit dem Schritt zur Verkehrsklassifizierung fortzufahren.

> Fehler in einer ILM-Richtlinie können zu irreparablem Datenverlust führen. Lesen Sie die Richtlinie vor der Aktivierung sorgfältig durch.

Schritt 8 von 9: Erstellen einer Verkehrsklassifizierungsrichtlinie

Optional kann der FabricPool Setup-Assistent eine Verkehrsklassifizierungsrichtlinie erstellen, mit der Sie die FabricPool Arbeitslast überwachen können. Die vom System erstellte Richtlinie verwendet eine Übereinstimmungsregel, um den gesamten Netzwerkverkehr zu identifizieren, der mit dem von Ihnen erstellten

Bucket in Zusammenhang steht. Diese Richtlinie überwacht nur den Datenverkehr. Sie beschränkt den Datenverkehr für FabricPool oder andere Clients nicht.

Einzelheiten zu diesem Schritt finden Sie unter"Erstellen einer Datenverkehrsklassifizierungsrichtlinie für FabricPool" .

Schritte

1. Überprüfen Sie die Richtlinie.
2. Wenn Sie diese Richtlinie zur Verkehrsklassifizierung erstellen möchten, wählen Sie **Erstellen und fortfahren**.

   Sobald FabricPool mit der Datenverteilung auf StorageGRID beginnt, können Sie auf der Seite „Richtlinien zur Verkehrsklassifizierung“ die Netzwerkverkehrsmetriken für diese Richtlinie anzeigen. Später können Sie auch Regeln hinzufügen, um andere Workloads zu begrenzen und sicherzustellen, dass der FabricPool Workload die meiste Bandbreite zur Verfügung steht.

3. Andernfalls wählen Sie **Diesen Schritt überspringen**.

Schritt 9 von 9: Zusammenfassung der Überprüfung

Die Zusammenfassung enthält Details zu den von Ihnen konfigurierten Elementen, einschließlich des Namens des Load Balancers, des Mandanten und des Buckets, der Datenverkehrsklassifizierungsrichtlinie und der aktiven ILM-Richtlinie.

Schritte

1. Lesen Sie die Zusammenfassung.
2. Wählen Sie **Fertig**.

Nächste Schritte

Führen Sie nach Abschluss des FabricPool Assistenten diese zusätzlichen Schritte aus.

Schritte

1. Gehe zu"ONTAP System Manager konfigurieren" um die gespeicherten Werte einzugeben und die ONTAP -Seite der Verbindung abzuschließen. Sie müssen StorageGRID als Cloud-Ebene hinzufügen, die Cloud-Ebene an eine lokale Ebene anhängen, um einen FabricPool zu erstellen, und Richtlinien für die Volume-Ebene festlegen.
2. Gehe zu"Konfigurieren des DNS-Servers" und stellen Sie sicher, dass das DNS einen Datensatz enthält, um den StorageGRID -Servernamen (vollqualifizierter Domänenname) jeder StorageGRID -IP-Adresse zuzuordnen, die Sie verwenden werden.
3. Gehe zu"Weitere Best Practices für StorageGRID und FabricPool" um die Best Practices für StorageGRID -Auditprotokolle und andere globale Konfigurationsoptionen kennenzulernen.

StorageGRID manuell konfigurieren

Erstellen einer Hochverfügbarkeitsgruppe (HA) für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, können Sie optional eine oder mehrere Hochverfügbarkeitsgruppen (HA) erstellen. 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 von FabricPool Datenverbindungen aufrechtzuerhalten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Dienst bereitzustellen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast mit geringen Auswirkungen auf den FabricPool -Betrieb verwalten.

Einzelheiten zu dieser Aufgabe finden Sie unter"Verwalten von Hochverfügbarkeitsgruppen" . Um diese Aufgabe mit dem FabricPool -Setup-Assistenten abzuschließen, gehen Sie zu"Greifen Sie auf den FabricPool -Setup-Assistenten zu und schließen Sie ihn ab" .

Bevor Sie beginnen

- Sie haben die"Best Practices für Hochverfügbarkeitsgruppen" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Wenn Sie ein VLAN verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Sehen "Konfigurieren von VLAN-Schnittstellen" .

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.
2. Wählen Sie **Erstellen**.
3. 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.

4. 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.

5. 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 zurückversetzt.

6. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation – eine IPv4-Adresse, gefolgt von einem Schrägstrich und der Subnetzlänge (0–32). Für die Netzwerkadresse dürfen keine Hostbits gesetzt sein. Beispiel: `192.16.0.0/22` .
Gateway-IP-Adresse (optional)	Optional. Wenn sich die für den Zugriff auf StorageGRID verwendeten ONTAP -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.
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.

7. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**.

Erstellen Sie einen Load Balancer-Endpunkt für FabricPool

StorageGRID verwendet einen Load Balancer, um die Arbeitslast von Clientanwendungen wie FabricPool zu verwalten. Durch Lastenausgleich werden Geschwindigkeit und Verbindungskapazität über mehrere Speicherknoten hinweg maximiert.

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, müssen Sie einen Load Balancer-Endpunkt konfigurieren und ein Load Balancer-Endpunktzertifikat hochladen oder generieren, das zum Sichern der Verbindung zwischen ONTAP und StorageGRID verwendet wird.

Um diese Aufgabe mit dem FabricPool -Setup-Assistenten abzuschließen, gehen Sie zu"Greifen Sie auf den FabricPool -Setup-Assistenten zu und schließen Sie ihn ab" .

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Sie haben die allgemeinen"Überlegungen zum Lastenausgleich" sowie die"Best Practices für den Lastenausgleich für FabricPool" .

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**.
2. Wählen Sie **Erstellen**.
3. 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. Diese Ports sind auf Admin-Knoten reserviert. **Hinweis:** Von anderen Grid-Diensten verwendete Ports sind nicht zulässig. Siehe die"Netzwerkportreferenz" . Sie geben diese Nummer an ONTAP weiter, wenn Sie StorageGRID als FabricPool Cloud-Tier anhängen.
Client-Typ	Wählen Sie **S3**.
Netzwerkprotokoll	Wählen Sie **HTTPS**. **Hinweis**: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

4. Geben Sie 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.
Knotenschnittstellen	Clients müssen die IP-Adressen (oder entsprechenden FQDNs) ausgewählter Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.

Modus	Beschreibung
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.

5. 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. **Alle Mandanten zulassen** ist fast immer die geeignete Option für den für FabricPool verwendeten Load Balancer-Endpunkt. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt 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.

6. 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	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID -Zertifikats hochgeladen oder generiert haben. Sehen"Konfigurieren von S3-API-Zertifikaten" für Details.

7. Wählen Sie **Erstellen**.

Es kann bis zu 15 Minuten dauern, bis Änderungen an einem Endpunktzertifikat auf alle Knoten angewendet werden.

Erstellen Sie ein Mandantenkonto für FabricPool

Sie müssen im Grid Manager ein Mandantenkonto für die Verwendung von FabricPool erstellen.

Mandantenkonten ermöglichen Clientanwendungen, Objekte auf StorageGRID zu speichern und abzurufen. Jedes Mandantenkonto verfügt über eine eigene Konto-ID, autorisierte Gruppen und Benutzer, Buckets und Objekte.

Einzelheiten zu dieser Aufgabe finden Sie unter"Mieterkonto erstellen" . Um diese Aufgabe mit dem FabricPool -Setup-Assistenten abzuschließen, gehen Sie zu"Greifen Sie auf den FabricPool -Setup-Assistenten zu und schließen Sie ihn ab" .

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **MIETER** aus.
2. Wählen Sie **Erstellen**.
3. Geben Sie für die Schritte „Details eingeben“ die folgenden Informationen ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Beim Anlegen des Mandantenkontos erhält dieses eine eindeutige, numerische Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mieters.
Client-Typ	Muss für FabricPool*S3* sein.
Speicherkontingent (optional)	Lassen Sie dieses Feld für FabricPool leer.

4. Für den Schritt „Berechtigungen auswählen“:
   a. Wählen Sie nicht **Plattformdienste zulassen** aus.

      FabricPool Mandanten müssen normalerweise keine Plattformdienste wie die CloudMirror-Replikation verwenden.

   b. Wählen Sie optional **Eigene Identitätsquelle verwenden** aus.
   c. Wählen Sie nicht **S3 Select zulassen** aus.

      FabricPool -Mieter müssen S3 Select normalerweise nicht verwenden.

   d. Wählen Sie optional **Grid-Föderationsverbindung verwenden**, um dem Mandanten die Verwendung eines"Netzverbundanschluss" für Kontoklonen und Cross-Grid-Replikation. Wählen Sie dann die zu verwendende Grid-Föderation-Verbindung aus.

5. Geben Sie im Schritt „Root-Zugriff definieren“ an, welcher Benutzer die anfängliche Root-Zugriffsberechtigung für das Mandantenkonto haben soll, 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.
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.

6. Wählen Sie **Mandanten erstellen**.

Erstellen Sie einen S3-Bucket und erhalten Sie Zugriffsschlüssel

Bevor Sie StorageGRID mit einer FabricPool -Workload verwenden, müssen Sie einen S3-Bucket für Ihre FabricPool -Daten erstellen. Sie müssen außerdem einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel für das Mandantenkonto erhalten, das Sie für FabricPool verwenden.

Einzelheiten zu dieser Aufgabe finden Sie unter"S3-Bucket erstellen" Und"Erstellen Sie Ihre eigenen S3-Zugriffsschlüssel" . Um diese Aufgabe mit dem FabricPool -Setup-Assistenten abzuschließen, gehen Sie zu"Greifen Sie auf den FabricPool -Setup-Assistenten zu und schließen Sie ihn ab" .

Bevor Sie beginnen

- Sie haben ein Mandantenkonto für die Verwendung von FabricPool erstellt.
- Sie haben Root-Zugriff auf das Mandantenkonto.

Schritte

1. Sign in .

   Sie können einen der folgenden Schritte ausführen:

   - Wählen Sie auf der Seite „Mandantenkonten“ im Grid Manager den Link * Sign in* für den Mandanten aus und geben Sie Ihre Anmeldeinformationen ein.
   - Geben Sie die URL für das Mandantenkonto in einen Webbrowser ein und geben Sie Ihre Anmeldeinformationen ein.

2. Erstellen Sie einen S3-Bucket für FabricPool -Daten.

   Sie müssen für jeden ONTAP Cluster, den Sie verwenden möchten, einen eindeutigen Bucket erstellen.

a. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
b. Wählen Sie **Bucket erstellen**.
c. Geben Sie den Namen des StorageGRID Buckets ein, den Sie mit FabricPool verwenden möchten. Beispiel: `fabricpool-bucket` .

> Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht mehr ändern.

d. Wählen Sie die Region für diesen Bucket aus.

   Standardmäßig werden alle Buckets im `us-east-1` Region.

e. Wählen Sie **Weiter**.
f. Wählen Sie **Bucket erstellen**.

> Wählen Sie für den FabricPool Bucket nicht **Objektversionierung aktivieren** aus. Bearbeiten Sie einen FabricPool Bucket auch nicht, um **Verfügbar** oder eine nicht standardmäßige Konsistenz zu verwenden. Die empfohlene Bucket-Konsistenz für FabricPool -Buckets ist **Lesen nach neuem Schreiben**, was die Standardkonsistenz für einen neuen Bucket ist.

3. Erstellen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel.

a. Wählen Sie **SPEICHER (S3)** > **Meine Zugriffsschlüssel**.
b. Wählen Sie **Schlüssel erstellen**.
c. Wählen Sie **Zugriffsschlüssel erstellen**.
d. Kopieren Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einen sicheren Ort oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.

   Sie geben diese Werte in ONTAP ein, wenn Sie StorageGRID als FabricPool Cloud-Tier konfigurieren.

> Wenn Sie in Zukunft einen neuen Zugriffsschlüssel und einen neuen geheimen Zugriffsschlüssel in StorageGRID generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls könnte ONTAP vorübergehend den Zugriff auf StorageGRID verlieren.

Konfigurieren von ILM für FabricPool -Daten

Sie können diese einfache Beispielrichtlinie als Ausgangspunkt für Ihre eigenen ILM-Regeln und -Richtlinien verwenden.

In diesem Beispiel wird davon ausgegangen, dass Sie die ILM-Regeln und eine ILM-Richtlinie für ein StorageGRID -System entwerfen, das über vier Speicherknoten in einem einzigen Rechenzentrum in Denver, Colorado, verfügt. Die FabricPool Daten in diesem Beispiel verwenden einen Bucket namens `fabricpool-bucket` .

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt. Weitere Informationen finden Sie unter"Objekte mit ILM verwalten" .

Um Datenverlust zu vermeiden, verwenden Sie keine ILM-Regel, die FabricPool Cloud-Tier-Daten ablaufen lässt oder löscht. Legen Sie die Aufbewahrungsdauer auf **für immer** fest, um sicherzustellen, dass FabricPool Objekte nicht von StorageGRID ILM gelöscht werden.

Bevor Sie beginnen

- Sie haben die"Best Practices für die Verwendung von ILM mit FabricPool -Daten" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"ILM- oder Root-Zugriffsberechtigung" .
- Wenn Sie von einer früheren StorageGRID -Version auf StorageGRID 11.9 aktualisiert haben, haben Sie den zu verwendenden Speicherpool konfiguriert. Im Allgemeinen sollten Sie für jede StorageGRID -Site, die Sie zum Speichern von Daten verwenden, einen Speicherpool erstellen.

  Diese Voraussetzung gilt nicht, wenn Sie StorageGRID 11.7 oder 11.8 ursprünglich installiert haben. Wenn Sie eine dieser Versionen zum ersten Mal installieren, werden für jeden Standort automatisch Speicherpools erstellt.

Schritte

1. Erstellen Sie eine ILM-Regel, die nur für die Daten in `fabricpool-bucket` . Diese Beispielregel erstellt Erasure-Coded-Kopien.

Regeldefinition	Beispielwert
Regelname	2 + 1 Erasure Coding für FabricPool -Daten
Bucket-Name	`fabricpool-bucket` Sie können auch nach dem FabricPool Mandantenkonto filtern.
Erweiterte Filter	Objektgröße größer als 0,2 MB. **Hinweis:** FabricPool schreibt nur 4 MB große Objekte, Sie müssen jedoch einen Objektgrößenfilter hinzufügen, da diese Regel Erasure Coding verwendet.
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte durch Erasure Coding mit dem 2+1 EC-Schema in Denver und behalten Sie diese Objekte für immer in StorageGRID . Um Datenverlust zu vermeiden, verwenden Sie keine ILM-Regel, die FabricPool Cloud-Tier-Daten ablaufen lässt oder löscht.
Aufnahmeverhalten	Ausgewogen

2. Erstellen Sie eine ILM-Standardregel, die zwei replizierte Kopien aller Objekte erstellt, die nicht der ersten Regel entsprechen. Wählen Sie keinen Basisfilter (Mandantenkonto oder Bucket-Name) oder erweiterte Filter aus.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Bucket-Name	*keiner*
Erweiterte Filter	*keiner*
Referenzzeit	Aufnahmezeit
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte, indem Sie 2 Kopien in Denver replizieren.
Aufnahmeverhalten	Ausgewogen

3. Erstellen Sie eine ILM-Richtlinie und wählen Sie die beiden Regeln aus. Da die Replikationsregel keine Filter verwendet, kann sie die Standardregel (letzte Regel) für die Richtlinie sein.
4. Testobjekte in das Raster aufnehmen.
5. Simulieren Sie die Richtlinie mit den Testobjekten, um das Verhalten zu überprüfen.
6. Aktivieren Sie die Richtlinie.

Wenn diese Richtlinie aktiviert ist, platziert StorageGRID Objektdaten wie folgt:

- Die Daten aus FabricPool in `fabricpool-bucket` wird mit dem 2+1-Erasure-Coding-Schema löschcodiert. Zwei Datenfragmente und ein Paritätsfragment werden auf drei verschiedenen Speicherknoten platziert.
- Alle Objekte in allen anderen Buckets werden repliziert. Es werden zwei Kopien erstellt und auf zwei verschiedenen Speicherknoten platziert.

- Die Kopien werden für immer in StorageGRID aufbewahrt. StorageGRID ILM löscht diese Objekte nicht.

Erstellen einer Datenverkehrsklassifizierungsrichtlinie für FabricPool

Sie können optional eine StorageGRID -Verkehrsklassifizierungsrichtlinie entwerfen, um die Servicequalität für die FabricPool -Arbeitslast zu optimieren.

Einzelheiten zu dieser Aufgabe finden Sie unter"Verwalten von Richtlinien zur Datenverkehrsklassifizierung" . Um diese Aufgabe mit dem FabricPool -Setup-Assistenten abzuschließen, gehen Sie zu"Greifen Sie auf den FabricPool -Setup-Assistenten zu und schließen Sie ihn ab" .

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Die Best Practices zum Erstellen einer Datenverkehrsklassifizierungsrichtlinie für FabricPool hängen wie folgt von der Arbeitslast ab:

- Wenn Sie planen, die primären Workload-Daten von FabricPool auf StorageGRID zu verschieben, sollten Sie sicherstellen, dass der FabricPool Workload die meiste Bandbreite zur Verfügung steht. Sie können eine Richtlinie zur Verkehrsklassifizierung erstellen, um alle anderen Arbeitslasten zu begrenzen.

  > Im Allgemeinen ist es wichtiger, FabricPool Lesevorgängen Priorität einzuräumen als Schreibvorgängen.

  Wenn beispielsweise andere S3-Clients dieses StorageGRID -System verwenden, sollten Sie eine Richtlinie zur Verkehrsklassifizierung erstellen. Sie können den Netzwerkverkehr für die anderen Buckets, Mandanten, IP-Subnetze oder Load Balancer-Endpunkte begrenzen.

- Im Allgemeinen sollten Sie keiner FabricPool -Arbeitslast Beschränkungen hinsichtlich der Dienstqualität auferlegen. Sie sollten nur die anderen Arbeitslasten beschränken.
- Die für andere Workloads festgelegten Beschränkungen sollten das Verhalten dieser Workloads berücksichtigen. Die auferlegten Beschränkungen variieren auch je nach Größe und Leistungsfähigkeit Ihres Netzes und der erwarteten Auslastung.

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**.
4. Fügen Sie im Schritt „Übereinstimmungsregeln hinzufügen“ mindestens eine Regel hinzu.
   a. Wählen Sie **Regel hinzufügen**
   b. Wählen Sie unter „Typ“ **Load Balancer-Endpunkt** und dann den Load Balancer-Endpunkt aus, den Sie für FabricPool erstellt haben.

      Sie können auch das FabricPool -Mandantenkonto oder den Bucket auswählen.

   c. Wenn diese Verkehrsrichtlinie den Verkehr für die anderen Endpunkte begrenzen soll, wählen Sie **Inverse Übereinstimmung**.

5. Fügen Sie optional ein oder mehrere Limits hinzu, um den Netzwerkverkehr zu steuern, der der Regel entspricht.

   > StorageGRID sammelt Metriken, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends verstehen können.

   a. Wählen Sie **Limit hinzufügen**.

   b. Wählen Sie die Art des Datenverkehrs aus, den Sie begrenzen möchten, und die anzuwendende Begrenzung.

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**.

Nach Ihrem Ziel

"Anzeigen von Netzwerkverkehrsmetriken"um zu überprüfen, ob die Polizei die von Ihnen erwarteten Verkehrsbeschränkungen durchsetzt.

ONTAP System Manager konfigurieren

Nachdem Sie die erforderlichen StorageGRID Informationen erhalten haben, können Sie zu ONTAP gehen, um StorageGRID als Cloud-Ebene hinzuzufügen.

Bevor Sie beginnen

- Wenn Sie den FabricPool -Setup-Assistenten abgeschlossen haben, verfügen Sie über die `ONTAP_FabricPool_settings_`*`bucketname`*`.txt` Datei, die Sie heruntergeladen haben.
- Wenn Sie StorageGRID manuell konfiguriert haben, verfügen Sie über den vollqualifizierten Domänennamen (FQDN), den Sie für StorageGRID verwenden, oder die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe, die Portnummer für den Load Balancer-Endpunkt, das Load Balancer-Zertifikat, die Zugriffsschlüssel-ID und den geheimen Schlüssel für den Root-Benutzer des Mandantenkontos sowie den Namen des Buckets, den ONTAP in diesem Mandanten verwenden wird.

Zugriff auf den ONTAP System Manager

Diese Anweisungen beschreiben, wie Sie mit ONTAP System Manager StorageGRID als Cloud-Tier hinzufügen. Sie können dieselbe Konfiguration mit der ONTAP CLI durchführen. Anweisungen finden Sie unter "ONTAP -Dokumentation für FabricPool" .

Schritte

1. Greifen Sie auf den System Manager für den ONTAP -Cluster zu, den Sie in StorageGRID einstufen möchten.
2. Sign in .
3. Navigieren Sie zu **SPEICHER** > **Ebenen** > **Cloud-Ebene hinzufügen**.
4. Wählen Sie * StorageGRID* aus der Liste der Objektspeicheranbieter aus.

Geben Sie StorageGRID -Werte ein

Sehen "ONTAP -Dokumentation für FabricPool" für weitere Informationen.

Schritte

1. Füllen Sie das Formular „Cloud-Stufe hinzufügen“ mithilfe der `ONTAP_FabricPool_settings_bucketname.txt` Datei oder die Werte, die Sie manuell erhalten haben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für diese Cloud-Ebene ein. Sie können den Standardwert übernehmen.
URL-Stil	Wenn du"konfigurierte S3-Endpunktdomänennamen" , wählen Sie **Virtual Hosted-Style URL**. **Pfad-URL** ist der Standard für ONTAP, für StorageGRID wird jedoch die Verwendung von Anfragen im virtuellen gehosteten Stil empfohlen. Sie müssen eine **Pfad-URL** verwenden, wenn Sie für das Feld **Servername (FQDN)** eine IP-Adresse anstelle eines Domänennamens angeben.
Servername (FQDN)	Geben Sie den vollqualifizierten Domänennamen (FQDN) ein, den Sie für StorageGRID verwenden, oder die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe. Beispiel: `s3.storagegrid.company.com` . Beachten Sie Folgendes: • Die IP-Adresse oder der Domänenname, den Sie hier angeben, muss mit dem Zertifikat übereinstimmen, das Sie für den StorageGRID Load Balancer-Endpunkt hochgeladen oder generiert haben. • Wenn Sie einen Domänennamen angeben, muss der DNS-Eintrag jeder IP-Adresse zugeordnet sein, die Sie für die Verbindung mit StorageGRID verwenden. Sehen "Konfigurieren des DNS-Servers" .
SSL	Aktiviert (Standard).
Objektspeicherzertifikat	Fügen Sie das PEM-Zertifikat ein, das Sie für den StorageGRID Load Balancer-Endpunkt verwenden, einschließlich: `-----BEGIN CERTIFICATE-----` Und `-----END CERTIFICATE-----` . **Hinweis:** Wenn das StorageGRID -Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt wurde, müssen Sie das Zwischenzertifizierungsstellenzertifikat vorlegen. Wenn das StorageGRID -Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat angeben.
Hafen	Geben Sie den vom StorageGRID Load Balancer-Endpunkt verwendeten Port ein. ONTAP verwendet diesen Port, wenn es eine Verbindung zu StorageGRID herstellt. Zum Beispiel 10433.

Feld	Beschreibung
Zugriffsschlüssel und geheimer Schlüssel	Geben Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer des StorageGRID Mandantenkontos ein. **Tipp**: Wenn Sie in Zukunft einen neuen Zugriffsschlüssel und einen neuen geheimen Zugriffsschlüssel in StorageGRID generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls könnte ONTAP vorübergehend den Zugriff auf StorageGRID verlieren.
Containername	Geben Sie den Namen des StorageGRID Buckets ein, den Sie zur Verwendung mit dieser ONTAP Stufe erstellt haben.

2. Schließen Sie die endgültige FabricPool -Konfiguration in ONTAP ab.
   a. Fügen Sie ein oder mehrere Aggregate an die Cloud-Ebene an.
   b. Erstellen Sie optional eine Volume-Tiering-Richtlinie.

Konfigurieren des DNS-Servers

Nachdem Sie Hochverfügbarkeitsgruppen, Load Balancer-Endpunkte und S3-Endpunktdomänennamen konfiguriert haben, müssen Sie sicherstellen, dass das DNS die erforderlichen Einträge für StorageGRID enthält. Sie müssen für jeden Namen im Sicherheitszertifikat und für jede IP-Adresse, die Sie möglicherweise verwenden, einen DNS-Eintrag einfügen.

Sehen "Überlegungen zum Lastenausgleich" .

DNS-Einträge für den StorageGRID -Servernamen

Fügen Sie DNS-Einträge hinzu, um den StorageGRID -Servernamen (vollqualifizierter Domänenname) jeder StorageGRID -IP-Adresse zuzuordnen, die Sie verwenden werden. Die IP-Adressen, die Sie in das DNS eingeben, hängen davon ab, ob Sie eine HA-Gruppe von Lastausgleichsknoten verwenden:

- Wenn Sie eine HA-Gruppe konfiguriert haben, stellt ONTAP eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, kann ONTAP über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens eine Verbindung zum StorageGRID Load Balancer-Dienst herstellen.
- Wenn der Servername in mehr als eine IP-Adresse aufgelöst wird, stellt ONTAP Clientverbindungen mit allen IP-Adressen her (bis zu maximal 16 IP-Adressen). Die IP-Adressen werden beim Verbindungsaufbau im Round-Robin-Verfahren bezogen.

DNS-Einträge für Anfragen im virtuellen gehosteten Stil

Wenn Sie definiert haben"S3-Endpunktdomänennamen" und Sie verwenden Anfragen im virtuellen gehosteten Stil und fügen DNS-Einträge für alle erforderlichen S3-Endpunktdomänennamen hinzu, einschließlich aller Platzhalternamen.

StorageGRID -Best Practices für FabricPool

Best Practices für Hochverfügbarkeitsgruppen (HA)

Informieren Sie sich vor dem Anhängen von StorageGRID als FabricPool Cloud-Ebene über StorageGRID Hochverfügbarkeitsgruppen (HA) und sehen Sie sich die Best Practices für die Verwendung von HA-Gruppen mit FabricPool an.

Was ist eine HA-Gruppe?

Eine Hochverfügbarkeitsgruppe (HA) ist eine Sammlung von Schnittstellen von mehreren StorageGRID -Gateway-Knoten, Admin-Knoten oder beiden. Eine HA-Gruppe hilft dabei, Client-Datenverbindungen verfügbar zu halten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast mit geringen Auswirkungen auf den FabricPool -Betrieb verwalten.

Jede HA-Gruppe bietet hochverfügbaren Zugriff auf die gemeinsam genutzten Dienste auf den zugehörigen Knoten. Beispielsweise bietet eine HA-Gruppe, die nur aus Schnittstellen auf Gateway-Knoten oder sowohl auf Admin-Knoten als auch auf Gateway-Knoten besteht, hochverfügbaren Zugriff auf den gemeinsam genutzten Load Balancer-Dienst.

Weitere Informationen zu Hochverfügbarkeitsgruppen finden Sie unter"Verwalten von Hochverfügbarkeitsgruppen (HA)" .

Verwenden von HA-Gruppen

Die Best Practices zum Erstellen einer StorageGRID HA-Gruppe für FabricPool hängen von der Arbeitslast ab.

- Wenn Sie FabricPool mit primären Workload-Daten verwenden möchten, müssen Sie eine HA-Gruppe erstellen, die mindestens zwei Lastausgleichsknoten enthält, um Unterbrechungen beim Datenabruf zu vermeiden.
- Wenn Sie die FabricPool -Volume-Tiering-Richtlinie „Nur Snapshots“ oder nicht primäre lokale Leistungsebenen (z. B. Disaster Recovery-Standorte oder NetApp SnapMirror® -Ziele) verwenden möchten, können Sie eine HA-Gruppe mit nur einem Knoten konfigurieren.

Diese Anweisungen beschreiben das Einrichten einer HA-Gruppe für Active-Backup HA (ein Knoten ist aktiv und ein Knoten dient als Backup). Möglicherweise bevorzugen Sie jedoch die Verwendung von DNS Round Robin oder Active-Active HA. Um die Vorteile dieser anderen HA-Konfigurationen kennenzulernen, siehe"Konfigurationsoptionen für HA-Gruppen" .

Bewährte Methoden für den Lastenausgleich für FabricPool

Bevor Sie StorageGRID als FabricPool Cloud-Ebene anhängen, lesen Sie die Best Practices für die Verwendung von Load Balancern mit FabricPool.

Allgemeine Informationen zum StorageGRID Load Balancer und dem Load Balancer-Zertifikat finden Sie unter"Überlegungen zum Lastenausgleich" .

Bewährte Methoden für den Mandantenzugriff auf den für FabricPool verwendeten Load Balancer-Endpunkt

Sie können steuern, welche Mandanten einen bestimmten Load Balancer-Endpunkt verwenden können, um auf ihre Buckets zuzugreifen. Sie können alle Mandanten zulassen, einige Mandanten zulassen oder einige Mandanten blockieren. Wählen Sie beim Erstellen eines Lastenausgleichsendpunkts für die Verwendung von FabricPool **Alle Mandanten zulassen** aus. ONTAP verschlüsselt die in StorageGRID Buckets abgelegten

Daten, sodass diese zusätzliche Sicherheitsebene nur wenig zusätzliche Sicherheit bieten würde.

Best Practices für das Sicherheitszertifikat

Wenn Sie einen StorageGRID Load Balancer-Endpunkt für die Verwendung mit FabricPool erstellen, stellen Sie das Sicherheitszertifikat bereit, das ONTAP die Authentifizierung bei StorageGRID ermöglicht.

In den meisten Fällen sollte die Verbindung zwischen ONTAP und StorageGRID die Transport Layer Security (TLS)-Verschlüsselung verwenden. Die Verwendung von FabricPool ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen. Wenn Sie das Netzwerkprotokoll für den StorageGRID Load Balancer-Endpunkt auswählen, wählen Sie **HTTPS**. Geben Sie dann das Sicherheitszertifikat ein, das ONTAP die Authentifizierung bei StorageGRID ermöglicht.

So erfahren Sie mehr über das Serverzertifikat für einen Lastenausgleichsendpunkt:

- "Sicherheitszertifikate verwalten"
- "Überlegungen zum Lastenausgleich"
- "Härtungsrichtlinien für Serverzertifikate"

Zertifikat zu ONTAP hinzufügen

Wenn Sie StorageGRID als FabricPool Cloud-Tier hinzufügen, müssen Sie dasselbe Zertifikat auf dem ONTAP Cluster installieren, einschließlich des Stammzertifikats und aller untergeordneten Zertifikate der Zertifizierungsstelle (CA).

Ablauf des Zertifikats verwalten

Wenn das zum Sichern der Verbindung zwischen ONTAP und StorageGRID verwendete Zertifikat abläuft, funktioniert FabricPool vorübergehend nicht mehr und ONTAP verliert vorübergehend den Zugriff auf die in StorageGRID abgelegten Daten.

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 StorageGRID und ONTAP -Versionen des Zertifikats 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 ONTAP für die Cloud-Ebene verwendet wird.
- Verwenden Sie ein öffentlich signiertes CA-Zertifikat. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie die Zertifikatsrotation mithilfe der Grid Management API automatisieren. Auf diese Weise können Sie Zertifikate, die bald ablaufen, 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 ONTAP manuell ersetzen, bevor das vorhandene Zertifikat abläuft. Wenn ein selbstsigniertes Zertifikat bereits abgelaufen ist, deaktivieren Sie die Zertifikatsvalidierung in ONTAP , um einen Zugriffsverlust zu verhindern.

  Sehen "NetApp Knowledge Base: So konfigurieren Sie ein neues selbstsigniertes StorageGRID -Serverzertifikat auf einer vorhandenen ONTAP FabricPool Bereitstellung" Anweisungen hierzu finden Sie unter.

Best Practices für die Verwendung von ILM mit FabricPool -Daten

Wenn Sie FabricPool zum Tiering von Daten in StorageGRID verwenden, müssen Sie die Anforderungen für die Verwendung des StorageGRID Information Lifecycle Management (ILM) mit FabricPool -Daten verstehen.

> FabricPool hat keine Kenntnis von den ILM-Regeln oder -Richtlinien von StorageGRID . Bei einer falschen Konfiguration der StorageGRID ILM-Richtlinie kann es zu Datenverlust kommen. Ausführliche Informationen finden Sie unter"Verwenden Sie ILM-Regeln zum Verwalten von Objekten" Und"Erstellen von ILM-Richtlinien" .

Richtlinien zur Verwendung von ILM mit FabricPool

Wenn Sie den FabricPool -Setup-Assistenten verwenden, erstellt der Assistent automatisch eine neue ILM-Regel für jeden von Ihnen erstellten S3-Bucket und fügt diese Regel einer inaktiven Richtlinie hinzu. Sie werden aufgefordert, die Richtlinie zu aktivieren. Die automatisch erstellte Regel folgt den empfohlenen Best Practices: Sie verwendet 2+1 Erasure Coding an einem einzelnen Standort.

Wenn Sie StorageGRID manuell konfigurieren, anstatt den FabricPool -Setup-Assistenten zu verwenden, lesen Sie diese Richtlinien, um sicherzustellen, dass Ihre ILM-Regeln und ILM-Richtlinien für FabricPool -Daten und Ihre Geschäftsanforderungen geeignet sind. Möglicherweise müssen Sie neue Regeln erstellen und Ihre aktiven ILM-Richtlinien aktualisieren, um diese Richtlinien zu erfüllen.

- Sie können zum Schutz von Cloud-Tier-Daten eine beliebige Kombination aus Replikations- und Erasure-Coding-Regeln verwenden.

  Die empfohlene Best Practice besteht darin, innerhalb einer Site 2+1-Löschcodierung zu verwenden, um einen kosteneffizienten Datenschutz zu gewährleisten. Erasure Coding verbraucht mehr CPU, bietet aber deutlich weniger Speicherkapazität als die Replikation. Die 4+1- und 6+1-Schemata nutzen weniger Kapazität als das 2+1-Schema. Die 4+1- und 6+1-Schemata sind jedoch weniger flexibel, wenn Sie während der Netzerweiterung Speicherknoten hinzufügen müssen. Weitere Informationen finden Sie unter "Speicherkapazität für Erasure-Coded-Objekte hinzufügen" .

- Jede auf FabricPool -Daten angewendete Regel muss entweder Erasure Coding verwenden oder mindestens zwei replizierte Kopien erstellen.

  > Eine ILM-Regel, die für einen bestimmten Zeitraum nur eine replizierte Kopie erstellt, birgt das Risiko eines dauerhaften Datenverlusts. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

- Wenn Sie"FabricPool -Daten aus StorageGRID entfernen" , verwenden Sie ONTAP , um alle Daten für das FabricPool -Volume abzurufen und es auf die Leistungsebene zu stufen.

  > Um Datenverlust zu vermeiden, verwenden Sie keine ILM-Regel, die FabricPool Cloud-Tier-Daten ablaufen lässt oder löscht. Legen Sie die Aufbewahrungsdauer in jeder ILM-Regel auf **für immer** fest, um sicherzustellen, dass FabricPool Objekte nicht von StorageGRID ILM gelöscht werden.

- Erstellen Sie keine Regeln, die FabricPool Cloud-Tier-Daten aus dem Bucket an einen anderen Speicherort verschieben. Sie können keinen Cloud-Speicherpool verwenden, um FabricPool Daten in einen anderen Objektspeicher zu verschieben.

Die Verwendung von Cloud Storage Pools mit FabricPool wird aufgrund der zusätzlichen Latenz beim Abrufen eines Objekts vom Cloud Storage Pool-Ziel nicht unterstützt.

- Ab ONTAP 9.8 können Sie optional Objekt-Tags erstellen, um die Klassifizierung und Sortierung gestaffelter Daten für eine einfachere Verwaltung zu erleichtern. Sie können beispielsweise Tags nur auf FabricPool -Volumes festlegen, die an StorageGRID angeschlossen sind. Wenn Sie dann ILM-Regeln in StorageGRID erstellen, können Sie den erweiterten Objekt-Tag-Filter verwenden, um diese Daten auszuwählen und zu platzieren.

Weitere Best Practices für StorageGRID und FabricPool

Wenn Sie ein StorageGRID -System für die Verwendung mit FabricPool konfigurieren, müssen Sie möglicherweise andere StorageGRID -Optionen ändern. Bevor Sie eine globale Einstellung ändern, bedenken Sie, welche Auswirkungen die Änderung auf andere S3-Anwendungen hat.

Prüfnachrichten- und Protokollziele

FabricPool -Workloads weisen häufig eine hohe Rate an Lesevorgängen auf, wodurch eine große Menge an Prüfmeldungen generiert werden kann.

- Wenn Sie keine Aufzeichnung der Client-Lesevorgänge für FabricPool oder eine andere S3-Anwendung benötigen, gehen Sie optional zu **KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**. Ändern Sie die Einstellung **Client Reads** in **Error**, um die Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu verringern. Sehen"Konfigurieren von Überwachungsmeldungen und Protokollzielen" für Details.
- Wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Anwendungen verwenden oder alle Auditdaten behalten möchten, konfigurieren Sie einen externen Syslog-Server und speichern Sie Auditinformationen remote. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Prüfnachrichten auf die Leistung minimiert, ohne die Vollständigkeit der Prüfdaten zu beeinträchtigen. Sehen"Überlegungen zum externen Syslog-Server" für Details.

Objektverschlüsselung

Bei der Konfiguration von StorageGRID können Sie optional die"globale Option zur Verschlüsselung gespeicherter Objekte" wenn für andere StorageGRID Clients eine Datenverschlüsselung erforderlich ist. Die von FabricPool zu StorageGRID verschobenen Daten sind bereits verschlüsselt, daher ist die Aktivierung der StorageGRID Einstellung nicht erforderlich. Clientseitige Verschlüsselungsschlüssel sind Eigentum von ONTAP.

Objektkomprimierung

Aktivieren Sie beim Konfigurieren von StorageGRID nicht die"globale Option zum Komprimieren gespeicherter Objekte" . Die von FabricPool zu StorageGRID verschobenen Daten sind bereits komprimiert. Durch die Verwendung der StorageGRID -Option wird die Größe eines Objekts nicht weiter reduziert.

Eimerkonsistenz

Für FabricPool -Buckets ist die empfohlene Bucket-Konsistenz **Lesen nach neuem Schreiben**, was die Standardkonsistenz für einen neuen Bucket ist. Bearbeiten Sie FabricPool Buckets nicht, um **Available** oder **Strong-site** zu verwenden.

FabricPool -Stufen

Wenn ein StorageGRID Knoten Speicher verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass für das Volume keine FabricPool -Tiering-Richtlinie aktiviert ist. Wenn beispielsweise ein StorageGRID Knoten auf einem VMware-Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datenspeicher für den StorageGRID Knoten unterstützt, keine FabricPool -Tiering -Richtlinie aktiviert ist. Das Deaktivieren der FabricPool Tiering-Funktion für Volumes, die mit StorageGRID -Knoten verwendet werden, vereinfacht die Fehlerbehebung und Speichervorgänge.

> ⚠ Verwenden Sie FabricPool niemals, um Daten im Zusammenhang mit StorageGRID zurück auf StorageGRID selbst zu verschieben. Das Zurückführen von StorageGRID -Daten in StorageGRID erhöht die Fehlerbehebung und die Betriebskomplexität.

Entfernen Sie FabricPool -Daten aus StorageGRID

Wenn Sie die FabricPool -Daten entfernen müssen, die derzeit in StorageGRID gespeichert sind, müssen Sie ONTAP verwenden, um alle Daten für das FabricPool -Volume abzurufen und es auf die Leistungsebene hochzustufen.

Bevor Sie beginnen

- Sie haben die Anweisungen und Hinweise in "Daten auf die Leistungsebene hochstufen" .
- Sie verwenden ONTAP 9.8 oder höher.
- Sie verwenden eine"unterstützter Webbrowser" .
- Sie gehören zu einer StorageGRID Benutzergruppe für das FabricPool Mandantenkonto, das über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Diese Anweisungen erklären, wie Sie Daten von StorageGRID zurück zu FabricPool verschieben. Sie führen dieses Verfahren mit ONTAP und StorageGRID Tenant Manager durch.

Schritte

1. Geben Sie von ONTAP aus die `volume modify` Befehl.

   Satz `tiering-policy` Zu `none` um neue Staffelungen zu stoppen und `cloud-retrieval-policy` Zu `promote` um alle Daten zurückzugeben, die zuvor in StorageGRID abgelegt wurden.

   Sehen "Alle Daten aus einem FabricPool -Volume auf die Leistungsebene hochstufen" .

2. Warten Sie, bis der Vorgang abgeschlossen ist.

   Sie können die `volume object-store` Befehl mit dem `tiering` Option zu "Überprüfen Sie den Status der Leistungsstufen-Aktion" .

3. Wenn der Heraufstufungsvorgang abgeschlossen ist, melden Sie sich beim StorageGRID Tenant Manager für das FabricPool Mandantenkonto an.
4. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
5. Bestätigen Sie, dass der FabricPool Bucket jetzt leer ist.
6. Wenn der Eimer leer ist,"den Bucket löschen" .

Nach Abschluss

Wenn Sie den Bucket löschen, kann das Tiering von FabricPool zu StorageGRID nicht mehr fortgesetzt werden. Da die lokale Ebene jedoch immer noch mit der StorageGRID Cloud-Ebene verbunden ist, gibt ONTAP System Manager Fehlermeldungen zurück, die darauf hinweisen, dass auf den Bucket nicht zugegriffen werden kann.

Um diese Fehlermeldungen zu vermeiden, führen Sie einen der folgenden Schritte aus:

- Verwenden Sie FabricPool Mirror, um dem Aggregat eine andere Cloud-Ebene hinzuzufügen.
- Verschieben Sie die Daten vom FabricPool -Aggregat in ein Nicht- FabricPool -Aggregat und löschen Sie dann das nicht verwendete Aggregat.

Siehe die "ONTAP -Dokumentation für FabricPool" Anweisungen hierzu finden Sie unter.

Verwenden Sie StorageGRID Mandanten und -Clients

Verwenden eines Mandantenkontos

Verwenden eines Mandantenkontos

Mit einem Mandantenkonto können Sie entweder die Simple Storage Service (S3) REST API oder die Swift REST API verwenden, um Objekte in einem StorageGRID -System zu speichern und abzurufen.

Was ist ein Mieterkonto?

Jedes Mandantenkonto verfügt über eigene föderierte oder lokale Gruppen, Benutzer, S3-Buckets oder Swift-Container 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 das StorageGRID -System innerhalb eines Unternehmens verwendet wird, kann der Objektspeicher des Grids nach den verschiedenen Abteilungen der Organisation getrennt sein. Beispielsweise kann es Mandantenkonten für die Marketingabteilung, die Kundensupportabteilung, die Personalabteilung usw. geben.

  > Wenn Sie das S3-Clientprotokoll verwenden, können Sie auch S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen in einem Unternehmen zu trennen. Sie müssen keine separaten Mieterkonten erstellen. Siehe Anweisungen zur Implementierung"S3-Buckets und Bucket-Richtlinien" für weitere Informationen.

- **Anwendungsfall für Dienstanbieter:** Wenn das StorageGRID -System von einem Dienstanbieter verwendet wird, kann der Objektspeicher des Grids nach den verschiedenen Einheiten, die den Speicher mieten, getrennt sein. Beispielsweise kann es Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. geben.

So erstellen Sie ein Mieterkonto

Mandantenkonten werden erstellt von einem"StorageGRID -Grid-Administrator mit dem Grid Manager" . Beim Erstellen eines Mandantenkontos gibt der Grid-Administrator Folgendes 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 Grid-Administratoren die S3 Object Lock-Einstellung 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.

Konfigurieren von S3-Mandanten

Nach einem"S3-Mandantenkonto wird erstellt" können Sie auf den Mandanten-Manager zugreifen, 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

Obwohl Sie S3-Buckets mit dem Tenant Manager erstellen und verwalten können, müssen Sie einen"S3-Client" oder"S3-Konsole" um Objekte aufzunehmen und zu verwalten.

So melden Sie sich an und ab

Sign in

Sie erreichen den Mandantenmanager, indem Sie die URL des Mandanten in die Adressleiste eines"unterstützter Webbrowser" .

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verfügen über eine URL für den Zugriff auf den Mandanten-Manager, die Sie von Ihrem Grid-Administrator erhalten haben. Die URL sieht wie eines dieser Beispiele aus:

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  Die URL enthält immer einen vollqualifizierten Domänennamen (FQDN), die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Knoten. Es kann auch eine Portnummer, die 20-stellige Mandantenkonto-ID oder beides enthalten.

- Wenn die URL nicht die 20-stellige Konto-ID des Mandanten enthält, verfügen Sie über diese Konto-ID.
- Sie verwenden eine"unterstützter Webbrowser" .
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie gehören zu einer Benutzergruppe, die"spezifische Zugriffsberechtigungen" .

Schritte

1. Starten Sie eine"unterstützter Webbrowser" .
2. Geben Sie in der Adressleiste des Browsers die URL für den Zugriff auf den Tenant Manager ein.
3. Wenn eine Sicherheitswarnung angezeigt wird, installieren Sie das Zertifikat mithilfe des Installationsassistenten des Browsers.
4. Sign in .

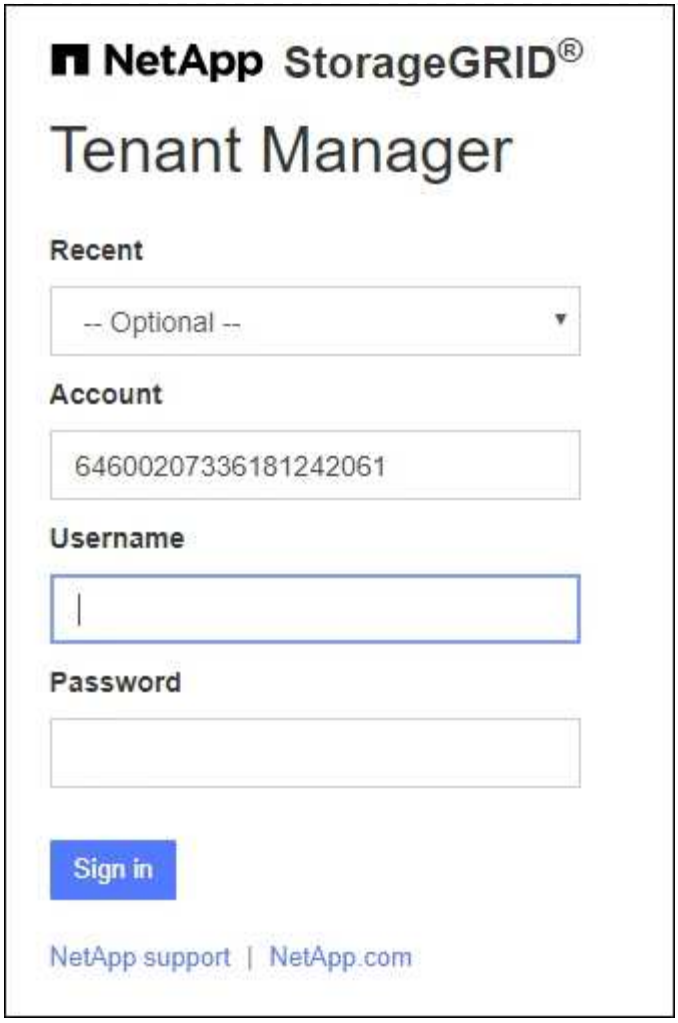
   Der angezeigte Anmeldebildschirm hängt von der eingegebenen URL ab und davon, ob Single Sign-On (SSO) für StorageGRID konfiguriert wurde.

Kein SSO verwenden

Wenn StorageGRID kein SSO verwendet, wird einer der folgenden Bildschirme angezeigt:

- Die Anmeldeseite des Grid Managers. Wählen Sie den Link **Mandantenanmeldung** aus.

- Die Anmeldeseite des Tenant Managers. Das Feld **Konto** ist möglicherweise bereits ausgefüllt, wie unten gezeigt.



i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn dieser in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.

ii. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.

iii. Wählen Sie * Sign in*.

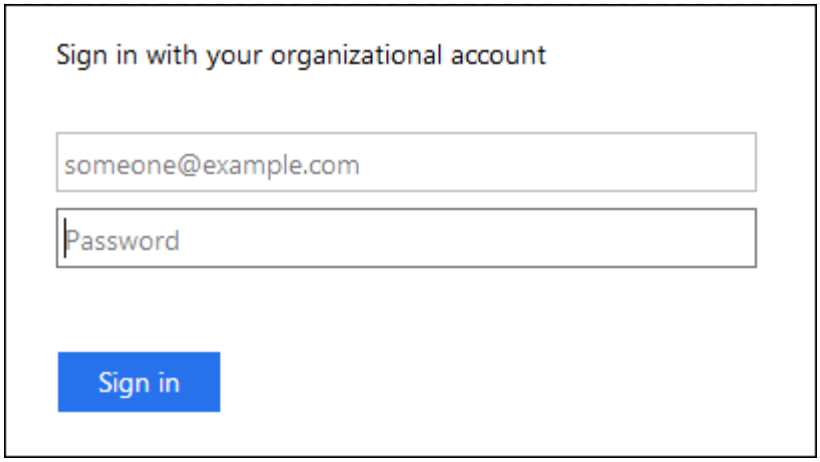
Das Tenant Manager-Dashboard wird angezeigt.

iv. Wenn Sie ein erstes Passwort von jemand anderem erhalten haben, wählen Sie ***Benutzername*** > **Passwort ändern**, um Ihr Konto zu sichern.

Verwenden von SSO

Wenn StorageGRID SSO verwendet, wird einer der folgenden Bildschirme angezeigt:

◦ Die SSO-Seite Ihrer Organisation. Beispiel:



Geben Sie Ihre Standard-SSO-Anmeldeinformationen ein und wählen Sie * Sign in*.

- Die SSO-Anmeldeseite des Tenant Managers.

  i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn dieser in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.

  ii. Wählen Sie * Sign in*.

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

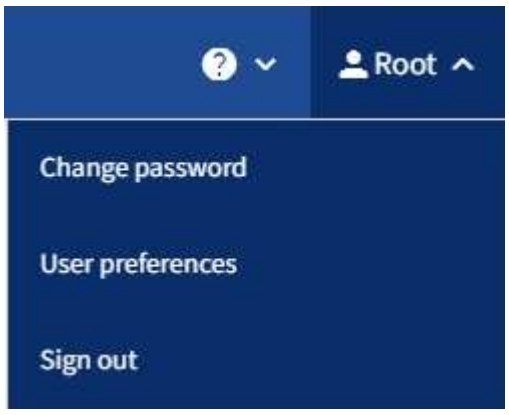
  Das Tenant Manager-Dashboard wird angezeigt.

Vom Tenant Manager abmelden

Wenn Sie mit der Arbeit mit dem Tenant 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. Suchen Sie das Dropdown-Menü für den Benutzernamen in der oberen rechten Ecke der Benutzeroberfläche.



2. Wählen Sie den Benutzernamen und dann **Abmelden**.

   - Wenn SSO nicht verwendet wird:

     Sie sind vom Admin-Knoten abgemeldet. Die Anmeldeseite des Tenant Managers wird angezeigt.

     > Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.

   - Wenn SSO aktiviert ist:

     Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugegriffen haben. Die StorageGRID Sign in wird angezeigt. Der Name des Mandantenkontos, auf das Sie gerade zugegriffen haben, wird standardmäßig im Dropdown-Menü **Letzte Konten** aufgeführt und die **Konto-ID** des Mandanten wird angezeigt.

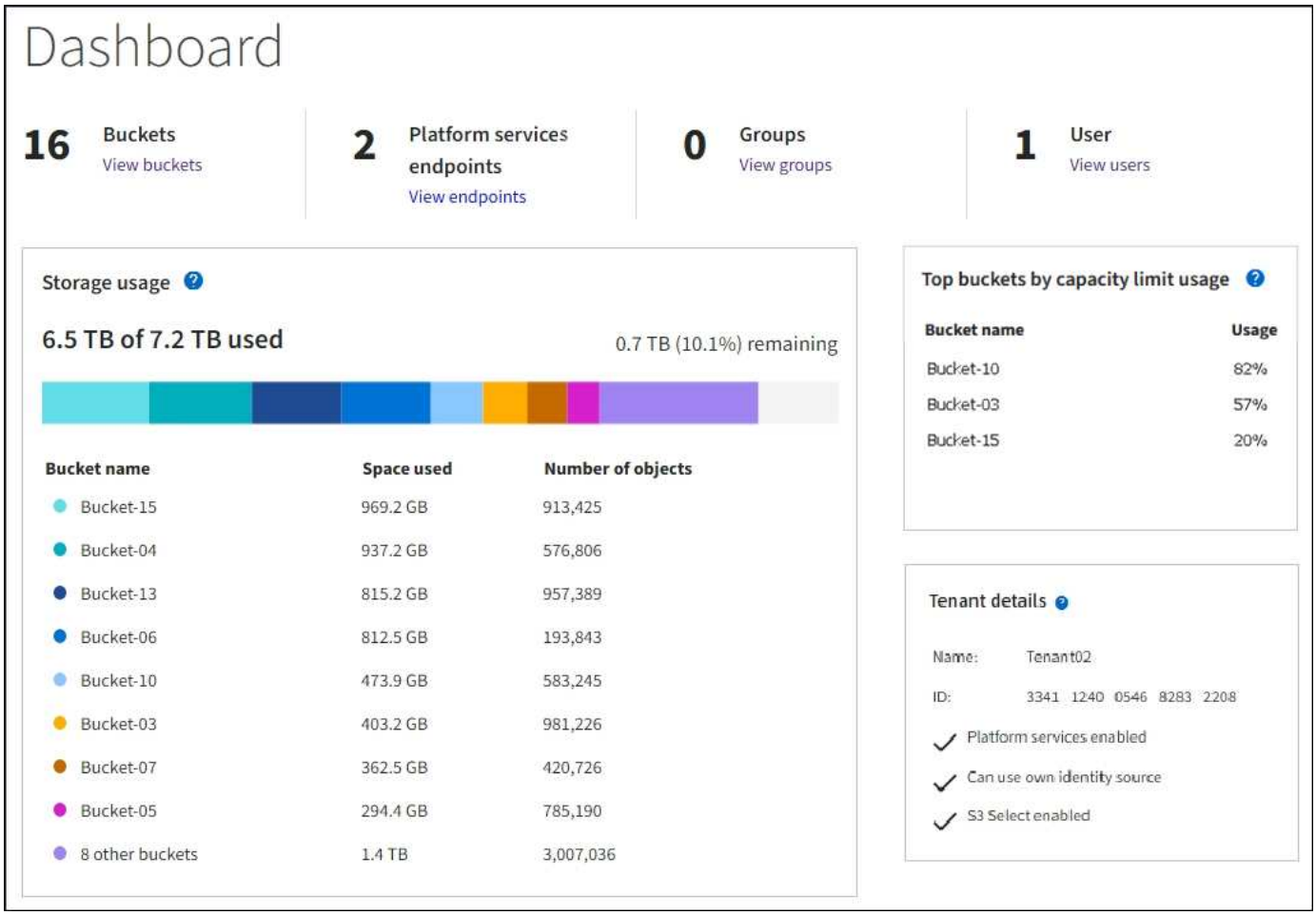
     > Wenn SSO aktiviert ist und Sie auch beim Grid Manager angemeldet sind, müssen Sie sich auch beim Grid Manager abmelden, um sich von SSO abzumelden.

Tenant Manager-Dashboard verstehen

Das Tenant Manager-Dashboard bietet einen Überblick über die Konfiguration eines Tenant-Kontos und den von Objekten in den Buckets (S3) oder Containern (Swift) des Tenant verwendeten Speicherplatz. Wenn der Mandant über ein Kontingent verfügt, zeigt das Dashboard an, wie viel des Kontingents genutzt wird und wie viel noch übrig ist. Wenn Fehler im Zusammenhang mit dem Mieterkonto auftreten, werden diese auf dem Dashboard angezeigt.

> Bei den Werten für den belegten Speicherplatz handelt es sich um Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst.

Wenn Objekte hochgeladen wurden, sieht das Dashboard wie im folgenden Beispiel aus:



Mandantenkontoinformationen

Oben im Dashboard wird die Anzahl der konfigurierten Buckets oder Container, Gruppen und Benutzer angezeigt. Außerdem wird die Anzahl der Plattformdienst-Endpunkte angezeigt, sofern welche konfiguriert wurden. Wählen Sie die Links aus, um die Details anzuzeigen.

Abhängig von der"Berechtigungen zur Mandantenverwaltung" Abhängig von Ihren Einstellungen und den von Ihnen konfigurierten Optionen werden im Rest des Dashboards verschiedene Kombinationen aus Richtlinien, Speichernutzung, Objektinformationen und Mandantendetails angezeigt.

Speicher- und Kontingentnutzung

Das Fenster „Speichernutzung“ enthält die folgenden Informationen:

- Die Menge der Objektdaten für den Mandanten.

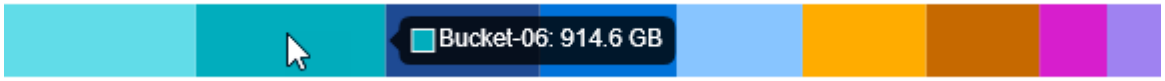
  Dieser Wert gibt die Gesamtmenge der hochgeladenen Objektdaten an und stellt nicht den Speicherplatz dar, der zum Speichern von Kopien dieser Objekte und ihrer Metadaten verwendet wird.

- Wenn ein Kontingent festgelegt ist, die Gesamtmenge des für Objektdaten verfügbaren Speicherplatzes sowie die Menge und der Prozentsatz des verbleibenden Speicherplatzes. Das Kontingent begrenzt die Menge der Objektdaten, die aufgenommen werden können.

Die Kontingentnutzung basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. Beispielsweise überprüft StorageGRID das Kontingent, wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen ab, wenn der Mandant das Kontingent überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kontingent überschritten wurde. Wenn Objekte gelöscht werden, kann es sein, dass ein Mandant vorübergehend daran gehindert wird, neue Objekte hochzuladen, bis die Kontingentnutzung neu berechnet wird. Die Berechnung der Kontingentnutzung kann 10 Minuten oder länger dauern.

- Ein Balkendiagramm, das die relativen Größen der größten Eimer oder Behälter darstellt.

  Sie können den Cursor über ein beliebiges Diagrammsegment bewegen, um den gesamten von diesem Bucket oder Container belegten Speicherplatz anzuzeigen.



- Passend zum Balkendiagramm eine Liste der größten Buckets oder Container, einschließlich der Gesamtmenge der Objektdaten und der Anzahl der Objekte für jeden Bucket oder Container.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

  Wenn der Mandant mehr als neun Buckets oder Container hat, werden alle anderen Buckets oder Container zu einem einzigen Eintrag am Ende der Liste zusammengefasst.

Um die Einheiten für die im Mandanten-Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Mandanten-Manager und dann **Benutzereinstellungen** aus.

Warnmeldungen zur Kontingentnutzung

Wenn im Grid Manager Warnmeldungen zur Kontingentnutzung aktiviert wurden, werden diese

Warnmeldungen im Tenant Manager angezeigt, wenn das Kontingent niedrig ist oder überschritten wird, und zwar wie folgt:

- Wenn 90 % oder mehr des Kontingents eines Mandanten genutzt wurden, wird die Warnung „Hohe Auslastung des Mandantenkontingents“ ausgelöst.

  Bitten Sie Ihren Grid-Administrator, das Kontingent zu erhöhen.

- Wenn Sie Ihr Kontingent überschreiten, werden Sie durch eine Benachrichtigung darüber informiert, dass Sie keine neuen Objekte hochladen können.

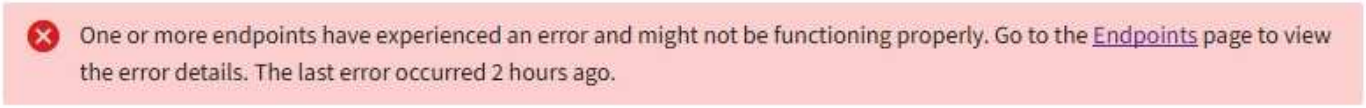
Kapazitätslimitnutzung

Wenn Sie für Ihre Buckets eine Kapazitätsgrenze festgelegt haben, zeigt das Tenant Manager-Dashboard eine Liste der Top-Buckets nach Kapazitätsgrenzenauslastung an.

Wenn für einen Bucket kein Limit festgelegt ist, ist seine Kapazität unbegrenzt. Wenn Ihr Mandantenkonto jedoch über ein Gesamtspeicherkontingent verfügt und dieses Kontingent erreicht ist, können Sie unabhängig von der verbleibenden Kapazitätsgrenze eines Buckets keine weiteren Objekte aufnehmen.

Endpunktfehler

Wenn Sie den Grid Manager verwendet haben, um einen oder mehrere Endpunkte für die Verwendung mit Plattformdiensten zu konfigurieren, zeigt das Tenant Manager-Dashboard eine Warnung an, wenn innerhalb der letzten sieben Tage Endpunktfehler aufgetreten sind.



Um Einzelheiten zu sehen über"Plattformdienst-Endpunktfehler" , wählen Sie **Endpunkte** aus, um die Seite „Endpunkte“ anzuzeigen.

Mandantenverwaltungs-API

Grundlegendes zur API für die Mandantenverwaltung

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

Die Tenant Management API:

- Verwendet die Open-Source-API-Plattform Swagger. Swagger bietet eine intuitive Benutzeroberfläche, die Entwicklern und Nicht-Entwicklern die Interaktion mit der API ermöglicht. Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.
- Anwendung"Versionierung zur Unterstützung unterbrechungsfreier Upgrades" .

So greifen Sie auf die Swagger-Dokumentation für die Tenant Management API zu:

1. Sign in .

2. Wählen Sie oben im Mandanten-Manager das Hilfesymbol und dann **API-Dokumentation** aus.

API-Operationen

Die Tenant Management API organisiert die verfügbaren API-Operationen in den folgenden Abschnitten:

- **Konto**: Vorgänge auf dem aktuellen Mandantenkonto, einschließlich des Abrufens von Informationen zur Speichernutzung.
- **auth**: Vorgänge zum Durchführen der Benutzersitzungsauthentifizierung.

  Die Tenant Management API unterstützt das Bearer Token Authentication Scheme. Für die Anmeldung als Mandant geben Sie im JSON-Text der Authentifizierungsanfrage einen Benutzernamen, ein Kennwort und eine Konto-ID an (d. h. `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“).

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

  > Wenn Single Sign-On (SSO) für das StorageGRID System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte ausführen. Siehe die"Anleitung zur Nutzung der Grid Management API" .

- **config**: Vorgänge im Zusammenhang mit der Produktversion und den Versionen der Tenant Management API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container**: Vorgänge an S3-Buckets oder Swift-Containern.
- **deaktivierte Funktionen**: Vorgänge zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **Endpunkte**: Vorgänge zum Verwalten eines Endpunkts. Endpunkte ermöglichen einem S3-Bucket die Verwendung eines externen Dienstes für die StorageGRID CloudMirror-Replikation, Benachrichtigungen oder Suchintegration.
- **grid-federation-connections**: Operationen an Grid-Föderationsverbindungen und Cross-Grid-Replikation.
- **Gruppen**: Vorgänge zum Verwalten lokaler Mandantengruppen und zum Abrufen föderierter Mandantengruppen aus einer externen Identitätsquelle.
- **Identitätsquelle**: Vorgänge zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm**: Vorgänge an den Einstellungen des Information Lifecycle Management (ILM).
- **Regionen**: Vorgänge zum Bestimmen, welche Regionen für das StorageGRID -System konfiguriert wurden.
- **s3**: Vorgänge zum Verwalten von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-object-lock**: Vorgänge an globalen S3-Objektsperreinstellungen, die zur Unterstützung der Einhaltung gesetzlicher Vorschriften verwendet werden.
- **Benutzer**: Vorgänge zum Anzeigen und Verwalten von Mandantenbenutzern.

Details zum Vorgang

Wenn Sie die einzelnen API-Vorgänge erweitern, können Sie deren HTTP-Aktion, Endpunkt-URL, eine Liste aller erforderlichen oder optionalen Parameter, ein Beispiel für den Anforderungstext (falls erforderlich) und die

möglichen Antworten sehen.

API-Anfragen stellen

> 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 die HTTP-Aktion aus, um die Anforderungsdetails anzuzeigen.
2. 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.
3. Stellen Sie fest, ob Sie den Beispielanforderungstext ändern müssen. Wenn ja, können Sie **Modell** auswählen, um die Anforderungen für jedes Feld zu erfahren.
4. Wählen Sie **Ausprobieren**.
5. Geben Sie alle erforderlichen Parameter an oder ändern Sie den Anforderungstext nach Bedarf.
6. Wählen Sie **Ausführen**.
7. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Versionierung der Mandantenverwaltungs-API

Die Tenant 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.

Um den CSRF-Schutz zu konfigurieren, verwenden Sie die"Grid-Management-API" oder"Mandantenverwaltungs-API" .

> 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.

Grid-Föderation-Verbindungen verwenden

Mandantengruppen und Benutzer klonen

Wenn ein Mandant erstellt oder bearbeitet wurde, um eine Grid-Föderation-Verbindung zu verwenden, wird dieser Mandant von einem StorageGRID -System (dem Quellmandanten) auf ein anderes StorageGRID System (dem Replikatmandanten) repliziert. Nachdem der Mandant repliziert wurde, werden alle dem Quellmandanten

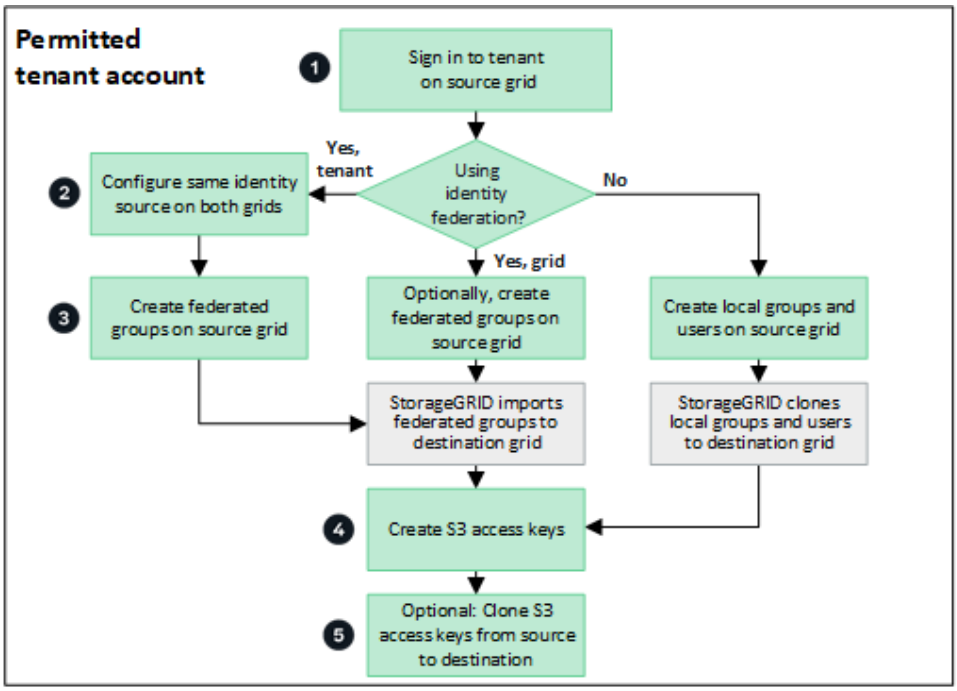
hinzugefügten Gruppen und Benutzer in den Replikatmandanten geklont.

Das StorageGRID -System, in dem der Mandant ursprünglich erstellt wurde, ist das *Quell-Grid* des Mandanten. Das StorageGRID -System, in dem der Mandant repliziert wird, ist das *Ziel-Grid* des Mandanten. Beide Mandantenkonten haben dieselbe Konto-ID, denselben Namen, dieselbe Beschreibung, dasselbe Speicherkontingent und dieselben zugewiesenen Berechtigungen, aber der Zielmandant hat zunächst kein Root-Benutzerkennwort. Weitere Einzelheiten finden Sie unter"Was ist ein Kontoklon?" Und"Zulässige Mandanten verwalten" .

Das Klonen von Mandantenkontoinformationen ist erforderlich für"Cross-Grid-Replikation" von Bucket-Objekten. Wenn Sie auf beiden Grids dieselben Mandantengruppen und Benutzer haben, können Sie auf beiden Grids auf die entsprechenden Buckets und Objekte zugreifen.

Mandanten-Workflow für Kontoklon

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, überprüfen Sie das Workflow-Diagramm, um die Schritte anzuzeigen, die Sie zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln ausführen müssen.



Dies sind die wichtigsten Schritte im Workflow:

1 **Beim Mandanten Sign in**

Sign in (das Raster, in dem der Mandant ursprünglich erstellt wurde).

2 **Optional: Konfigurieren Sie die Identitätsföderation**

Wenn Ihr Mandantenkonto über die Berechtigung **Eigene Identitätsquelle verwenden** zur Verwendung föderierter Gruppen und Benutzer verfügt, konfigurieren Sie dieselbe Identitätsquelle (mit denselben Einstellungen) sowohl für das Quell- als auch das Zielmandantenkonto. Föderierte Gruppen und Benutzer können nicht geklont werden, es sei denn, beide Grids verwenden dieselbe Identitätsquelle. Anweisungen hierzu finden Sie unter"Verwenden der Identitätsföderation" .

3 Erstellen von Gruppen und Benutzern

Beginnen Sie beim Erstellen von Gruppen und Benutzern immer mit dem Quellraster des Mandanten. Wenn Sie eine neue Gruppe hinzufügen, klont StorageGRID sie automatisch in das Zielraster.

- Wenn die Identitätsföderation für das gesamte StorageGRID -System oder für Ihr Mandantenkonto konfiguriert ist,"Erstellen Sie neue Mandantengruppen" durch Importieren föderierter Gruppen aus der Identitätsquelle.
- Wenn Sie keine Identitätsföderation verwenden,"neue lokale Gruppen erstellen" und dann"lokale Benutzer erstellen" .

4 Erstellen von S3-Zugriffsschlüsseln

Du kannst"Erstellen Sie Ihre eigenen Zugriffsschlüssel" oder zu"Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers" entweder auf dem Quell- oder dem Zielraster, um auf Buckets auf diesem Raster zuzugreifen.

5 Optional: S3-Zugriffsschlüssel klonen

Wenn Sie auf Buckets mit denselben Zugriffsschlüsseln auf beiden Grids zugreifen müssen, erstellen Sie die Zugriffsschlüssel auf dem Quellgrid und verwenden Sie dann die Tenant Manager-API, um sie manuell in das Zielgrid zu klonen. Anweisungen hierzu finden Sie unter"Klonen Sie S3-Zugriffsschlüssel mithilfe der API" .

Wie werden Gruppen, Benutzer und S3-Zugriffsschlüssel geklont?

Lesen Sie diesen Abschnitt, um zu verstehen, wie Gruppen, Benutzer und S3-Zugriffsschlüssel zwischen dem Mandantenquellraster und dem Mandantenzielraster geklont werden.

Lokale Gruppen, die im Quellraster erstellt wurden, werden geklont

Nachdem ein Mandantenkonto erstellt und in das Zielraster repliziert wurde, klont StorageGRID automatisch alle lokalen Gruppen, die Sie zum Quellraster des Mandanten hinzufügen, in das Zielraster des Mandanten.

Sowohl die ursprüngliche Gruppe als auch ihr Klon haben denselben Zugriffsmodus, dieselben Gruppenberechtigungen und dieselbe S3-Gruppenrichtlinie. Anweisungen hierzu finden Sie unter"Erstellen Sie Gruppen für den S3-Mandanten" .

> ⓘ Alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quellraster auswählen, werden nicht einbezogen, wenn die Gruppe in das Zielraster geklont wird. Wählen Sie aus diesem Grund beim Erstellen der Gruppe keine Benutzer aus. Wählen Sie stattdessen die Gruppe aus, wenn Sie die Benutzer erstellen.

Lokale Benutzer, die im Quellraster erstellt wurden, werden geklont

Wenn Sie einen neuen lokalen Benutzer im Quell-Grid erstellen, klont StorageGRID diesen Benutzer automatisch in das Ziel-Grid. Sowohl der ursprüngliche Benutzer als auch sein Klon haben denselben vollständigen Namen, Benutzernamen und dieselbe Einstellung für **Zugriff verweigern**. Beide Benutzer gehören außerdem denselben Gruppen an. Anweisungen hierzu finden Sie unter"Lokale Benutzer verwalten" .

Aus Sicherheitsgründen werden lokale Benutzerkennwörter nicht in das Zielraster geklont. Wenn ein lokaler Benutzer auf den Mandantenmanager im Zielraster zugreifen muss, muss der Root-Benutzer für das Mandantenkonto ein Kennwort für diesen Benutzer im Zielraster hinzufügen. Anweisungen hierzu finden Sie unter"Lokale Benutzer verwalten" .

Im Quellraster erstellte föderierte Gruppen werden geklont

Vorausgesetzt, die Voraussetzungen für die Verwendung des Kontoklonens mit"Einmaliges Anmelden" Und"Identitätsföderation" erfüllt sind, werden föderierte Gruppen, die Sie für den Mandanten im Quellraster erstellen (importieren), automatisch auf den Mandanten im Zielraster geklont.

Beide Gruppen haben denselben Zugriffsmodus, dieselben Gruppenberechtigungen und dieselbe S3-Gruppenrichtlinie.

Nachdem Verbundgruppen für den Quellmandanten erstellt und auf den Zielmandanten geklont wurden, können sich Verbundbenutzer in beiden Rastern beim Mandanten anmelden.

S3-Zugriffsschlüssel können manuell geklont werden

StorageGRID klont S3-Zugriffsschlüssel nicht automatisch, da die Sicherheit durch unterschiedliche Schlüssel in jedem Grid verbessert wird.

Um Zugriffsschlüssel in den beiden Rastern zu verwalten, können Sie einen der folgenden Schritte ausführen:

- Wenn Sie nicht für jedes Raster die gleichen Schlüssel verwenden müssen, können Sie"Erstellen Sie Ihre eigenen Zugriffsschlüssel" oder"Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers" auf jedem Raster.
- Wenn Sie die gleichen Schlüssel auf beiden Grids verwenden müssen, können Sie Schlüssel auf dem Quell-Grid erstellen und dann die Tenant Manager API verwenden, um manuell"Klonen Sie die Schlüssel" zum Zielraster.

> Wenn Sie S3-Zugriffsschlüssel für einen Verbundbenutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel in den Zielmandanten geklont.

Zum Zielraster hinzugefügte Gruppen und Benutzer werden nicht geklont

Das Klonen erfolgt nur vom Quellraster des Mandanten zum Zielraster des Mandanten. Wenn Sie Gruppen und Benutzer im Zielraster des Mandanten erstellen oder importieren, klont StorageGRID diese Elemente nicht zurück in das Quellraster des Mandanten.

Bearbeitete oder gelöschte Gruppen, Benutzer und Zugriffsschlüssel werden nicht geklont

Das Klonen erfolgt nur, wenn Sie neue Gruppen und Benutzer erstellen.

Wenn Sie Gruppen, Benutzer oder Zugriffsschlüssel in einem der Raster bearbeiten oder löschen, werden Ihre Änderungen nicht in das andere Raster geklont.

Klonen Sie S3-Zugriffsschlüssel mithilfe der API

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen.

Bevor Sie beginnen

- Das Mandantenkonto verfügt über die Berechtigung **Grid-Föderationsverbindung verwenden**.
- Die Grid-Föderation-Verbindung hat den **Verbindungsstatus Verbunden**.
- Sie sind beim Mandantenmanager im Quellraster des Mandanten angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie Ihre eigenen S3-Anmeldeinformationen oder Root-Zugriffsberechtigungen" .
- Wenn Sie Zugriffsschlüssel für einen lokalen Benutzer klonen, ist der Benutzer bereits in beiden Grids vorhanden.

> ⓘ Wenn Sie S3-Zugriffsschlüssel für einen Verbundbenutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel dem Zielmandanten hinzugefügt.

Klonen Sie Ihre eigenen Zugriffsschlüssel

Sie können Ihre eigenen Zugriffsschlüssel klonen, wenn Sie auf beiden Grids auf dieselben Buckets zugreifen müssen.

Schritte

1. Verwenden Sie den Mandantenmanager im Quellraster."Erstellen Sie Ihre eigenen Zugriffsschlüssel" und laden Sie die `.csv` Datei.
2. Wählen Sie oben im Mandanten-Manager das Hilfesymbol und dann **API-Dokumentation** aus.
3. Wählen Sie im Abschnitt **s3** den folgenden Endpunkt aus:

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. Wählen Sie **Ausprobieren**.
5. Ersetzen Sie im Textfeld **body** die Beispieleinträge für **accessKey** und **secretAccessKey** durch die Werte aus der heruntergeladenen **.csv**-Datei.

   Achten Sie darauf, die doppelten Anführungszeichen um jede Zeichenfolge beizubehalten.

6. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Ablaufzeit als Zeichenfolge im ISO 8601-Daten-/Zeitformat (z. B. `2024-02-28T22:46:33-08:00`). Wenn der Schlüssel nicht abläuft, geben Sie **null** als Wert für den Eintrag **expires** ein (oder entfernen Sie die Zeile **Expires** und das vorangestellte Komma).
7. Wählen Sie **Ausführen**.

8. Bestätigen Sie, dass der Serverantwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

Klonen Sie die Zugriffsschlüssel eines anderen Benutzers

Sie können die Zugriffsschlüssel eines anderen Benutzers klonen, wenn dieser auf beiden Grids auf dieselben Buckets zugreifen muss.

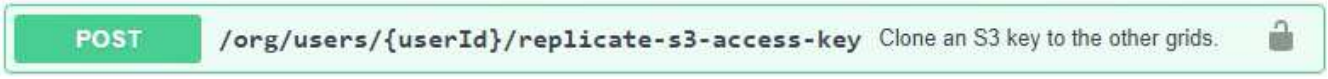
Schritte

1. Verwenden Sie den Mandantenmanager im Quellraster."Erstellen Sie die S3-Zugriffsschlüssel des anderen Benutzers" und laden Sie die `.csv` Datei.
2. Wählen Sie oben im Mandanten-Manager das Hilfesymbol und dann **API-Dokumentation** aus.
3. Besorgen Sie sich die Benutzer-ID. Sie benötigen diesen Wert, um die Zugriffsschlüssel des anderen Benutzers zu klonen.
   a. Wählen Sie im Abschnitt **Benutzer** den folgenden Endpunkt aus:

      ```
      GET /org/users
      ```

   b. Wählen Sie **Ausprobieren**.
   c. Geben Sie alle Parameter an, die Sie beim Suchen von Benutzern verwenden möchten.
   d. Wählen Sie **Ausführen**.
   e. Suchen Sie den Benutzer, dessen Schlüssel Sie klonen möchten, und kopieren Sie die Nummer in das Feld **id**.
4. Wählen Sie im Abschnitt **s3** den folgenden Endpunkt aus:

   ```
   POST /org/users/{userId}/replicate-s3-access-key
   ```

5. Wählen Sie **Ausprobieren**.
6. Fügen Sie in das Textfeld **userId** die kopierte Benutzer-ID ein.
7. Ersetzen Sie im Textfeld **Body** die Beispieleinträge für **Beispielzugriffsschlüssel** und **Geheimer Zugriffsschlüssel** durch die Werte aus der **.csv**-Datei für diesen Benutzer.

   Achten Sie darauf, die doppelten Anführungszeichen um die Zeichenfolge beizubehalten.

8. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Ablaufzeit als Zeichenfolge im ISO 8601-Daten-/Zeitformat (z. B. `2023-02-28T22:46:33-08:00`). Wenn der Schlüssel nicht abläuft, geben Sie **null** als Wert für den Eintrag **expires** ein (oder entfernen Sie die Zeile **Expires** und das vorangestellte Komma).
9. Wählen Sie **Ausführen**.
10. Bestätigen Sie, dass der Serverantwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

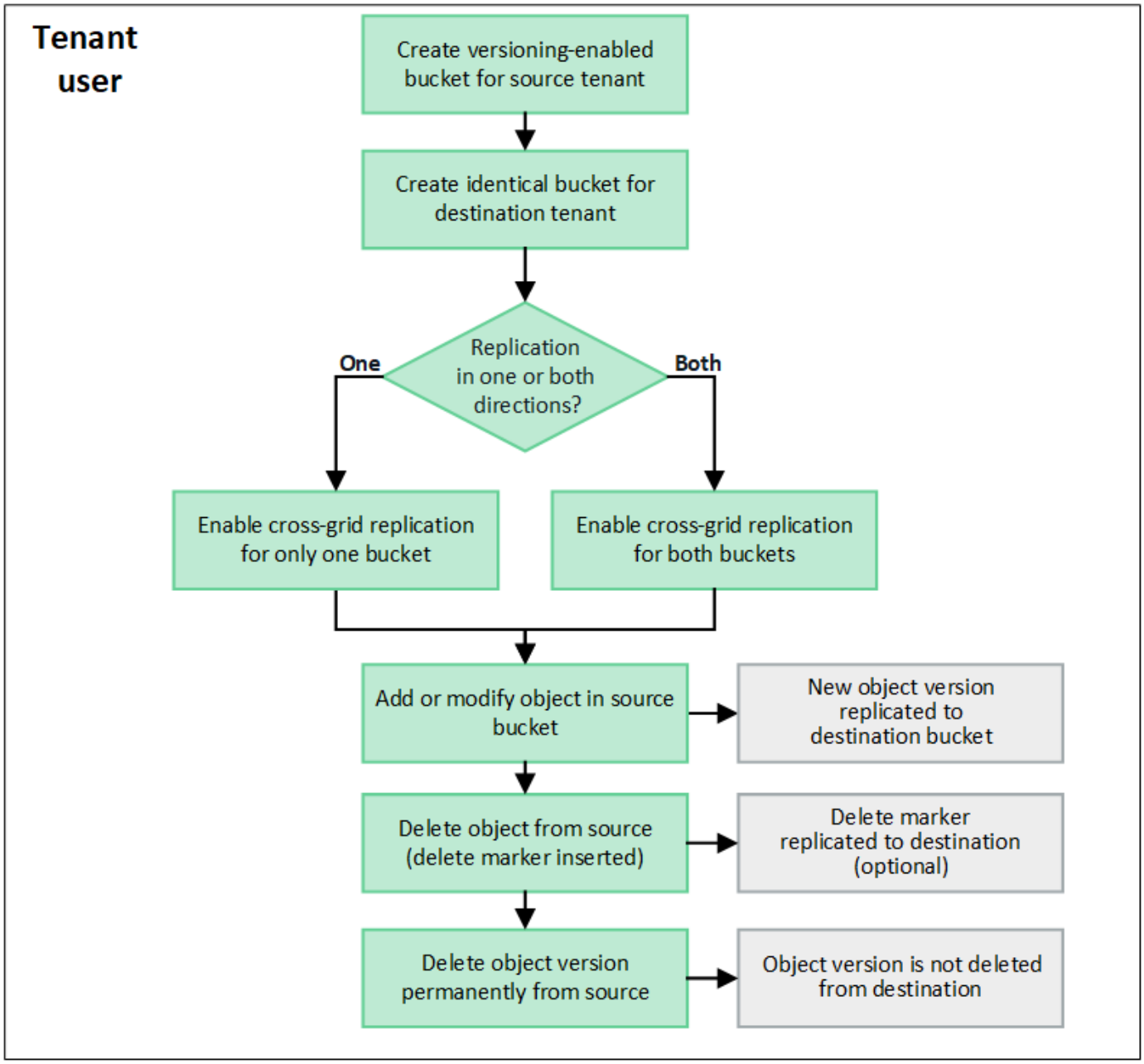
Verwalten der Cross-Grid-Replikation

Wenn Ihrem Mandantenkonto bei der Erstellung die Berechtigung **Grid-Föderationsverbindung verwenden** zugewiesen wurde, können Sie mithilfe der Cross-

Grid-Replikation Objekte automatisch zwischen Buckets im Quell-Grid des Mandanten und Buckets im Ziel-Grid des Mandanten replizieren. Die Cross-Grid-Replikation kann in eine oder beide Richtungen erfolgen.

Workflow für die Cross-Grid-Replikation

Das Workflow-Diagramm fasst die Schritte zusammen, die Sie zum Konfigurieren der Cross-Grid-Replikation zwischen Buckets auf zwei Grids ausführen. Diese Schritte werden im Folgenden genauer beschrieben.



Konfigurieren der Cross-Grid-Replikation

Bevor Sie die Cross-Grid-Replikation verwenden können, müssen Sie sich bei den entsprechenden Mandantenkonten auf jedem Grid anmelden und identische Buckets erstellen. Anschließend können Sie die Cross-Grid-Replikation für einen oder beide Buckets aktivieren.

Bevor Sie beginnen

- Sie haben die Anforderungen für die Cross-Grid-Replikation überprüft. Sehen "Was ist Cross-Grid-Replikation?" .
- Sie verwenden eine"unterstützter Webbrowser" .
- Das Mandantenkonto verfügt über die Berechtigung **Grid-Föderationsverbindung verwenden** und auf beiden Grids sind identische Mandantenkonten vorhanden. Sehen "Verwalten Sie die zulässigen Mandanten für die Grid-Föderation-Verbindung" .
- Der Mandantenbenutzer, als der Sie sich anmelden, ist bereits in beiden Rastern vorhanden und gehört zu einer Benutzergruppe mit der"Root-Zugriffsberechtigung" .
- Wenn Sie sich als lokaler Benutzer beim Zielraster des Mandanten anmelden, hat der Root-Benutzer für das Mandantenkonto ein Kennwort für Ihr Benutzerkonto in diesem Raster festgelegt.

Erstellen Sie zwei identische Eimer

Melden Sie sich als ersten Schritt bei den entsprechenden Mandantenkonten in jedem Raster an und erstellen Sie identische Buckets.

Schritte

1. Erstellen Sie ausgehend von einem der Grids in der Grid-Föderationsverbindung einen neuen Bucket:
   a. Sign in beim Mandantenkonto mit den Anmeldeinformationen eines Mandantenbenutzers an, der in beiden Grids vorhanden ist.

      Wenn Sie sich nicht als lokaler Benutzer beim Zielraster des Mandanten anmelden können, vergewissern Sie sich, dass der Root-Benutzer des Mandantenkontos ein Kennwort für Ihr Benutzerkonto festgelegt hat.

   b. Folgen Sie den Anweisungen, um"Erstellen Sie einen S3-Bucket" .
   c. Wählen Sie auf der Registerkarte **Objekteinstellungen verwalten** die Option **Objektversionierung aktivieren**.
   d. Wenn S3 Object Lock für Ihr StorageGRID System aktiviert ist, aktivieren Sie S3 Object Lock nicht für den Bucket.
   e. Wählen Sie **Bucket erstellen**.
   f. Wählen Sie **Fertig**.
2. Wiederholen Sie diese Schritte, um einen identischen Bucket für dasselbe Mandantenkonto im anderen Grid in der Grid-Föderationsverbindung zu erstellen.

   Je nach Bedarf kann jeder Bucket eine andere Region verwenden.

Aktivieren Sie die Cross-Grid-Replikation

Sie müssen diese Schritte ausführen, bevor Sie einem der Buckets Objekte hinzufügen.

Schritte

1. Ausgehend von einem Raster, dessen Objekte Sie replizieren möchten, aktivieren Sie"Cross-Grid-Replikation in eine Richtung" :
   a. Sign in .
   b. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Bucket-Detailseite zuzugreifen.

d. Wählen Sie die Registerkarte **Cross-Grid-Replikation**.

e. Wählen Sie **Aktivieren** und überprüfen Sie die Liste der Anforderungen.

f. Wenn alle Voraussetzungen erfüllt sind, wählen Sie die Grid-Föderation-Verbindung aus, die Sie verwenden möchten.

g. Ändern Sie optional die Einstellung von **Löschmarkierungen replizieren**, um festzulegen, was im Zielraster geschieht, wenn ein S3-Client eine Löschanforderung an das Quellraster sendet, die keine Versions-ID enthält:

   - **Ja** (Standard): Dem Quell-Bucket wird eine Löschmarkierung hinzugefügt und in den Ziel-Bucket repliziert.
   - **Nein**: Dem Quell-Bucket wird eine Löschmarkierung hinzugefügt, die jedoch nicht in den Ziel-Bucket repliziert wird.

> Wenn die Löschanforderung eine Versions-ID enthält, wird diese Objektversion dauerhaft aus dem Quell-Bucket entfernt. StorageGRID repliziert keine Löschanforderungen, die eine Versions-ID enthalten, sodass dieselbe Objektversion nicht vom Ziel gelöscht wird.

Sehen"Was ist Cross-Grid-Replikation?" für Details.

a. Ändern Sie optional die Einstellung der Auditkategorie **Gridübergreifende Replikation**, um das Volumen der Auditmeldungen zu verwalten:

   - **Fehler** (Standard): Nur fehlgeschlagene Cross-Grid-Replikationsanforderungen werden in die Prüfausgabe aufgenommen.
   - **Normal**: Alle Cross-Grid-Replikationsanforderungen werden einbezogen, wodurch das Volumen der Audit-Ausgabe erheblich erhöht wird.

b. Überprüfen Sie Ihre Auswahl. Sie können diese Einstellungen nur ändern, wenn beide Buckets leer sind.

c. Wählen Sie **Aktivieren und testen**.

   Nach einigen Augenblicken erscheint eine Erfolgsmeldung. Zu diesem Bucket hinzugefügte Objekte werden jetzt automatisch in das andere Raster repliziert. **Cross-Grid-Replikation** wird auf der Bucket-Detailseite als aktivierte Funktion angezeigt.

2. Optional können Sie zum entsprechenden Eimer auf dem anderen Raster gehen und"ermöglichen Cross-Grid-Replikation in beide Richtungen" .

Testen Sie die Replikation zwischen Grids

Wenn die Cross-Grid-Replikation für einen Bucket aktiviert ist, müssen Sie möglicherweise überprüfen, ob die Verbindung und die Cross-Grid-Replikation ordnungsgemäß funktionieren und ob die Quell- und Ziel-Buckets noch alle Anforderungen erfüllen (z. B. ist die Versionierung noch aktiviert).

Bevor Sie beginnen

- Sie verwenden eine"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .

Schritte

1. Sign in .
2. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
3. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Bucket-Detailseite zuzugreifen.
4. Wählen Sie die Registerkarte **Cross-Grid-Replikation**.
5. Wählen Sie **Verbindung testen**.

   Wenn die Verbindung in Ordnung ist, wird ein Erfolgsbanner angezeigt. Andernfalls wird eine Fehlermeldung angezeigt, die Sie und der Grid-Administrator zur Lösung des Problems verwenden können. Weitere Informationen finden Sie unter "Beheben von Grid-Föderationsfehlern" .

6. Wenn die Cross-Grid-Replikation so konfiguriert ist, dass sie in beide Richtungen erfolgt, gehen Sie zum entsprechenden Bucket im anderen Grid und wählen Sie **Verbindung testen** aus, um zu überprüfen, ob die Cross-Grid-Replikation in die andere Richtung funktioniert.

Deaktivieren der Cross-Grid-Replikation

Sie können die Cross-Grid-Replikation dauerhaft stoppen, wenn Sie keine Objekte mehr in das andere Grid kopieren möchten.

Beachten Sie Folgendes, bevor Sie die Cross-Grid-Replikation deaktivieren:

- Durch das Deaktivieren der Cross-Grid-Replikation werden keine Objekte entfernt, die bereits zwischen Grids kopiert wurden. Beispielsweise können Objekte in `my-bucket` auf Grid 1, die kopiert wurden nach `my-bucket` auf Grid 2 werden nicht entfernt, wenn Sie die Cross-Grid-Replikation für diesen Bucket deaktivieren. Wenn Sie diese Objekte löschen möchten, müssen Sie sie manuell entfernen.
- Wenn die Cross-Grid-Replikation für jeden Bucket aktiviert wurde (d. h., wenn die Replikation in beide Richtungen erfolgt), können Sie die Cross-Grid-Replikation für einen oder beide Buckets deaktivieren. Beispielsweise möchten Sie möglicherweise die Replikation von Objekten deaktivieren von `my-bucket` auf Raster 1 bis `my-bucket` auf Grid 2, während weiterhin Objekte aus `my-bucket` auf Grid 2 zu `my-bucket` auf Raster 1.
- Sie müssen die Cross-Grid-Replikation deaktivieren, bevor Sie einem Mandanten die Berechtigung zur Verwendung der Grid-Föderationsverbindung entziehen können. Sehen "Zulässige Mandanten verwalten" .
- Wenn Sie die Cross-Grid-Replikation für einen Bucket deaktivieren, der Objekte enthält, können Sie die Cross-Grid-Replikation nicht wieder aktivieren, es sei denn, Sie löschen alle Objekte sowohl aus dem Quell- als auch aus dem Ziel-Bucket.

  Sie können die Replikation erst wieder aktivieren, wenn beide Buckets leer sind.

Bevor Sie beginnen

- Sie verwenden eine"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .

Schritte

1. Beginnen Sie mit dem Grid, dessen Objekte Sie nicht mehr replizieren möchten, und beenden Sie die Grid-übergreifende Replikation für den Bucket:
   a. Sign in .
   b. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
   c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Bucket-Detailseite zuzugreifen.

d. Wählen Sie die Registerkarte **Cross-Grid-Replikation**.

e. Wählen Sie **Replikation deaktivieren**.

f. Wenn Sie sicher sind, dass Sie die Cross-Grid-Replikation für diesen Bucket deaktivieren möchten, geben Sie **Ja** in das Textfeld ein und wählen Sie **Deaktivieren** aus.

   Nach einigen Augenblicken erscheint eine Erfolgsmeldung. Neue Objekte, die diesem Bucket hinzugefügt werden, können nicht mehr automatisch in das andere Raster repliziert werden. **Cross-Grid-Replikation** wird auf der Buckets-Seite nicht mehr als aktivierte Funktion angezeigt.

2. Wenn die Cross-Grid-Replikation so konfiguriert wurde, dass sie in beide Richtungen erfolgt, gehen Sie zum entsprechenden Bucket auf dem anderen Grid und stoppen Sie die Cross-Grid-Replikation in die andere Richtung.

Grid-Föderation-Verbindungen anzeigen

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie die zulässigen Verbindungen anzeigen.

Bevor Sie beginnen

- Das Mandantenkonto verfügt über die Berechtigung **Grid-Föderationsverbindung verwenden**.
- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .

Schritte

1. Wählen Sie **STORAGE (S3)** > **Grid-Föderationsverbindungen**.

   Die Seite „Grid-Föderationsverbindung“ wird angezeigt und enthält eine Tabelle mit einer Zusammenfassung der folgenden Informationen:

Spalte	Beschreibung
Verbindungsname	Die Grid-Föderation-Verbindungen, für deren Verwendung dieser Mandant berechtigt ist.
Buckets mit Cross-Grid-Replikation	Für jede Grid-Föderationsverbindung die Mandanten-Buckets, für die die Cross-Grid-Replikation aktiviert ist. Zu diesen Buckets hinzugefügte Objekte werden in das andere Raster in der Verbindung repliziert.
Letzter Fehler	Für jede Grid-Föderationsverbindung der letzte Fehler, der ggf. beim Replizieren der Daten in das andere Grid aufgetreten ist. Sehen Löschen Sie den letzten Fehler .

2. Wählen Sie optional einen Bucket-Namen aus, um"Bucket-Details anzeigen" .

Lösche den letzten Fehler

In der Spalte **Letzter Fehler** kann aus einem der folgenden Gründe ein Fehler angezeigt werden:

- 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.

> In dieser Spalte wird nur der letzte aufgetretene Cross-Grid-Replikationsfehler angezeigt. Eventuell zuvor aufgetretene Fehler werden nicht angezeigt.

Schritte

1. Wenn in der Spalte **Letzter Fehler** eine Meldung angezeigt wird, sehen Sie sich den Nachrichtentext an.

   Dieser Fehler weist beispielsweise darauf hin, dass sich der Ziel-Bucket für die Cross-Grid-Replikation in einem ungültigen Zustand befand, möglicherweise weil die Versionierung ausgesetzt oder die S3-Objektsperre aktiviert war.

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 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.

7. Um festzustellen, ob Objekte aufgrund des Bucket-Fehlers nicht repliziert werden konnten, siehe"Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge" .

Verwalten von Gruppen und Benutzern

Verwenden der Identitätsföderation

Durch die Verwendung der Identitätsföderation lässt sich das Einrichten von

Mandantengruppen und Benutzern beschleunigen und Mandantenbenutzer können sich mit vertrauten Anmeldeinformationen beim Mandantenkonto anmelden.

Konfigurieren der Identitätsföderation für den Mandantenmanager

Sie können die Identitätsföderation für den Mandantenmanager konfigurieren, wenn Sie Mandantengruppen und Benutzer in einem anderen System wie Active Directory, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server verwalten möchten.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- 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 des OpenLDAP-Servers .
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, muss der Identitätsanbieter TLS 1.2 oder 1.3 verwenden. Sehen "Unterstützte Verschlüsselungen für ausgehende TLS-Verbindungen" .

Informationen zu diesem Vorgang

Ob Sie einen Identitätsföderationsdienst für Ihren Mandanten konfigurieren können, hängt davon ab, wie Ihr Mandantenkonto eingerichtet wurde. Ihr Mandant nutzt möglicherweise den für den Grid Manager konfigurierten Identitätsföderationsdienst gemeinsam. Wenn diese Meldung beim Zugriff auf die Seite „Identitätsföderation“ angezeigt wird, können Sie für diesen Mandanten keine separate föderierte Identitätsquelle konfigurieren.

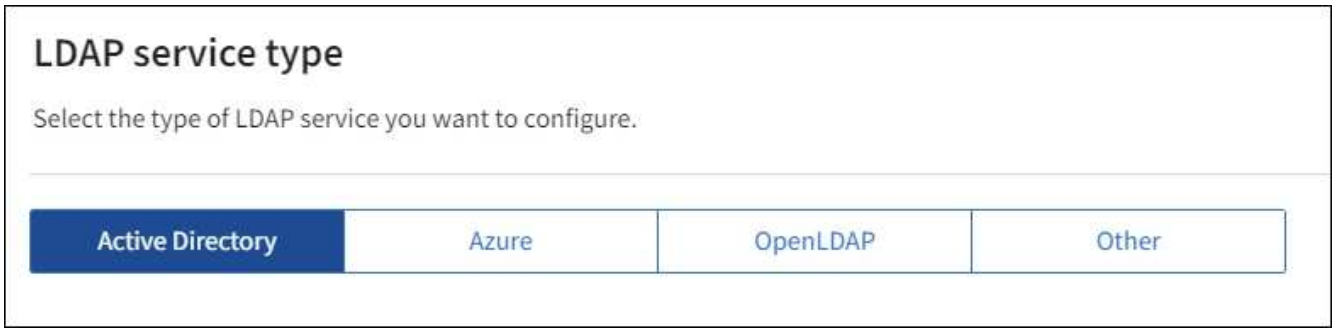
> This tenant account uses the LDAP server that is configured for the Grid Manager.
> Contact the grid administrator for information or to change this setting.

Konfiguration eingeben

Wenn Sie die Identifizierungsföderation konfigurieren, geben Sie die Werte an, die StorageGRID für die Verbindung mit einem LDAP-Dienst benötigt.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **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.

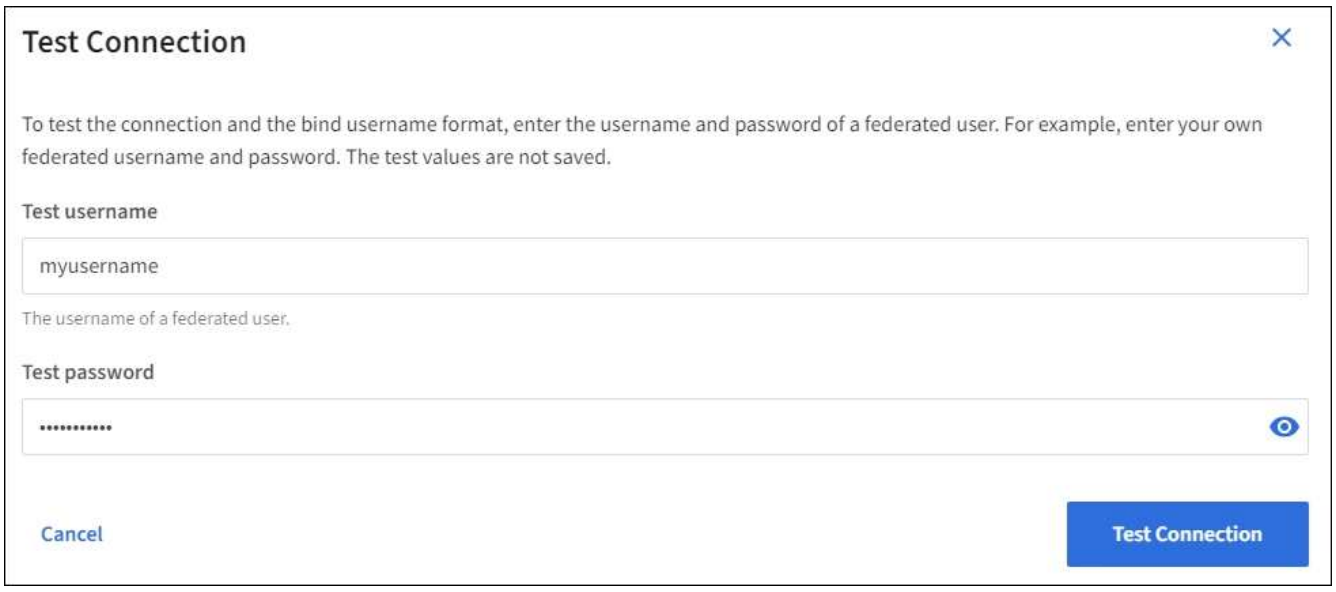
Testen Sie die Verbindung und speichern Sie die Konfiguration

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.

Synchronisierung mit Identitätsquelle erzwingen

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 des 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 Mandantengruppen

Erstellen von Gruppen für einen S3-Mandanten

Sie können Berechtigungen für S3-Benutzergruppen verwalten, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie"konfigurierte Identitätsföderation" , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, haben Sie den Workflow und die Überlegungen für"Klonen von Mandantengruppen und Benutzern" , und Sie sind beim Quellraster des Mandanten angemeldet.

Greifen Sie auf den Assistenten „Gruppe erstellen“ zu

Rufen Sie als ersten Schritt den Assistenten „Gruppe erstellen“ auf.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, bestätigen Sie, dass ein blaues Banner angezeigt wird, das darauf hinweist, dass neue Gruppen, die in diesem Grid erstellt werden, in denselben Mandanten im anderen Grid in der Verbindung geklont werden. Wenn dieses Banner nicht angezeigt wird, sind Sie möglicherweise beim Zielraster des Mandanten angemeldet.

3. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp

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

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe**, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Verbundgruppe**, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

   Wenn Single Sign-On (SSO) für Ihr StorageGRID -System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Tenant Manager anmelden, obwohl sie Clientanwendungen verwenden können, um die Ressourcen des Mandanten basierend auf Gruppenberechtigungen zu verwalten.

2. Geben Sie den Namen der Gruppe ein.
   - **Lokale Gruppe**: Geben Sie sowohl einen Anzeigenamen als auch einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.

     Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, tritt ein Klonfehler auf, wenn derselbe **eindeutige Name** für den Mandanten im Zielgrid bereits vorhanden ist.

   - **Föderierte Gruppe**: Geben Sie den eindeutigen Namen ein. Für Active Directory ist der eindeutige Name der Name, der mit dem `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der mit dem `uid` Attribut.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer im Tenant Manager und in der Tenant Management API ausführen können.

Schritte

1. Wählen Sie für **Zugriffsmodus** eine der folgenden Optionen aus:
   - **Lesen/Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Tenant-Konfiguration verwalten.
   - **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können im Tenant Manager oder in der Tenant Management API keine Änderungen vornehmen oder Vorgänge ausführen. Lokale Benutzer mit Leseberechtigung können ihre eigenen Passwörter ändern.

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

2. Wählen Sie eine oder mehrere Berechtigungen für diese Gruppe aus.

   Sehen "Berechtigungen zur Mandantenverwaltung" .

3. Wählen Sie **Weiter**.

S3-Gruppenrichtlinie festlegen

Die Gruppenrichtlinie bestimmt, welche S3-Zugriffsberechtigungen Benutzer haben.

Schritte

1. Wählen Sie die Richtlinie aus, die Sie für diese Gruppe verwenden möchten.

Gruppenrichtlinie	Beschreibung
Kein S3-Zugriff	Standard. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat standardmäßig nur der Root-Benutzer Zugriff auf S3-Ressourcen.
Nur-Lese-Zugriff	Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Beispielsweise können Benutzer dieser Gruppe Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine schreibgeschützte Gruppenrichtlinie im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.
Vollzugriff	Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine Gruppenrichtlinie mit vollem Zugriff im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.

Gruppenrichtlinie	Beschreibung
Ransomware-Minderung	Diese Beispielrichtlinie gilt für alle Buckets dieses Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber keine Objekte dauerhaft aus Buckets löschen, für die die Objektversionierung aktiviert ist. Tenant Manager-Benutzer mit der Berechtigung **Alle Buckets verwalten** können diese Gruppenrichtlinie außer Kraft setzen. Beschränken Sie die Berechtigung „Alle Buckets verwalten“ auf vertrauenswürdige Benutzer und verwenden Sie, sofern verfügbar, die Multi-Faktor-Authentifizierung (MFA).
Brauch	Den Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.

2. Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie die Gruppenrichtlinie ein. Jede Gruppenrichtlinie hat eine Größenbeschränkung von 5.120 Byte. Sie müssen eine gültige Zeichenfolge im JSON-Format eingeben.

   Ausführliche Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispielen, finden Sie unter"Beispiele für Gruppenrichtlinien" .

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)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional bereits vorhandene lokale Benutzer hinzufügen.

> ⓘ Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, werden alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quell-Grid auswählen, nicht einbezogen, wenn die Gruppe in das Ziel-Grid geklont wird. Wählen Sie aus diesem Grund beim Erstellen der Gruppe keine Benutzer aus. Wählen Sie stattdessen die Gruppe aus, wenn Sie die Benutzer erstellen.

Schritte

1. Wählen Sie optional einen oder mehrere lokale Benutzer für diese Gruppe aus.
2. Wählen Sie **Gruppe erstellen** und **Fertig**.

   Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

   Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie sich im Quell-Grid des Mandanten befinden, wird die neue Gruppe in das Ziel-Grid des Mandanten geklont. **Erfolg** wird als **Klonstatus** im Abschnitt „Übersicht“ der Detailseite der Gruppe angezeigt.

Erstellen Sie Gruppen für einen Swift-Mandanten

Sie können Zugriffsberechtigungen für ein Swift-Mandantenkonto verwalten, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen. Mindestens eine Gruppe

muss über die Berechtigung „Swift-Administrator“ verfügen, die zum Verwalten der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.

> Die Unterstützung für Swift-Clientanwendungen ist veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie"konfigurierte Identitätsföderation" , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Greifen Sie auf den Assistenten „Gruppe erstellen“ zu

Schritte

Rufen Sie als ersten Schritt den Assistenten „Gruppe erstellen“ auf.

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp

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

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe**, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Verbundgruppe**, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

   Wenn Single Sign-On (SSO) für Ihr StorageGRID -System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Tenant Manager anmelden, obwohl sie Clientanwendungen verwenden können, um die Ressourcen des Mandanten basierend auf Gruppenberechtigungen zu verwalten.

2. Geben Sie den Namen der Gruppe ein.
   - **Lokale Gruppe**: Geben Sie sowohl einen Anzeigenamen als auch einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
   - **Föderierte Gruppe**: Geben Sie den eindeutigen Namen ein. Für Active Directory ist der eindeutige Name der Name, der mit dem `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der mit dem `uid` Attribut.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer im Tenant Manager und in der Tenant Management API ausführen können.

Schritte

1. Wählen Sie für **Zugriffsmodus** eine der folgenden Optionen aus:

- **Lesen/Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Tenant-Konfiguration verwalten.
- **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können im Tenant Manager oder in der Tenant Management API keine Änderungen vornehmen oder Vorgänge ausführen. Lokale Benutzer mit Leseberechtigung können ihre eigenen Passwörter ändern.

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

2. Aktivieren Sie das Kontrollkästchen **Root-Zugriff**, wenn sich Gruppenbenutzer beim Tenant Manager oder der Tenant Management API anmelden müssen.
3. Wählen Sie **Weiter**.

Swift-Gruppenrichtlinie festlegen

Swift-Benutzer benötigen Administratorberechtigungen, um sich bei der Swift REST-API zu authentifizieren, Container zu erstellen und Objekte aufzunehmen.

1. Aktivieren Sie das Kontrollkästchen **Swift-Administrator**, wenn Gruppenbenutzer die Swift REST-API zum Verwalten von Containern und Objekten verwenden müssen.
2. 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)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional bereits vorhandene lokale Benutzer hinzufügen.

Schritte

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

   Wenn Sie noch keine lokalen Benutzer erstellt haben, können Sie diese Gruppe auf der Seite „Benutzer“ zum Benutzer hinzufügen. Sehen "Lokale Benutzer verwalten" .

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

   Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Berechtigungen zur Mandantenverwaltung

Überlegen Sie vor dem Erstellen einer Mandantengruppe, welche Berechtigungen Sie dieser Gruppe zuweisen möchten. Die Berechtigungen zur Mandantenverwaltung legen fest, welche Aufgaben Benutzer mit dem Mandantenmanager oder der Mandantenverwaltungs-API ausführen können. Ein Benutzer kann einer oder mehreren Gruppen angehören. Berechtigungen sind kumulativ, wenn ein Benutzer mehreren Gruppen angehört.

Um sich beim Tenant Manager anzumelden oder die Tenant Management API zu verwenden, müssen Benutzer einer Gruppe angehören, die über mindestens eine Berechtigung verfügt. Alle Benutzer, die sich anmelden können, können die folgenden Aufgaben ausführen:

- Dashboard anzeigen
- Das eigene Passwort ändern (für lokale Benutzer)

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 für eine der Gruppen der Lesezugriff aktiviert ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

Sie können einer Gruppe die folgenden Berechtigungen zuweisen. Beachten Sie, dass S3-Mandanten und Swift-Mandanten unterschiedliche Gruppenberechtigungen haben.

Erlaubnis	Beschreibung	Details
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Tenant Management API.	Swift-Benutzer müssen über Root-Zugriffsberechtigungen verfügen, um sich beim Mandantenkonto anmelden zu können.
Administrator	Nur Swift-Mieter. Bietet vollständigen Zugriff auf die Swift-Container und -Objekte für dieses Mandantenkonto	Swift-Benutzer müssen über die Berechtigung „Swift-Administrator“ verfügen, um Vorgänge mit der Swift-REST-API ausführen zu können.
Verwalten Sie Ihre eigenen S3-Anmeldeinformationen	Ermöglicht Benutzern das Erstellen und Entfernen eigener S3-Zugriffsschlüssel.	Benutzer ohne diese Berechtigung sehen die Menüoption **STORAGE (S3)** > **Meine S3-Zugriffsschlüssel** nicht.
Alle Eimer anzeigen	**S3-Mandanten**: Ermöglicht Benutzern, alle Buckets und Bucket-Konfigurationen anzuzeigen. **Swift-Mandanten**: Ermöglicht Swift-Benutzern, alle Container und Containerkonfigurationen mithilfe der Tenant Management API anzuzeigen.	Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption **Buckets** nicht sehen. Diese Berechtigung wird durch die Berechtigung „Alle Buckets verwalten“ ersetzt. Es hat keine Auswirkungen auf S3-Bucket- oder Gruppenrichtlinien, die von S3-Clients oder der S3-Konsole verwendet werden. Sie können diese Berechtigung nur Swift-Gruppen über die Tenant Management API zuweisen. Sie können diese Berechtigung nicht mithilfe des Mandanten-Managers Swift-Gruppen zuweisen.

Erlaubnis	Beschreibung	Details
Alle Buckets verwalten	**S3-Mandanten**: Ermöglicht Benutzern die Verwendung des Mandantenmanagers und der Mandantenverwaltungs-API zum Erstellen und Löschen von S3-Buckets und zum Verwalten der Einstellungen für alle S3-Buckets im Mandantenkonto, unabhängig von S3-Bucket- oder Gruppenrichtlinien. **Swift-Mandanten**: Ermöglicht Swift-Benutzern, die Konsistenz für Swift-Container mithilfe der Tenant Management API zu steuern.	Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption **Buckets** nicht sehen. Diese Berechtigung ersetzt die Berechtigung „Alle Buckets anzeigen“. Es hat keine Auswirkungen auf S3-Bucket- oder Gruppenrichtlinien, die von S3-Clients oder der S3-Konsole verwendet werden. Sie können diese Berechtigung nur Swift-Gruppen über die Tenant Management API zuweisen. Sie können diese Berechtigung nicht mithilfe des Mandanten-Managers Swift-Gruppen zuweisen.
Verwalten von Endpunkten	Ermöglicht Benutzern die Verwendung des Tenant Managers oder der Tenant Management API zum Erstellen oder Bearbeiten von Plattformdienst-Endpunkten, die als Ziel für StorageGRID -Plattformdienste verwendet werden.	Benutzern ohne diese Berechtigung wird die Menüoption **Plattformdienst-Endpunkte** nicht angezeigt.
Registerkarte „S3-Konsole verwenden“	In Kombination mit der Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ können Benutzer Objekte über die Registerkarte „S3-Konsole“ auf der Detailseite für einen Bucket anzeigen und verwalten.	

Verwalten von Gruppen

Verwalten Sie Ihre Mandantengruppen nach Bedarf, um eine Gruppe anzuzeigen, zu bearbeiten oder zu duplizieren und mehr.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .

Gruppe anzeigen oder bearbeiten

Sie können die grundlegenden Informationen und Details für jede Gruppe anzeigen und bearbeiten.

Schritte

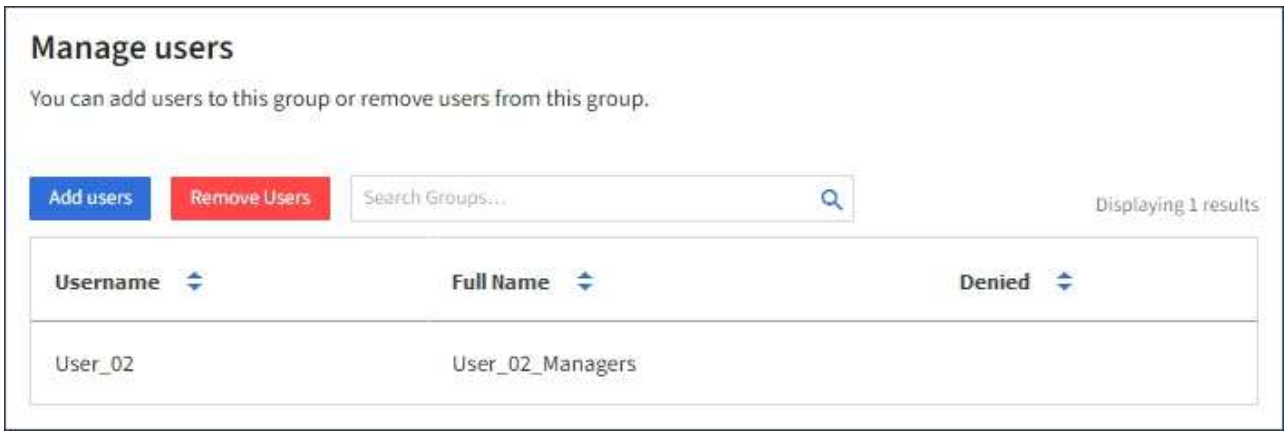
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Überprüfen Sie die Informationen auf der Seite „Gruppen“, auf der grundlegende Informationen zu allen lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

Wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie Gruppen im Quell-Grid des Mandanten anzeigen:

- Eine Bannermeldung weist darauf hin, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie eine Gruppe bearbeiten oder entfernen.
- Bei Bedarf zeigt eine Bannermeldung an, ob Gruppen nicht auf den Mandanten im Zielraster geklont wurden. Du kannstErneuter Versuch eines Gruppenklons das ist fehlgeschlagen.

3. Wenn Sie den Namen der Gruppe ändern möchten:
   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**.
4. Wenn Sie weitere Details anzeigen oder zusätzliche Änderungen vornehmen möchten, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie den Gruppennamen aus.
   - Aktivieren Sie das Kontrollkästchen für die Gruppe und wählen Sie **Aktionen** > **Gruppendetails anzeigen**.
5. Sehen Sie sich den Abschnitt „Übersicht“ an, der für jede Gruppe die folgenden Informationen enthält:
   - Anzeigename
   - Eindeutiger Name
   - Typ
   - Zugriffsmodus
   - Berechtigungen
   - S3-Richtlinie
   - Anzahl der Benutzer in dieser Gruppe
   - Zusätzliche Felder, wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie die Gruppe im Quell-Grid des Mandanten anzeigen:
     - Klonstatus, entweder **Erfolg** oder **Fehler**
     - Ein blaues Banner zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diese Gruppe bearbeiten oder löschen.
6. Bearbeiten Sie die Gruppeneinstellungen nach Bedarf. Sehen"Erstellen von Gruppen für einen S3-Mandanten" Und"Erstellen Sie Gruppen für einen Swift-Mandanten" für Details zu den einzugebenden Informationen.
   a. Ändern Sie im Abschnitt „Übersicht“ den Anzeigenamen, indem Sie den Namen oder das Bearbeitungssymbol auswählen .
   b. Aktualisieren Sie auf der Registerkarte **Gruppenberechtigungen** die Berechtigungen und wählen Sie **Änderungen speichern**.
   c. Nehmen Sie auf der Registerkarte **Gruppenrichtlinie** die gewünschten Änderungen vor und wählen Sie **Änderungen speichern**.
      - Wenn Sie eine S3-Gruppe bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus oder geben Sie bei Bedarf die JSON-Zeichenfolge für eine benutzerdefinierte Richtlinie ein.
      - Wenn Sie eine Swift-Gruppe bearbeiten, aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Swift-Administrator**.

7. So fügen Sie der Gruppe einen oder mehrere vorhandene lokale Benutzer hinzu:
   a. Wählen Sie die Registerkarte „Benutzer“ aus.



   b. Wählen Sie **Benutzer hinzufügen**.
   c. Wählen Sie die vorhandenen Benutzer aus, die Sie hinzufügen möchten, und wählen Sie **Benutzer hinzufügen**.

      Oben rechts erscheint eine Erfolgsmeldung.

8. So entfernen Sie lokale Benutzer aus der Gruppe:
   a. Wählen Sie die Registerkarte „Benutzer“ aus.
   b. Wählen Sie **Benutzer entfernen**.
   c. Wählen Sie die Benutzer aus, die Sie entfernen möchten, und wählen Sie **Benutzer entfernen**.

      Oben rechts erscheint eine Erfolgsmeldung.

9. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt die Option **Änderungen speichern** ausgewählt haben.

Gruppe duplizieren

Sie können eine vorhandene Gruppe duplizieren, um schneller neue Gruppen zu erstellen.

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie eine Gruppe aus dem Quell-Grid des Mandanten duplizieren, wird die duplizierte Gruppe in das Ziel-Grid des Mandanten geklont.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
3. Wählen Sie **Aktionen** > **Gruppe duplizieren**.
4. Sehen"Erstellen von Gruppen für einen S3-Mandanten" oder"Erstellen Sie Gruppen für einen Swift-Mandanten" für Details zu den einzugebenden Informationen.
5. Wählen Sie **Gruppe erstellen**.

Gruppenklon erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klonvorgang:

1. Wählen Sie jede Gruppe aus, bei der unter dem Gruppennamen *(Klonen fehlgeschlagen)* angezeigt wird.
2. Wählen Sie **Aktionen** > **Gruppen klonen**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jeder Gruppe an, die Sie klonen.

Weitere Informationen finden Sie unter"Mandantengruppen und Benutzer klonen" .

Löschen einer oder mehrerer Gruppen

Sie können eine oder mehrere Gruppen löschen. Alle Benutzer, die nur zu einer gelöschten Gruppe gehören, können sich nicht mehr beim Mandanten-Manager anmelden oder das Mandantenkonto verwenden.

> ⓘ Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie eine Gruppe löschen, löscht StorageGRID die entsprechende Gruppe im anderen Grid nicht. Wenn Sie diese Informationen synchron halten müssen, müssen Sie dieselbe Gruppe aus beiden Rastern löschen.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für jede Gruppe, die Sie löschen möchten.
3. Wählen Sie **Aktionen** > **Gruppe löschen** oder **Aktionen** > **Gruppen löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie **Gruppe löschen** oder **Gruppen löschen**.

Lokale Benutzer verwalten

Sie können lokale Benutzer erstellen und sie lokalen Gruppen zuweisen, um festzulegen, auf welche Funktionen diese Benutzer zugreifen können. Der Tenant Manager umfasst einen vordefinierten lokalen Benutzer namens „root“. Obwohl Sie lokale Benutzer hinzufügen und entfernen können, können Sie den Root-Benutzer nicht entfernen.

> ⓘ Wenn Single Sign-On (SSO) für Ihr StorageGRID -System aktiviert ist, können sich lokale Benutzer nicht beim Tenant Manager oder der Tenant Management API anmelden, obwohl sie basierend auf Gruppenberechtigungen Clientanwendungen verwenden können, um auf die Ressourcen des Mandanten zuzugreifen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, haben Sie den Workflow und die Überlegungen für"Klonen von Mandantengruppen und Benutzern" , und Sie sind beim Quellraster des Mandanten angemeldet.

Erstellen Sie einen lokalen Benutzer

Sie können einen lokalen Benutzer erstellen und ihn einer oder mehreren lokalen Gruppen zuweisen, um seine Zugriffsberechtigungen zu steuern.

Auf S3-Benutzer, die keiner Gruppe angehören, werden keine Verwaltungsberechtigungen oder S3-Gruppenrichtlinien angewendet. Diesen Benutzern wird möglicherweise über eine Bucket-Richtlinie Zugriff auf den S3-Bucket gewährt.

Swift-Benutzer, die keiner Gruppe angehören, verfügen weder über Verwaltungsberechtigungen noch über Zugriff auf Swift-Container.

Greifen Sie auf den Assistenten „Benutzer erstellen“ zu

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.

   Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, zeigt ein blaues Banner an, dass dies das Quell-Grid des Mandanten ist. Alle lokalen Benutzer, die Sie in diesem Raster erstellen, werden in das andere Raster in der Verbindung geklont.

2. Wählen Sie **Benutzer erstellen**.

Anmeldeinformationen eingeben

Schritte

1. Füllen Sie für den Schritt **Benutzeranmeldeinformationen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Vollständiger Name	Der vollständige Name dieses Benutzers, beispielsweise der Vor- und Nachname einer Person oder der Name einer Anwendung.
Benutzername	Der Name, den dieser Benutzer zum Anmelden verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden. **Hinweis**: Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, tritt ein Klonfehler auf, wenn derselbe **Benutzername** für den Mandanten im Zielgrid bereits vorhanden ist.
Passwort und Passwort bestätigen	Das Kennwort, das der Benutzer zunächst bei der Anmeldung verwendet.
Zugriff verweigern	Wählen Sie **Ja** aus, um zu verhindern, dass sich dieser Benutzer beim Mandantenkonto anmeldet, auch wenn er möglicherweise noch einer oder mehreren Gruppen angehört. Wählen Sie beispielsweise **Ja** aus, um die Anmeldemöglichkeit eines Benutzers vorübergehend zu sperren.

2. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

Schritte

1. Weisen Sie den Benutzer einer oder mehreren lokalen Gruppen zu, um festzulegen, welche Aufgaben er ausführen kann.

   Die Zuweisung eines Benutzers zu Gruppen ist optional. Wenn Sie möchten, können Sie beim Erstellen oder Bearbeiten von Gruppen Benutzer auswählen.

   Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören. Sehen "Berechtigungen zur Mandantenverwaltung" .

2. Wählen Sie **Benutzer erstellen**.

   Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie sich im Quell-Grid des Mandanten befinden, wird der neue lokale Benutzer in das Ziel-Grid des Mandanten geklont. **Erfolg** wird als **Klonstatus** im Abschnitt „Übersicht“ der Detailseite des Benutzers angezeigt.

3. Wählen Sie **Fertig**, um zur Seite „Benutzer“ zurückzukehren.

Lokalen Benutzer anzeigen oder bearbeiten

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Überprüfen Sie die Informationen auf der Seite „Benutzer“, auf der grundlegende Informationen zu allen lokalen und föderierten Benutzern für dieses Mandantenkonto aufgeführt sind.

   Wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie den Benutzer im Quell-Grid des Mandanten anzeigen:

   - Eine Bannermeldung weist darauf hin, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie einen Benutzer bearbeiten oder entfernen.
   - Bei Bedarf zeigt eine Bannermeldung an, ob Benutzer nicht in den Mandanten im Zielraster geklont wurden. Sie können Wiederholen Sie den Versuch, einen fehlgeschlagenen Benutzerklon auszuführen .
3. Wenn Sie den vollständigen Namen des Benutzers ändern möchten:
   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**.
4. Wenn Sie weitere Details anzeigen oder zusätzliche Änderungen vornehmen möchten, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie den Benutzernamen aus.
   - Aktivieren Sie das Kontrollkästchen für den Benutzer und wählen Sie **Aktionen** > **Benutzerdetails anzeigen**.
5. Sehen Sie sich den Abschnitt „Übersicht“ an, in dem für jeden Benutzer die folgenden Informationen angezeigt werden:

- Vollständiger Name
- Benutzername
- Benutzertyp
- Zugriff verweigert
- Zugriffsmodus
- Gruppenmitgliedschaft
- Zusätzliche Felder, wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie den Benutzer im Quell-Grid des Mandanten anzeigen:
  - Klonstatus, entweder **Erfolg** oder **Fehler**
  - Ein blaues Banner zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diesen Benutzer bearbeiten.

6. Bearbeiten Sie die Benutzereinstellungen nach Bedarf. SehenLokalen Benutzer erstellen für Details zu den einzugebenden Informationen.
   a. Ändern Sie im Abschnitt „Übersicht“ den vollständigen Namen, indem Sie den Namen oder das Bearbeitungssymbol auswählen .

      Sie können den Benutzernamen nicht ändern.

   b. Ändern Sie auf der Registerkarte **Passwort** das Passwort des Benutzers und wählen Sie **Änderungen speichern**.
   c. Wählen Sie auf der Registerkarte **Zugriff Nein** aus, um dem Benutzer die Anmeldung zu erlauben, oder wählen Sie **Ja** aus, um die Anmeldung des Benutzers zu verhindern. Wählen Sie dann **Änderungen speichern** aus.
   d. Wählen Sie auf der Registerkarte **Zugriffsschlüssel** die Option **Schlüssel erstellen** und folgen Sie den Anweisungen für"Erstellen der S3-Zugriffsschlüssel eines anderen Benutzers" .
   e. Wählen Sie auf der Registerkarte **Gruppen** die Option **Gruppen bearbeiten** aus, um den Benutzer zu Gruppen hinzuzufügen oder aus Gruppen zu entfernen. Wählen Sie dann **Änderungen speichern**.
7. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt die Option **Änderungen speichern** ausgewählt haben.

Duplizieren Sie den lokalen Benutzer

Sie können einen lokalen Benutzer duplizieren, um schneller einen neuen Benutzer zu erstellen.

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie einen Benutzer aus dem Quell-Grid des Mandanten duplizieren, wird der duplizierte Benutzer in das Ziel-Grid des Mandanten geklont.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Aktivieren Sie das Kontrollkästchen für den Benutzer, den Sie duplizieren möchten.
3. Wählen Sie **Aktionen** > **Benutzer duplizieren**.
4. SehenLokalen Benutzer erstellen für Details zu den einzugebenden Informationen.
5. Wählen Sie **Benutzer erstellen**.

Benutzerklon erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klonvorgang:

1. Wählen Sie jeden Benutzer aus, bei dem unter dem Benutzernamen *(Klonen fehlgeschlagen)* angezeigt wird.
2. Wählen Sie **Aktionen** > **Benutzer klonen**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jedes Benutzers an, den Sie klonen.

Weitere Informationen finden Sie unter"Mandantengruppen und Benutzer klonen" .

Löschen eines oder mehrerer lokaler Benutzer

Sie können einen oder mehrere lokale Benutzer dauerhaft löschen, die keinen Zugriff mehr auf das StorageGRID Mandantenkonto benötigen.

> Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie einen lokalen Benutzer löschen, löscht StorageGRID den entsprechenden Benutzer im anderen Grid nicht. Wenn Sie diese Informationen synchron halten müssen, müssen Sie denselben Benutzer aus beiden Rastern löschen.

> Sie müssen die Verbundidentitätsquelle verwenden, um Verbundbenutzer zu löschen.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie löschen möchten.
3. Wählen Sie **Aktionen** > **Benutzer löschen** oder **Aktionen** > **Benutzer löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie **Benutzer löschen** oder **Benutzer löschen**.

S3-Zugriffsschlüssel verwalten

S3-Zugriffsschlüssel verwalten

Jeder Benutzer eines S3-Mandantenkontos muss über einen Zugriffsschlüssel verfügen, um Objekte im StorageGRID System zu speichern und abzurufen. Ein Zugriffsschlüssel besteht aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel.

S3-Zugriffsschlüssel können wie folgt verwaltet werden:

- Benutzer mit der Berechtigung **Eigene S3-Anmeldeinformationen verwalten** können ihre eigenen S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit der Berechtigung **Root-Zugriff** können die Zugriffsschlüssel für das S3-Root-Konto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel bieten dem Mandanten vollständigen Zugriff auf alle Buckets und Objekte, sofern dies nicht ausdrücklich durch eine Bucket-Richtlinie deaktiviert wird.

StorageGRID unterstützt die Authentifizierung mit Signature Version 2 und Signature Version 4. Der kontoübergreifende Zugriff ist nicht zulässig, es sei denn, er wird ausdrücklich durch eine Bucket-Richtlinie aktiviert.

Erstellen Sie Ihre eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechende Berechtigung verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel erstellen. Sie benötigen einen Zugriffsschlüssel, um auf Ihre Buckets und Objekte zugreifen zu können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie Ihre eigenen S3-Anmeldeinformationen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Sie können einen oder mehrere S3-Zugriffsschlüssel erstellen, mit denen Sie Buckets für Ihr Mandantenkonto erstellen und verwalten können. Nachdem Sie einen neuen Zugriffsschlüssel erstellt haben, aktualisieren Sie die Anwendung mit Ihrer neuen Zugriffsschlüssel-ID und Ihrem geheimen Zugriffsschlüssel. Erstellen Sie aus Sicherheitsgründen nicht mehr Schlüssel als nötig und löschen Sie die Schlüssel, die Sie nicht verwenden. Wenn Sie nur einen Schlüssel haben und dieser bald abläuft, erstellen Sie einen neuen Schlüssel, bevor der alte abläuft, und löschen Sie dann den alten.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder nicht ablaufen. Befolgen Sie diese Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für Ihre Schlüssel fest, um Ihren Zugriff auf einen bestimmten Zeitraum zu beschränken. Durch das Festlegen einer kurzen Ablaufzeit können Sie Ihr Risiko verringern, wenn Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel versehentlich offengelegt werden. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie für Ihre Schlüssel keine Ablaufzeit festlegen. Wenn Sie sich später entscheiden, neue Schlüssel zu erstellen, löschen Sie die alten Schlüssel manuell.

> Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **SPEICHER (S3)** > **Meine Zugriffsschlüssel**.

   Die Seite „Meine Zugriffsschlüssel“ wird angezeigt und listet alle vorhandenen Zugriffsschlüssel auf.

2. Wählen Sie **Schlüssel erstellen**.
3. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie **Keine Ablaufzeit festlegen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
   - Wählen Sie **Ablaufzeit festlegen** und legen Sie das Ablaufdatum und die Ablaufzeit fest.

     > Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Ablaufzeit kann mindestens eine Minute nach der aktuellen Zeit liegen.

4. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld „Zugriffsschlüssel herunterladen“ wird angezeigt und listet Ihre Zugriffsschlüssel-ID und Ihren geheimen Zugriffsschlüssel auf.

5. Kopieren Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einen sicheren Ort oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.

   > Schließen Sie dieses Dialogfeld nicht, bis Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

6. Wählen Sie **Fertig**.

   Der neue Schlüssel wird auf der Seite „Meine Zugriffsschlüssel“ aufgeführt.

7. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie optional die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen. Sehen "Klonen Sie S3-Zugriffsschlüssel mithilfe der API" .

Zeigen Sie Ihre S3-Zugriffsschlüssel an

Wenn Sie einen S3-Tenant verwenden und über die"entsprechende Erlaubnis" können Sie eine Liste Ihrer S3-Zugriffsschlüssel anzeigen. Sie können die Liste nach Ablaufzeit sortieren, um festzustellen, welche Schlüssel bald ablaufen. Bei Bedarf können Sie"neue Schlüssel erstellen" oder"Schlüssel löschen" die Sie nicht mehr verwenden.

> Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören zu einer Benutzergruppe, die über die Berechtigung „S3-Anmeldeinformationen selbst verwalten“ verfügt."Erlaubnis" .

Schritte

1. Wählen Sie **SPEICHER (S3)** > **Meine Zugriffsschlüssel**.
2. Sortieren Sie auf der Seite „Meine Zugriffsschlüssel“ alle vorhandenen Zugriffsschlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie bei Bedarf neue Schlüssel oder löschen Sie alle Schlüssel, die Sie nicht mehr verwenden.

   Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, können Sie die neuen Schlüssel verwenden, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

   Abgelaufene Schlüssel werden automatisch entfernt.

Löschen Sie Ihre eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechende Berechtigung verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel löschen. Nachdem ein Zugriffsschlüssel gelöscht wurde, kann er nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten Sie Ihre eigenen S3-Anmeldeinformationen" .

> Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **SPEICHER (S3)** > **Meine Zugriffsschlüssel**.
2. Aktivieren Sie auf der Seite „Meine Zugriffsschlüssel“ das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie entfernen möchten.
3. Wählen Sie **Löschtaste**.
4. Wählen Sie im Bestätigungsdialogfeld **Schlüssel löschen** aus.

   In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.

Erstellen Sie die S3-Zugriffsschlüssel eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechende Berechtigung verfügen, können Sie S3-Zugriffsschlüssel für andere Benutzer erstellen, beispielsweise für Anwendungen, die Zugriff auf Buckets und Objekte benötigen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Sie können einen oder mehrere S3-Zugriffsschlüssel für andere Benutzer erstellen, damit diese Buckets für ihr Mandantenkonto erstellen und verwalten können. Nachdem Sie einen neuen Zugriffsschlüssel erstellt haben, aktualisieren Sie die Anwendung mit der neuen Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Erstellen Sie aus Sicherheitsgründen nicht mehr Schlüssel, als der Benutzer benötigt, und löschen Sie die Schlüssel, die nicht verwendet werden. Wenn Sie nur einen Schlüssel haben und dieser bald abläuft, erstellen Sie einen neuen Schlüssel, bevor der alte abläuft, und löschen Sie dann den alten.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder nicht ablaufen. Befolgen Sie diese Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für die Schlüssel fest, um den Zugriff des Benutzers auf einen bestimmten Zeitraum zu beschränken. Durch Festlegen einer kurzen Ablaufzeit können Sie das Risiko verringern,

wenn die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel versehentlich offengelegt werden. Abgelaufene Schlüssel werden automatisch entfernt.

- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie für die Schlüssel keine Ablaufzeit festlegen. Wenn Sie sich später entscheiden, neue Schlüssel zu erstellen, löschen Sie die alten Schlüssel manuell.

> Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Wählen Sie den Benutzer aus, dessen S3-Zugriffsschlüssel Sie verwalten möchten.

   Die Benutzerdetailseite wird angezeigt.

3. Wählen Sie **Zugriffsschlüssel** und dann **Schlüssel erstellen**.
4. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie **Keine Ablaufzeit festlegen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
   - Wählen Sie **Ablaufzeit festlegen** und legen Sie das Ablaufdatum und die Ablaufzeit fest.

     > Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Ablaufzeit kann mindestens eine Minute nach der aktuellen Zeit liegen.

5. Wählen Sie **Zugriffsschlüssel erstellen**.

   Das Dialogfeld „Zugriffsschlüssel herunterladen“ wird angezeigt und listet die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel auf.

6. Kopieren Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einen sicheren Ort oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.

   > Schließen Sie dieses Dialogfeld nicht, bis Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

7. Wählen Sie **Fertig**.

   Der neue Schlüssel wird auf der Registerkarte „Zugriffsschlüssel“ der Benutzerdetailseite aufgeführt.

8. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie optional die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen. Sehen "Klonen Sie S3-Zugriffsschlüssel mithilfe der API" .

Anzeigen der S3-Zugriffsschlüssel eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers anzeigen. Sie können die Liste nach Ablaufzeit sortieren, um festzustellen, welche Schlüssel bald ablaufen. Bei Bedarf können Sie neue Schlüssel erstellen und nicht mehr verwendete Schlüssel löschen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

> Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Wählen Sie auf der Seite „Benutzer“ den Benutzer aus, dessen S3-Zugriffsschlüssel Sie anzeigen möchten.
3. Wählen Sie auf der Seite „Benutzerdetails“ **Zugriffsschlüssel** aus.
4. Sortieren Sie die Schlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
5. Erstellen Sie bei Bedarf neue Schlüssel und löschen Sie nicht mehr verwendete Schlüssel manuell.

   Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, kann der Benutzer die neuen Schlüssel verwenden, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

   Abgelaufene Schlüssel werden automatisch entfernt.

Ähnliche Informationen

- "Erstellen Sie die S3-Zugriffsschlüssel eines anderen Benutzers"
- "Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers"

Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers löschen. Nachdem ein Zugriffsschlüssel gelöscht wurde, kann er nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.
2. Wählen Sie auf der Seite „Benutzer“ den Benutzer aus, dessen S3-Zugriffsschlüssel Sie verwalten möchten.
3. Wählen Sie auf der Seite „Benutzerdetails“ **Zugriffsschlüssel** aus und aktivieren Sie dann das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie löschen möchten.
4. Wählen Sie **Aktionen** > **Ausgewählten Schlüssel löschen**.
5. Wählen Sie im Bestätigungsdialogfeld **Schlüssel löschen** aus.

   In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.

S3-Buckets verwalten

Erstellen eines S3-Buckets

Mit dem Tenant Manager können Sie S3-Buckets für Objektdaten erstellen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören zu einer Benutzergruppe, die über Root-Zugriff oder die Möglichkeit verfügt, alle Buckets zu verwalten."Erlaubnis" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

  Berechtigungen zum Festlegen oder Ändern der S3 Object Lock-Eigenschaften von Buckets oder Objekten können erteilt werden durch"Bucket-Richtlinie oder Gruppenrichtlinie" .

- Wenn Sie S3 Object Lock für einen Bucket aktivieren möchten, hat ein Grid-Administrator die globale S3 Object Lock-Einstellung für das StorageGRID System aktiviert und Sie haben die Anforderungen für S3 Object Lock-Buckets und -Objekte überprüft.
- Wenn jeder Mandant über 5.000 Buckets verfügt, verfügt jeder Speicherknoten im Grid über mindestens 64 GB RAM.

  Jedes Raster kann maximal 100.000 Buckets enthalten.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie **Bucket erstellen**.

Details eingeben

Schritte

1. Geben Sie Details zum Bucket ein.

Feld	Beschreibung
Bucket-Name	Ein Name für den Bucket, der diesen Regeln entspricht: • Muss in jedem StorageGRID -System eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-kompatibel sein. • Muss mindestens 3 und darf nicht mehr als 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten. • Darf in Anfragen im virtuell gehosteten Stil keine Punkte enthalten. Punkte verursachen Probleme bei der Überprüfung des Platzhalterzertifikats des Servers. Weitere Informationen finden Sie im "Amazon Web Services (AWS)-Dokumentation zu Bucket-Benennungsregeln" . **Hinweis**: Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht mehr ändern.
Region	Die Region des Buckets. Ihr StorageGRID Administrator verwaltet die verfügbaren Regionen. Die Region eines Buckets kann sich auf die auf Objekte angewendete Datenschutzrichtlinie auswirken. Standardmäßig werden alle Buckets im `us-east-1` Region. **Hinweis**: Sie können die Region nach dem Erstellen des Buckets nicht mehr ändern.

2. Wählen Sie **Weiter**.

Einstellungen verwalten

Schritte

1. Aktivieren Sie optional die Objektversionierung für den Bucket.

   Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann bei Bedarf frühere Versionen eines Objekts abrufen. Sie müssen die Objektversionierung aktivieren, wenn der Bucket für die gitterübergreifende Replikation verwendet wird.

2. Wenn die globale Einstellung „S3 Object Lock“ aktiviert ist, aktivieren Sie optional „S3 Object Lock“ für den Bucket, um Objekte mithilfe eines WORM-Modells (Write-Once-Read-Many) zu speichern.

   Aktivieren Sie die S3-Objektsperre für einen Bucket nur, wenn Sie Objekte für einen festgelegten Zeitraum aufbewahren müssen, beispielsweise um bestimmte gesetzliche Anforderungen zu erfüllen. S3 Object

Lock ist eine permanente Einstellung, mit der Sie das Löschen oder Überschreiben von Objekten für einen festgelegten Zeitraum oder auf unbestimmte Zeit verhindern können.

> Nachdem die S3-Objektsperreinstellung für einen Bucket aktiviert wurde, kann sie nicht mehr deaktiviert werden. Jeder mit den entsprechenden Berechtigungen kann diesem Bucket Objekte hinzufügen, die nicht geändert werden können. Möglicherweise können Sie diese Objekte oder den Bucket selbst nicht löschen.

Wenn Sie S3 Object Lock für einen Bucket aktivieren, wird die Bucket-Versionierung automatisch aktiviert.

3. Wenn Sie **S3-Objektsperre aktivieren** ausgewählt haben, aktivieren Sie optional **Standardaufbewahrung** für diesen Bucket.

> Ihr Grid-Administrator muss Ihnen die Berechtigung erteilen,"Verwenden Sie bestimmte Funktionen von S3 Object Lock" .

Wenn die **Standardaufbewahrung** aktiviert ist, werden neue Objekte, die dem Bucket hinzugefügt werden, automatisch vor dem Löschen oder Überschreiben geschützt. Die Einstellung **Standardaufbewahrung** gilt nicht für Objekte, die über eigene Aufbewahrungszeiträume verfügen.

a. Wenn **Standardaufbewahrung** aktiviert ist, geben Sie einen **Standardaufbewahrungsmodus** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Führung	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung kann die `x-amz-bypass-governance-retention: true` Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen. • Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.
Einhaltung	• Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist. **Hinweis**: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.

b. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsdauer** für den Bucket an.

Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die diesem Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. Geben Sie einen Wert an, der kleiner oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsdauer für den

Mandanten ist.

Eine *maximale* Aufbewahrungsdauer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsdauer festlegen, darf diese den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsdauer zu verlängern oder zu verkürzen.

4. Wählen Sie optional **Kapazitätslimit aktivieren** aus.

   Die Kapazitätsgrenze ist die maximal verfügbare Kapazität für die Objekte dieses Buckets. Dieser Wert stellt eine logische Menge (Objektgröße) dar, keine physische Menge (Größe auf der Festplatte).

   Wenn kein Limit festgelegt ist, ist die Kapazität für diesen Bucket unbegrenzt. Weitere Informationen finden Sie unter "Kapazitätslimitnutzung" für weitere Informationen.

5. Wählen Sie **Bucket erstellen**.

   Der Bucket wird erstellt und der Tabelle auf der Seite „Buckets“ hinzugefügt.

6. Wählen Sie optional **Zur Bucket-Detailseite**, um"Bucket-Details anzeigen" und führen Sie zusätzliche Konfigurationen durch.

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto einsehen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriff, Alle Buckets verwalten oder Alle Buckets anzeigen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

   Die Seite „Buckets“ wird angezeigt.

2. Überprüfen Sie die Übersichtstabelle für jeden Bucket.

   Sie können die Informationen je nach Bedarf nach beliebigen Spalten sortieren oder in der Liste vor- und zurückblättern.

   > Die angezeigten Werte für Objektanzahl, belegten Speicherplatz und Nutzung sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektzählung einbezogen.

   Name

   Der eindeutige Name des Buckets, der nicht geändert werden kann.

Aktivierte Funktionen

Die Liste der Funktionen, die für den Bucket aktiviert sind.

S3-Objektsperre

Ob die S3-Objektsperre für den Bucket aktiviert ist.

Diese Spalte wird nur angezeigt, wenn die S3-Objektsperre für das Raster aktiviert ist. Diese Spalte zeigt auch Informationen zu allen älteren konformen Buckets an.

Region

Die Region des Buckets, die nicht geändert werden kann. Diese Spalte ist standardmäßig ausgeblendet.

Objektanzahl

Die Anzahl der Objekte in diesem Bucket. Wenn für Buckets die Versionierung aktiviert ist, sind nicht aktuelle Objektversionen in diesem Wert enthalten.

Wenn Objekte hinzugefügt oder gelöscht werden, wird dieser Wert möglicherweise nicht sofort aktualisiert.

Verwendeter Speicherplatz

Die logische Größe aller Objekte im Bucket. Die logische Größe umfasst nicht den tatsächlichen Speicherplatz, der für replizierte oder löschcodierte Kopien oder für Objektmetadaten benötigt wird.

Die Aktualisierung dieses Werts kann bis zu 10 Minuten dauern.

Verwendung

Der verwendete Prozentsatz der Kapazitätsgrenze des Buckets, sofern eine festgelegt wurde.

Der Nutzungswert basiert auf internen Schätzungen und kann in Einzelfällen überschritten werden. Beispielsweise überprüft StorageGRID das Kapazitätslimit (sofern festgelegt), wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen in diesen Bucket ab, wenn der Mandant das Kapazitätslimit überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kapazitätslimit überschritten wurde. Wenn Objekte gelöscht werden, kann es einem Mandanten vorübergehend untersagt werden, neue Objekte in diesen Bucket hochzuladen, bis die Kapazitätslimitnutzung neu berechnet wird. Die Berechnungen können 10 Minuten oder länger dauern.

Dieser Wert gibt die logische Größe an, nicht die physische Größe, die zum Speichern der Objekte und ihrer Metadaten erforderlich ist.

Kapazität

Falls festgelegt, die Kapazitätsgrenze für den Bucket.

Erstellungsdatum

Datum und Uhrzeit der Bucket-Erstellung. Diese Spalte ist standardmäßig ausgeblendet.

3. Um Details zu einem bestimmten Bucket anzuzeigen, wählen Sie den Bucket-Namen aus der Tabelle aus.
   a. Sehen Sie sich die zusammenfassenden Informationen oben auf der Webseite an, um die Details für den Bucket zu bestätigen, z. B. Region und Objektanzahl.
   b. Zeigen Sie die Kapazitätslimit-Nutzungsleiste an. Wenn die Nutzung 100 % oder nahe 100 % beträgt, sollten Sie eine Erhöhung des Limits oder das Löschen einiger Objekte in Erwägung ziehen.

c. Wählen Sie bei Bedarf **Objekte im Bucket löschen** und **Bucket löschen**.

> Achten Sie genau auf die Warnhinweise, die bei der Auswahl der einzelnen Optionen angezeigt werden. Weitere Informationen finden Sie unter:
>
> - "Alle Objekte in einem Bucket löschen"
> - "Löschen eines Buckets"(Eimer muss leer sein)

d. Zeigen Sie die Einstellungen für den Bucket in den einzelnen Registerkarten nach Bedarf an oder ändern Sie sie.

- **S3-Konsole**: Zeigen Sie die Objekte für den Bucket an. Weitere Informationen finden Sie unter "Verwenden Sie die S3-Konsole" .
- **Bucket-Optionen**: Optionseinstellungen anzeigen oder ändern. Einige Einstellungen, wie z. B. S3 Object Lock, können nach der Erstellung des Buckets nicht mehr geändert werden.
  - "Verwalten der Bucket-Konsistenz"
  - "Aktualisierungen der letzten Zugriffszeit"
  - "Kapazitätsgrenze"
  - "Objektversionierung"
  - "S3-Objektsperre"
  - "Standardmäßige Bucket-Aufbewahrung"
  - "Verwalten der Cross-Grid-Replikation"(sofern für den Mieter zulässig)
- **Plattformdienste**:"Plattformdienste verwalten" (sofern für den Mieter zulässig)
- **Bucket-Zugriff**: Optionseinstellungen anzeigen oder ändern. Sie müssen über bestimmte Zugriffsberechtigungen verfügen.
  - Konfigurieren"Cross-Origin-Ressourcenfreigabe (CORS)" sodass der Bucket und die Objekte im Bucket für Webanwendungen in anderen Domänen zugänglich sind.
  - "Benutzerzugriff steuern"für einen S3-Bucket und Objekte in diesem Bucket.

Anwenden eines ILM-Richtlinientags auf einen Bucket

Wählen Sie basierend auf Ihren Objektspeicheranforderungen ein ILM-Richtlinien-Tag aus, das auf einen Bucket angewendet werden soll.

Die ILM-Richtlinie steuert, wo die Objektdaten gespeichert werden und ob sie nach einer bestimmten Zeit gelöscht werden. Ihr Grid-Administrator erstellt ILM-Richtlinien und weist sie ILM-Richtlinien-Tags zu, wenn mehrere aktive Richtlinien verwendet werden.

> Vermeiden Sie die häufige Neuzuweisung des Richtlinien-Tags eines Buckets. Andernfalls können Leistungsprobleme auftreten.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriff, Alle Buckets verwalten oder Alle Buckets anzeigen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

   Die Seite „Buckets“ wird angezeigt. Sie können die Informationen je nach Bedarf nach beliebigen Spalten sortieren oder in der Liste vor- und zurückblättern.

2. Wählen Sie den Namen des Buckets aus, dem Sie ein ILM-Richtlinien-Tag zuweisen möchten.

   Sie können die ILM-Richtlinien-Tag-Zuweisung auch für einen Bucket ändern, dem bereits ein Tag zugewiesen ist.

   Die angezeigten Werte für „Objektanzahl“ und „Benutzter Speicherplatz“ sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektzählung einbezogen.

3. Erweitern Sie auf der Registerkarte „Bucket-Optionen“ das Akkordeon „ILM-Richtlinientag“. Dieses Akkordeon wird nur angezeigt, wenn Ihr Grid-Administrator die Verwendung benutzerdefinierter Richtlinien-Tags aktiviert hat.
4. Lesen Sie die Beschreibung jedes Richtlinien-Tags, um zu bestimmen, welches Tag auf den Bucket angewendet werden soll.

   Das Ändern des ILM-Richtlinientags für einen Bucket löst eine ILM-Neubewertung aller Objekte im Bucket aus. Wenn die neue Richtlinie Objekte für eine begrenzte Zeit aufbewahrt, werden ältere Objekte gelöscht.

5. Wählen Sie das Optionsfeld für das Tag aus, das Sie dem Bucket zuweisen möchten.
6. Wählen Sie **Änderungen speichern**. Ein neues S3-Bucket-Tag wird auf dem Bucket mit dem Schlüssel gesetzt `NTAP-SG-ILM-BUCKET-TAG` und der Wert des ILM-Richtlinien-Tag-Namens.

   Stellen Sie sicher, dass Ihre S3-Anwendungen das neue Bucket-Tag nicht versehentlich überschreiben oder löschen. Wenn dieses Tag beim Anwenden eines neuen TagSets auf den Bucket weggelassen wird, werden die Objekte im Bucket wieder anhand der ILM-Standardrichtlinie ausgewertet.

   Legen Sie ILM-Richtlinien-Tags fest und ändern Sie sie nur mithilfe des Tenant Managers oder der Tenant Manager-API, wo das ILM-Richtlinien-Tag validiert wird. Ändern Sie nicht die `NTAP-SG-ILM-BUCKET-TAG` ILM-Richtlinientag mithilfe der S3 PutBucketTagging-API oder der S3 DeleteBucketTagging-API.

   Das Ändern des einem Bucket zugewiesenen Richtlinientags hat vorübergehende Auswirkungen auf die Leistung, während Objekte mithilfe der neuen ILM-Richtlinie neu ausgewertet werden.

Bucket-Richtlinie verwalten

Sie können den Benutzerzugriff für einen S3-Bucket und die Objekte in diesem Bucket steuern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" . Die Berechtigungen „Alle Buckets anzeigen“ und „Alle Buckets verwalten“ erlauben nur das Anzeigen.
- Sie haben überprüft, dass die erforderliche Anzahl an Speicherknoten und Sites verfügbar ist. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder ein Standort nicht verfügbar ist, können diese Einstellungen möglicherweise nicht geändert werden.

Schritte

1. Wählen Sie **Buckets** und dann den Bucket aus, den Sie verwalten möchten.
2. Wählen Sie auf der Bucket-Detailseite **Bucket-Zugriff** > **Bucket-Richtlinie** aus.
3. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie eine Bucket-Richtlinie ein, indem Sie das Kontrollkästchen **Richtlinie aktivieren** aktivieren. Geben Sie dann eine gültige Zeichenfolge im JSON-Format ein.

     Jede Bucket-Richtlinie hat eine Größenbeschränkung von 20.480 Bytes.
   - Ändern Sie eine vorhandene Richtlinie, indem Sie die Zeichenfolge bearbeiten.
   - Deaktivieren Sie eine Richtlinie, indem Sie die Option **Richtlinie aktivieren** abwählen.

Ausführliche Informationen zu Bucket-Richtlinien, einschließlich Sprachsyntax und Beispielen, finden Sie unter"Beispiele für Bucket-Richtlinien" .

Verwalten der Bucket-Konsistenz

Konsistenzwerte können verwendet werden, um die Verfügbarkeit von Bucket-Einstellungsänderungen anzugeben und um ein Gleichgewicht zwischen der Verfügbarkeit der Objekte innerhalb eines Buckets und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Sites hinweg herzustellen. Sie können die Konsistenzwerte so ändern, dass sie von den Standardwerten abweichen, damit Clientanwendungen ihre Betriebsanforderungen erfüllen können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Richtlinien zur Eimerkonsistenz

Die Bucket-Konsistenz wird verwendet, um die Konsistenz für Clientanwendungen zu bestimmen, die sich auf Objekte innerhalb dieses S3-Buckets auswirken. Im Allgemeinen sollten Sie für Ihre Buckets die Konsistenz **Lesen nach neuem Schreiben** verwenden.

Konsistenz des Änderungs-Buckets

Wenn die Konsistenz von **Read-after-new-write** nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz ändern, indem Sie die Bucket-Konsistenz festlegen oder indem Sie die `Consistency-Control` Kopfzeile. Der `Consistency-Control` Header überschreibt die Bucket-Konsistenz.

Wenn Sie die Konsistenz eines Buckets ändern, wird nur für die Objekte, die nach der Änderung aufgenommen werden, garantiert, dass sie der überarbeiteten Einstellung entsprechen.

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

   Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das ** Akkordeon aus.
4. Wählen Sie eine Konsistenz für Vorgänge aus, die an den Objekten in diesem Bucket ausgeführt werden.
   - **Alle**: Bietet das höchste Maß an Konsistenz. Alle Knoten empfangen die Daten sofort, andernfalls schlägt die Anforderung fehl.
   - **Stark global**: Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites.
   - **Strong-Site**: Garantiert die Lese-nach-Schreib-Konsistenz für alle Clientanforderungen innerhalb einer Site.
   - **Lesen nach neuem Schreiben** (Standard): Bietet Lese-nach-Schreib-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
   - **Verfügbar**: Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.
5. Wählen Sie **Änderungen speichern**.

Was passiert, wenn Sie die Bucket-Einstellungen ändern?

Buckets verfügen über mehrere Einstellungen, die das Verhalten der Buckets und der Objekte in diesen Buckets beeinflussen.

Die folgenden Bucket-Einstellungen verwenden standardmäßig **starke** Konsistenz. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder wenn ein Standort nicht verfügbar ist, sind Änderungen an diesen Einstellungen möglicherweise nicht möglich.

- "Löschen eines leeren Buckets im Hintergrund"
- "Letzter Zugriffszeitpunkt"
- "Bucket-Lebenszyklus"
- "Bucket-Richtlinie"
- "Bucket-Tagging"
- "Bucket-Versionierung"
- "S3-Objektsperre"
- "Bucket-Verschlüsselung"

Der Konsistenzwert für Bucket-Versionierung, S3-Objektsperre und Bucket-Verschlüsselung kann nicht auf einen Wert eingestellt werden, der nicht stark konsistent ist.

Die folgenden Bucket-Einstellungen verwenden keine starke Konsistenz und weisen eine höhere Verfügbarkeit für Änderungen auf. Es kann einige Zeit dauern, bis Änderungen an diesen Einstellungen wirksam werden.

- "Konfiguration der Plattformdienste: Benachrichtigung, Replikation oder Suchintegration"
- "CORS-Konfiguration"
- Eimerkonsistenz ändern

> Wenn die beim Ändern der Bucket-Einstellungen verwendete Standardkonsistenz nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz mithilfe der `Consistency-Control` Kopfzeile für die"S3 REST API" oder mithilfe der `reducedConsistency` oder `force` Optionen in der"Mandantenverwaltungs-API" .

Aktivieren oder Deaktivieren der Aktualisierung der letzten Zugriffszeit

Wenn Grid-Administratoren die Regeln für das Information Lifecycle Management (ILM) für ein StorageGRID System erstellen, können sie optional angeben, dass der Zeitpunkt des letzten Zugriffs auf ein Objekt verwendet werden soll, um zu bestimmen, ob dieses Objekt an einen anderen Speicherort verschoben werden soll. Wenn Sie einen S3-Mandanten verwenden, können Sie solche Regeln nutzen, indem Sie Aktualisierungen der letzten Zugriffszeit für die Objekte in einem S3-Bucket aktivieren.

Diese Anweisungen gelten nur für StorageGRID -Systeme, die mindestens eine ILM-Regel enthalten, die die Option **Letzter Zugriffszeitpunkt** als erweiterten Filter oder als Referenzzeit verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System keine solche Regel enthält. Sehen"Verwenden der letzten Zugriffszeit in ILM-Regeln" für Details.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Informationen zu diesem Vorgang

Letzter Zugriffszeitpunkt ist eine der verfügbaren Optionen für die Platzierungsanweisung **Referenzzeitpunkt** für eine ILM-Regel. Durch Festlegen der Referenzzeit für eine Regel auf „Letzter Zugriffszeitpunkt“ können Grid-Administratoren festlegen, dass Objekte an bestimmten Speicherorten abgelegt werden, basierend auf dem Zeitpunkt, zu dem diese Objekte zuletzt abgerufen (gelesen oder angezeigt) wurden.

Um beispielsweise sicherzustellen, dass kürzlich angezeigte Objekte auf einem schnelleren Speicher verbleiben, kann ein Grid-Administrator eine ILM-Regel erstellen, die Folgendes angibt:

- Objekte, die im letzten Monat abgerufen wurden, sollten auf lokalen Speicherknoten verbleiben.
- Objekte, die im letzten Monat nicht abgeholt wurden, sollten an einen externen Standort gebracht werden.

Standardmäßig sind Aktualisierungen der letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option **Letzter Zugriffszeitpunkt** verwendet, und Sie möchten, dass diese Option auf Objekte in diesem Bucket angewendet wird, müssen Sie Aktualisierungen des letzten Zugriffszeitpunkts für die in dieser Regel angegebenen S3-Buckets aktivieren.

Das Aktualisieren der letzten Zugriffszeit beim Abrufen eines Objekts kann die StorageGRID Leistung verringern, insbesondere bei kleinen Objekten.

Bei Aktualisierungen der letzten Zugriffszeit kommt es zu Leistungseinbußen, da StorageGRID bei jedem Abrufen von Objekten die folgenden zusätzlichen Schritte ausführen muss:

- Aktualisieren Sie die Objekte mit neuen Zeitstempeln
- Fügen Sie die Objekte zur ILM-Warteschlange hinzu, damit sie anhand der aktuellen ILM-Regeln und -Richtlinien neu bewertet werden können

Die Tabelle fasst das Verhalten zusammen, das auf alle Objekte im Bucket angewendet wird, wenn die letzte Zugriffszeit deaktiviert oder aktiviert ist.

Art der Anfrage	Verhalten, wenn die letzte Zugriffszeit deaktiviert ist (Standard)		Verhalten bei aktivierter letzter Zugriffszeit	
	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?
Anforderung zum Abrufen eines Objekts, seiner Zugriffskontrollliste oder seiner Metadaten	Nein	Nein	Ja	Ja
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja	Ja	Ja	Ja
Anfrage zum Auflisten von Objekten oder Objektversionen	Nein	Nein	Nein	Nein
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
Anfrage zum Abschließen eines mehrteiligen Uploads	Ja, für das montierte Objekt	Ja, für das montierte Objekt	Ja, für das montierte Objekt	Ja, für das montierte Objekt

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

   Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **Aktualisierungen der letzten Zugriffszeit** aus.
4. Aktivieren oder deaktivieren Sie Aktualisierungen der letzten Zugriffszeit.
5. Wählen Sie **Änderungen speichern**.

Ändern der Objektversionierung für einen Bucket

Wenn Sie einen S3-Mandanten verwenden, können Sie den Versionsstatus für S3-Buckets ändern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Sie haben überprüft, dass die erforderliche Anzahl an Speicherknoten und Sites verfügbar ist. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder ein Standort nicht verfügbar ist, können diese Einstellungen möglicherweise nicht geändert werden.

Informationen zu diesem Vorgang

Sie können die Objektversionierung für einen Bucket aktivieren oder aussetzen. Nachdem Sie die Versionierung für einen Bucket aktiviert haben, kann dieser nicht mehr in einen nicht versionierten Zustand zurückversetzt werden. Sie können die Versionierung für den Bucket jedoch aussetzen.

- Deaktiviert: Die Versionierung wurde nie aktiviert
- Aktiviert: Versionierung ist aktiviert
- Ausgesetzt: Die Versionsverwaltung war zuvor aktiviert und ist ausgesetzt

Weitere Informationen finden Sie unter:

- "Objektversionierung"
- "ILM-Regeln und -Richtlinien für versionierte S3-Objekte (Beispiel 4)"
- "So werden Objekte gelöscht"

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

   Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **Objektversionierung** aus.
4. Wählen Sie einen Versionsstatus für die Objekte in diesem Bucket aus.

   Die Objektversionierung muss für einen Bucket aktiviert bleiben, der für die Cross-Grid-Replikation

verwendet wird. Wenn S3 Object Lock oder Legacy-Compliance aktiviert ist, sind die Optionen zur **Objektversionierung** deaktiviert.

Option	Beschreibung
Aktivieren der Versionsverwaltung	Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann bei Bedarf frühere Versionen eines Objekts abrufen. Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.
Versionsverwaltung aussetzen	Unterbrechen Sie die Objektversionierung, wenn Sie nicht mehr möchten, dass neue Objektversionen erstellt werden. Sie können weiterhin alle vorhandenen Objektversionen abrufen.

5. Wählen Sie **Änderungen speichern**.

Verwenden Sie S3 Object Lock, um Objekte beizubehalten

Sie können S3 Object Lock verwenden, wenn Buckets und Objekte den gesetzlichen Aufbewahrungsanforderungen entsprechen müssen.

Ihr Grid-Administrator muss Ihnen die Berechtigung zur Verwendung bestimmter Funktionen von S3 Object Lock erteilen.

Was ist S3 Object Lock?

Die StorageGRID S3 Object Lock-Funktion ist eine Objektschutzlösung, die S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

Wenn die globale S3-Objektsperre-Einstellung für ein StorageGRID -System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn für einen Bucket die S3-Objektsperre aktiviert ist, ist eine Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Ein Bucket ohne S3-Objektsperre kann nur Objekte ohne angegebene Aufbewahrungseinstellungen enthalten. Für aufgenommene Objekte werden keine Aufbewahrungseinstellungen festgelegt.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen enthalten, die von S3-Clientanwendungen angegeben werden. Für einige aufgenommene Objekte gelten Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann hochgeladene Objekte mit angegebenen Aufbewahrungseinstellungen und neue Objekte ohne Aufbewahrungseinstellungen enthalten. Die neuen Objekte verwenden die Standardeinstellung, da die Aufbewahrungseinstellung nicht auf Objektebene konfiguriert wurde.

Tatsächlich verfügen alle neu aufgenommenen Objekte über Aufbewahrungseinstellungen, wenn die Standardaufbewahrung konfiguriert ist. Vorhandene Objekte ohne Objektaufbewahrungseinstellungen bleiben davon unberührt.

Aufbewahrungsmodi

Die StorageGRID S3 Object Lock-Funktion unterstützt zwei Aufbewahrungsmodi, um unterschiedliche Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Aufbewahrungsmodi von Amazon S3.

- Im Compliance-Modus:
  - Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
  - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
  - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
  - Benutzer mit Sonderberechtigung können in Anfragen einen Bypass-Header verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
  - Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.
  - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mit der S3-Clientanwendung optional die folgenden Aufbewahrungseinstellungen für jedes dem Bucket hinzugefügte Objekt angeben:

- **Aufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Aufbewahrungsdatum**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Rechtliche Sperre**: Durch Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise müssen Sie möglicherweise ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht, rechtlich sperren. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie ausdrücklich aufgehoben wird. Rechtliche Sperren sind unabhängig vom Aufbewahrungsdatum.

  > ⓘ Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

  Details zu den Objekteinstellungen finden Sie unter"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .

Standardaufbewahrungseinstellung für Buckets

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Standardaufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Standardaufbewahrungszeitraum**: Wie lange neue Objektversionen, die diesem Bucket hinzugefügt werden, ab dem Tag ihrer Hinzufügung aufbewahrt werden sollen.

Die Standard-Bucket-Einstellungen gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Vorhandene Bucket-Objekte sind nicht betroffen, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

Sehen"Erstellen eines S3-Buckets" Und"Standardaufbewahrung für S3 Object Lock aktualisieren" .

S3 Object Lock-Aufgaben

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die allgemeinen Aufgaben zur Verwendung der S3 Object Lock-Funktion.

Grid-Administrator

- Aktivieren Sie die globale S3-Objektsperreinstellung für das gesamte StorageGRID System.
- Stellen Sie sicher, dass die Richtlinien für das Information Lifecycle Management (ILM) *konform* sind; das heißt, sie erfüllen die"Anforderungen an Buckets mit aktivierter S3-Objektsperre" .
- Erlauben Sie einem Mandanten bei Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungsdauer für einen Mandanten fest.

Mandantenbenutzer

- Überprüfen Sie die Überlegungen zu Buckets und Objekten mit S3 Object Lock.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3-Objektsperreinstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen Sie Buckets mit aktivierter S3-Objektsperre.
- Konfigurieren Sie optional die Standardaufbewahrungseinstellungen für einen Bucket:
  - Standardaufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Standardaufbewahrungszeitraum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.
- Verwenden Sie die S3-Clientanwendung, um Objekte hinzuzufügen und optional eine objektspezifische Aufbewahrung festzulegen:
  - Aufbewahrungsmodus. Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Aufbewahrungsdatum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.

Anforderungen für Buckets mit aktivierter S3-Objektsperre

- Wenn die globale S3-Objektsperre-Einstellung für das StorageGRID -System aktiviert ist, können Sie den Tenant Manager, die Tenant Management API oder die S3 REST API verwenden, um Buckets mit aktivierter S3-Objektsperre zu erstellen.
- Wenn Sie S3 Object Lock verwenden möchten, müssen Sie S3 Object Lock beim Erstellen des Buckets aktivieren. Sie können S3 Object Lock nicht für einen vorhandenen Bucket aktivieren.
- Wenn S3 Object Lock für einen Bucket aktiviert ist, aktiviert StorageGRID automatisch die Versionierung für diesen Bucket. Sie können die S3-Objektsperre nicht deaktivieren oder die Versionsverwaltung für den Bucket aussetzen.
- Optional können Sie mithilfe des Tenant Managers, der Tenant Management API oder der S3 REST API einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer für jeden Bucket angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt werden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen überschreiben, indem Sie beim Hochladen für jede Objektversion einen Aufbewahrungsmodus und ein Aufbewahrungsdatum angeben.
- Die Bucket-Lebenszykluskonfiguration wird für Buckets mit aktivierter S3-Objektsperre unterstützt.
- Die CloudMirror-Replikation wird für Buckets mit aktivierter S3-Objektsperre nicht unterstützt.

Anforderungen für Objekte in Buckets mit aktivierter S3-Objektsperre

- Um eine Objektversion zu schützen, können Sie Standardaufbewahrungseinstellungen für den Bucket oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mithilfe der S3-Clientanwendung oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl über eine Aufbewahrungsfrist als auch über eine gesetzliche Aufbewahrungsfrist verfügen, über eine der beiden Einstellungen, aber nicht über die andere, oder über keine von beiden. Durch die Angabe eines Aufbewahrungsdatums oder einer Einstellung für die rechtliche Aufbewahrung eines Objekts wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets mit aktivierter S3-Objektsperre

Jedes Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft die folgenden Phasen:

1. **Objektaufnahme**

   Wenn eine Objektversion zu einem Bucket hinzugefügt wird, für den die S3-Objektsperre aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

   - Wenn für das Objekt Aufbewahrungseinstellungen angegeben sind, werden die Einstellungen auf Objektebene angewendet. Alle Standard-Bucket-Einstellungen werden ignoriert.
   - Wenn für das Objekt keine Aufbewahrungseinstellungen angegeben sind, werden die Standard-Bucket-Einstellungen angewendet, sofern diese vorhanden sind.
   - Wenn für das Objekt oder den Bucket keine Aufbewahrungseinstellungen angegeben sind, ist das Objekt nicht durch S3 Object Lock geschützt.

   Wenn Aufbewahrungseinstellungen angewendet werden, sind sowohl das Objekt als auch alle benutzerdefinierten S3-Metadaten geschützt.

2. **Objektaufbewahrung und -löschung**

   Von jedem geschützten Objekt werden von StorageGRID mehrere Kopien für den angegebenen Aufbewahrungszeitraum gespeichert. Die genaue Anzahl und Art der Objektkopien sowie die Speicherorte werden durch die konformen Regeln in den aktiven ILM-Richtlinien bestimmt. Ob ein geschütztes Objekt vor Erreichen seines Aufbewahrungsdatums gelöscht werden kann, hängt von seinem Aufbewahrungsmodus ab.

   - Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

Kann ich weiterhin ältere konforme Buckets verwalten?

Die S3 Object Lock-Funktion ersetzt die Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war. Wenn Sie konforme Buckets mit einer früheren Version von StorageGRID erstellt haben, können Sie die Einstellungen dieser Buckets weiterhin verwalten. Sie können jedoch keine neuen konformen Buckets mehr erstellen. Anweisungen hierzu finden Sie unterhttps://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"^] .

Standardaufbewahrung für S3 Object Lock aktualisieren

Wenn Sie beim Erstellen des Buckets die S3-Objektsperre aktiviert haben, können Sie den Bucket bearbeiten, um die Standardaufbewahrungseinstellungen zu ändern. Sie können die Standardaufbewahrung aktivieren (oder deaktivieren) und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer festlegen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Object Lock ist global für Ihr StorageGRID -System aktiviert und Sie haben S3 Object Lock beim Erstellen des Buckets aktiviert. Sehen "Verwenden Sie S3 Object Lock, um Objekte beizubehalten" .

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

   Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **S3-Objektsperre** aus.
4. Aktivieren oder deaktivieren Sie optional die **Standardaufbewahrung** für diesen Bucket.

   Änderungen an dieser Einstellung gelten nicht für Objekte, die sich bereits im Bucket befinden, oder für Objekte, die möglicherweise eigene Aufbewahrungszeiträume haben.

5. Wenn **Standardaufbewahrung** aktiviert ist, geben Sie einen **Standardaufbewahrungsmodus** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Führung	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung kann die `x-amz-bypass-governance-retention: true` Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen. • Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Standardaufbewahrungsmodus	Beschreibung
Einhaltung	• Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist. **Hinweis**: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.

6. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsdauer** für den Bucket an.

   Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die diesem Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. Geben Sie einen Wert an, der kleiner oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsdauer für den Mandanten ist.

   Eine *maximale* Aufbewahrungsdauer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsdauer festlegen, darf diese den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsdauer zu verlängern oder zu verkürzen.

7. Wählen Sie **Änderungen speichern**.

Konfigurieren Sie Cross-Origin Resource Sharing (CORS)

Sie können Cross-Origin Resource Sharing (CORS) für einen S3-Bucket konfigurieren, wenn dieser Bucket und die darin enthaltenen Objekte für Webanwendungen in anderen Domänen zugänglich sein sollen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Für GET CORS-Konfigurationsanfragen gehören Sie zu einer Benutzergruppe, die über die"Berechtigung „Alle Buckets verwalten“ oder „Alle Buckets anzeigen““ . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Für PUT CORS-Konfigurationsanfragen gehören Sie zu einer Benutzergruppe, die über die"Berechtigung „Alle Buckets verwalten““ . Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Der"Root-Zugriffsberechtigung" bietet Zugriff auf alle CORS-Konfigurationsanforderungen.

Informationen zu diesem Vorgang

Cross-Origin Resource Sharing (CORS) ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, Sie verwenden einen S3-Bucket namens `Images` zum Speichern von Grafiken. Durch die Konfiguration von CORS für die `Images` Bucket, können Sie die Anzeige der Bilder in diesem Bucket auf der Website zulassen `http://www.example.com` .

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um das erforderliche XML zu erstellen. Dieses Beispiel zeigt das XML, das zum Aktivieren von CORS für einen S3-Bucket verwendet wird. Speziell:
   - Ermöglicht jeder Domäne, GET-Anfragen an den Bucket zu senden
   - Erlaubt nur die `http://www.example.com` Domäne zum Senden von GET-, POST- und DELETE-Anfragen
   - Alle Anforderungsheader sind zulässig

   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedMethod>POST</AllowedMethod>
           <AllowedMethod>DELETE</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
   </CORSConfiguration>
   ```

   Weitere Informationen zur CORS-Konfigurations-XML finden Sie unter "Amazon Web Services (AWS)-Dokumentation: Amazon Simple Storage Service-Benutzerhandbuch" .

2. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
3. Wählen Sie den Bucket-Namen aus der Tabelle aus.

   Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie auf der Registerkarte **Bucket-Zugriff** das Akkordeon **Cross-Origin Resource Sharing (CORS)** aus.
5. Aktivieren Sie das Kontrollkästchen **CORS aktivieren**.
6. Fügen Sie die CORS-Konfigurations-XML in das Textfeld ein.
7. Wählen Sie **Änderungen speichern**.

CORS-Einstellung ändern

Schritte

1. Aktualisieren Sie die CORS-Konfigurations-XML im Textfeld oder wählen Sie **Löschen** aus, um von vorne zu beginnen.
2. Wählen Sie **Änderungen speichern**.

CORS-Einstellung deaktivieren

Schritte

1. Deaktivieren Sie das Kontrollkästchen **CORS aktivieren**.
2. Wählen Sie **Änderungen speichern**.

Objekte im Bucket löschen

Mit dem Tenant Manager können Sie die Objekte in einem oder mehreren Buckets löschen.

Überlegungen und Anforderungen

Beachten Sie vor der Durchführung dieser Schritte Folgendes:

- Wenn Sie die Objekte in einem Bucket löschen, entfernt StorageGRID dauerhaft alle Objekte und alle Objektversionen in jedem ausgewählten Bucket von allen Knoten und Sites in Ihrem StorageGRID System. StorageGRID entfernt auch alle zugehörigen Objektmetadaten. Sie können diese Informationen nicht wiederherstellen.
- Das Löschen aller Objekte in einem Bucket kann je nach Anzahl der Objekte, Objektkopien und gleichzeitigen Vorgängen Minuten, Tage oder sogar Wochen dauern.
- Wenn ein Eimer"S3-Objektsperre aktiviert" , kann es *Jahre* lang im Status **Objekte werden gelöscht: schreibgeschützt** verbleiben.

  Ein Bucket, der S3 Object Lock verwendet, verbleibt im Status **Objekte werden gelöscht: schreibgeschützt**, bis das Aufbewahrungsdatum für alle Objekte erreicht ist und alle rechtlichen Sperren aufgehoben wurden.

- Während Objekte gelöscht werden, lautet der Status des Buckets **Objekte werden gelöscht: schreibgeschützt**. In diesem Zustand können Sie dem Bucket keine neuen Objekte hinzufügen.
- Wenn alle Objekte gelöscht wurden, bleibt der Bucket im schreibgeschützten Zustand. Sie können einen der folgenden Schritte ausführen:
  - Setzen Sie den Bucket wieder in den Schreibmodus und verwenden Sie ihn erneut für neue Objekte
  - Löschen Sie den Bucket
  - Behalten Sie den Bucket im schreibgeschützten Modus, um seinen Namen für die zukünftige Verwendung zu reservieren
- Wenn für einen Bucket die Objektversionierung aktiviert ist, können Löschmarkierungen, die in StorageGRID 11.8 oder höher erstellt wurden, mithilfe der Vorgänge „Objekte im Bucket löschen“ entfernt werden.
- Wenn für einen Bucket die Objektversionierung aktiviert ist, werden beim Löschen von Objekten keine Löschmarkierungen entfernt, die in StorageGRID 11.7 oder früher erstellt wurden. Informationen zum Löschen von Objekten in einem Bucket finden Sie in"So werden versionierte S3-Objekte gelöscht" .
- Wenn Sie"Cross-Grid-Replikation" , beachten Sie Folgendes:
  - Durch die Verwendung dieser Option werden keine Objekte aus dem Bucket im anderen Raster gelöscht.
  - Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **Fehler bei der Grid-übergreifenden Replikation** ausgelöst, wenn Sie dem Ziel-Bucket im anderen Grid Objekte hinzufügen. Wenn Sie nicht garantieren können, dass niemand Objekte zum Bucket auf dem anderen Raster hinzufügt,"Deaktivieren Sie die Cross-Grid-Replikation" für diesen Bucket, bevor alle Bucket-

Objekte gelöscht werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" . Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

   Die Seite „Buckets“ wird angezeigt und zeigt alle vorhandenen S3-Buckets.

2. Verwenden Sie das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket.

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, aus dem Sie Objekte löschen möchten.

   b. Wählen Sie **Aktionen** > **Objekte im Bucket löschen**.

   Detailseite

   a. Wählen Sie einen Bucket-Namen aus, um dessen Details anzuzeigen.

   b. Wählen Sie **Objekte im Bucket löschen**.

3. Wenn das Bestätigungsdialogfeld angezeigt wird, überprüfen Sie die Details, geben Sie **Ja** ein und wählen Sie **OK**.
4. Warten Sie, bis der Löschvorgang beginnt.

   Nach einigen Minuten:

   - Auf der Bucket-Detailseite wird ein gelbes Statusbanner angezeigt. Der Fortschrittsbalken zeigt an, wie viel Prozent der Objekte gelöscht wurden.
   - **(schreibgeschützt)** wird nach dem Bucket-Namen auf der Bucket-Detailseite angezeigt.
   - **(Objekte löschen: schreibgeschützt)** wird neben dem Namen des Buckets auf der Seite „Buckets“ angezeigt.

5. Wählen Sie bei Bedarf während der Ausführung des Vorgangs **Löschen von Objekten stoppen** aus, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Vorgang fortzusetzen.

   Wenn Sie „Löschen von Objekten beenden“ auswählen, wird der Bucket wieder in den Schreibmodus versetzt. Sie können jedoch nicht auf gelöschte Objekte zugreifen oder diese wiederherstellen.

6. Warten Sie, bis der Vorgang abgeschlossen ist.

   Wenn der Bucket leer ist, wird das Statusbanner aktualisiert, der Bucket bleibt jedoch schreibgeschützt.

7. Führen Sie einen der folgenden Schritte aus:

   - Verlassen Sie die Seite, um den Bucket im schreibgeschützten Modus zu belassen. Sie können beispielsweise einen leeren Bucket im schreibgeschützten Modus belassen, um den Bucket-Namen für

die zukünftige Verwendung zu reservieren.

- Löschen Sie den Bucket. Sie können **Bucket löschen** auswählen, um einen einzelnen Bucket zu löschen, oder zur Buckets-Seite zurückkehren und **Aktionen** > **Buckets löschen** auswählen, um mehr als einen Bucket zu entfernen.

  > ⓘ Wenn Sie einen versionierten Bucket nicht löschen können, nachdem alle Objekte gelöscht wurden, bleiben möglicherweise Löschmarkierungen zurück. Um den Bucket zu löschen, müssen Sie alle verbleibenden Löschmarkierungen entfernen.

- Bringen Sie den Bucket zurück in den Schreibmodus und verwenden Sie ihn optional für neue Objekte erneut. Sie können **Löschen von Objekten stoppen** für einen einzelnen Bucket auswählen oder zur Buckets-Seite zurückkehren und **Aktion** > **Löschen von Objekten stoppen** für mehr als einen Bucket auswählen.

S3-Bucket löschen

Mit dem Tenant Manager können Sie einen oder mehrere leere S3-Buckets löschen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Die Buckets, die Sie löschen möchten, sind leer. Wenn die Buckets, die Sie löschen möchten, *nicht* leer sind,"Objekte aus dem Bucket löschen" .

Informationen zu diesem Vorgang

Diese Anweisungen beschreiben, wie Sie einen S3-Bucket mit dem Tenant Manager löschen. Sie können S3-Buckets auch löschen, indem Sie"Mandantenverwaltungs-API" oder die"S3 REST API" .

Sie können einen S3-Bucket nicht löschen, wenn er Objekte, nicht aktuelle Objektversionen oder Löschmarkierungen enthält. Informationen zum Löschen versionierter S3-Objekte finden Sie unter"So werden Objekte gelöscht" .

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

   Die Seite „Buckets“ wird angezeigt und zeigt alle vorhandenen S3-Buckets.

2. Verwenden Sie das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket.

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, den Sie löschen möchten.

   b. Wählen Sie **Aktionen** > **Buckets löschen**.

   Detailseite

   a. Wählen Sie einen Bucket-Namen aus, um dessen Details anzuzeigen.

   b. Wählen Sie **Bucket löschen**.

3. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**.

   StorageGRID bestätigt, dass jeder Bucket leer ist, und löscht dann jeden Bucket. Dieser Vorgang kann einige Minuten dauern.

   Wenn ein Bucket nicht leer ist, erscheint eine Fehlermeldung. Sie müssen"alle Objekte und alle Löschmarkierungen im Bucket löschen" bevor Sie den Bucket löschen können.

Verwenden Sie die S3-Konsole

Sie können die S3-Konsole verwenden, um die Objekte in einem S3-Bucket anzuzeigen und zu verwalten.

Mit der S3-Konsole können Sie:

- Objekte hochladen, herunterladen, umbenennen, kopieren, verschieben und löschen
- Objektversionen anzeigen, zurücksetzen, herunterladen und löschen
- Suche nach Objekten anhand des Präfixes
- Objekt-Tags verwalten
- Objektmetadaten anzeigen
- Ordner anzeigen, erstellen, umbenennen, kopieren, verschieben und löschen

> Die S3-Konsole bietet in den gängigsten Fällen eine verbesserte Benutzererfahrung. Es ist nicht dafür gedacht, CLI- oder API-Operationen in allen Situationen zu ersetzen.
>
> Wenn die Verwendung der S3-Konsole dazu führt, dass Vorgänge zu lange dauern (z. B. Minuten oder Stunden), sollten Sie Folgendes in Betracht ziehen:
>
> - Reduzieren der Anzahl ausgewählter Objekte
> - Verwenden nicht-grafischer Methoden (API oder CLI) für den Zugriff auf Ihre Daten

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Wenn Sie Objekte verwalten möchten, gehören Sie zu einer Benutzergruppe, die über die Root-Zugriffsberechtigung verfügt. Alternativ gehören Sie zu einer Benutzergruppe, die über die Berechtigung „Registerkarte „S3-Konsole verwenden“ und entweder die Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ verfügt. Sehen "Berechtigungen zur Mandantenverwaltung" .
- Für den Benutzer wurde eine S3-Gruppen- oder Bucket-Richtlinie konfiguriert. Sehen "Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien" .
- Sie kennen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers. Optional haben Sie eine `.csv` Datei, die diese Informationen enthält. Siehe die"Anleitung zum Erstellen von Zugriffsschlüsseln" .

Schritte

1. Wählen Sie **SPEICHER** > **Buckets** > ***Bucketname***.
2. Wählen Sie die Registerkarte „S3-Konsole“ aus.
3. Fügen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Felder ein. Andernfalls wählen Sie **Zugriffsschlüssel hochladen** und wählen Sie Ihre `.csv` Datei.

4. Wählen Sie * Sign in*.
5. Die Tabelle mit den Bucket-Objekten wird angezeigt. Sie können Objekte nach Bedarf verwalten.

Weitere Informationen

- **Suche nach Präfix**: Die Präfix-Suchfunktion sucht nur nach Objekten, die relativ zum aktuellen Ordner mit einem bestimmten Wort beginnen. Die Suche umfasst keine Objekte, die das Wort an anderer Stelle enthalten. Diese Regel gilt auch für Objekte innerhalb von Ordnern. Beispielsweise eine Suche nach `folder1/folder2/somefile-` würde Objekte zurückgeben, die innerhalb der `folder1/folder2/` Ordner und beginnen Sie mit dem Wort `somefile-` .
- **Drag & Drop**: Sie können Dateien per Drag & Drop aus dem Dateimanager Ihres Computers in die S3-Konsole ziehen. Sie können jedoch keine Ordner hochladen.
- **Operationen an Ordnern**: Wenn Sie einen Ordner verschieben, kopieren oder umbenennen, werden alle Objekte im Ordner einzeln aktualisiert, was einige Zeit dauern kann.
- **Dauerhaftes Löschen bei deaktivierter Bucket-Versionierung**: Wenn Sie ein Objekt in einem Bucket mit deaktivierter Versionierung überschreiben oder löschen, ist der Vorgang dauerhaft. Sehen "Ändern der Objektversionierung für einen Bucket" .

Verwalten von S3-Plattformdiensten

S3-Plattformdienste

Übersicht und Überlegungen zu Plattformdiensten

Lesen Sie vor der Implementierung von Plattformdiensten die Übersicht und die Überlegungen zur Verwendung dieser Dienste.

Informationen zu S3 finden Sie unter"Verwenden Sie die S3 REST-API" .

Übersicht der Plattformdienste

Die StorageGRID -Plattformdienste können Ihnen bei der Implementierung einer Hybrid-Cloud-Strategie helfen, indem sie Ihnen das Senden von Ereignisbenachrichtigungen und Kopien von S3-Objekten und Objektmetadaten an externe Ziele ermöglichen.

Da sich der Zielspeicherort für Plattformdienste normalerweise außerhalb Ihrer StorageGRID Bereitstellung befindet, bieten Ihnen Plattformdienste die Leistung und Flexibilität, die Sie durch die Verwendung externer Speicherressourcen, Benachrichtigungsdienste und Such- oder Analysedienste für Ihre Daten erhalten.

Für einen einzelnen S3-Bucket kann jede beliebige Kombination von Plattformdiensten konfiguriert werden. Sie können beispielsweise sowohl die"CloudMirror-Dienst" Und"Benachrichtigungen" auf einem StorageGRID S3-Bucket, sodass Sie bestimmte Objekte auf den Amazon Simple Storage Service (S3) spiegeln können, während Sie zu jedem dieser Objekte eine Benachrichtigung an eine Überwachungsanwendung eines Drittanbieters senden, die Ihnen bei der Verfolgung Ihrer AWS-Ausgaben hilft.

Die Nutzung der Plattformdienste muss für jedes Mandantenkonto von einem StorageGRID -Administrator über den Grid Manager oder die Grid Management API aktiviert werden.

So werden Plattformdienste konfiguriert

Plattformdienste kommunizieren mit externen Endpunkten, die Sie mithilfe der"Mietermanager" oder die"Mandantenverwaltungs-API" . Jeder Endpunkt stellt ein externes Ziel dar, beispielsweise einen

StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Amazon SNS-Thema oder einen Elasticsearch-Cluster, der lokal, auf AWS oder anderswo gehostet wird.

Nachdem Sie einen externen Endpunkt erstellt haben, können Sie einen Plattformdienst für einen Bucket aktivieren, indem Sie dem Bucket eine XML-Konfiguration hinzufügen. Die XML-Konfiguration identifiziert die Objekte, auf die der Bucket einwirken soll, die Aktion, die der Bucket ausführen soll, und den Endpunkt, den der Bucket für den Dienst verwenden soll.

Sie müssen für jeden Plattformdienst, den Sie konfigurieren möchten, separate XML-Konfigurationen hinzufügen. Beispiel:

- Wenn Sie alle Objekte möchten, deren Schlüssel mit `/images` Um in einen Amazon S3-Bucket repliziert zu werden, müssen Sie dem Quell-Bucket eine Replikationskonfiguration hinzufügen.
- Wenn Sie auch Benachrichtigungen senden möchten, wenn diese Objekte im Bucket gespeichert werden, müssen Sie eine Benachrichtigungskonfiguration hinzufügen.
- Wenn Sie die Metadaten für diese Objekte indizieren möchten, müssen Sie die Metadatenbenachrichtigungskonfiguration hinzufügen, die zum Implementieren der Suchintegration verwendet wird.

Das Format für die XML-Konfiguration wird durch die S3-REST-APIs bestimmt, die zur Implementierung der StorageGRID -Plattformdienste verwendet werden:

Plattformdienst	S3 REST API	Siehe
CloudMirror-Replikation	• GetBucketReplication • PutBucketReplication	• "CloudMirror-Replikation" • "Operationen an Buckets"
Benachrichtigungen	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Benachrichtigungen" • "Operationen an Buckets"
Suchintegration	• GET Bucket-Metadaten-Benachrichtigungskonfiguration • Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten	• "Suchintegration" • "Benutzerdefinierte StorageGRID -Vorgänge"

Überlegungen zur Verwendung von Plattformdiensten

Rücksichtnahme	Details
Zielendpunktüberwachung	Sie müssen die Verfügbarkeit jedes Zielendpunkts überwachen. Wenn die Verbindung zum Zielendpunkt über einen längeren Zeitraum unterbrochen ist und ein großer Rückstand an Anfragen besteht, schlagen weitere Clientanfragen (z. B. PUT-Anfragen) an StorageGRID fehl. Sie müssen diese fehlgeschlagenen Anfragen wiederholen, wenn der Endpunkt erreichbar ist.

Rücksichtnahme	Details
Drosselung des Zielendpunkts	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.
Bestellgarantien	StorageGRID garantiert die Reihenfolge der Vorgänge an einem Objekt innerhalb einer Site. Solange alle Vorgänge für ein Objekt innerhalb derselben Site erfolgen, entspricht der endgültige Objektstatus (für die Replikation) immer dem Status in StorageGRID. StorageGRID versucht nach besten Kräften, Anfragen zu ordnen, wenn Vorgänge über StorageGRID -Sites hinweg ausgeführt werden. Wenn Sie beispielsweise ein Objekt zunächst an Standort A schreiben und dasselbe Objekt später an Standort B überschreiben, ist nicht garantiert, dass das endgültige, von CloudMirror in den Ziel-Bucket replizierte Objekt das neuere Objekt ist.
ILM-gesteuerte Objektlöschungen	Um dem Löschverhalten von AWS CRR und Amazon Simple Notification Service zu entsprechen, werden CloudMirror- und Ereignisbenachrichtigungsanforderungen nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID ILM-Regeln gelöscht wird. Beispielsweise werden keine CloudMirror- oder Ereignisbenachrichtigungsanforderungen gesendet, wenn eine ILM-Regel ein Objekt nach 14 Tagen löscht. Im Gegensatz dazu werden Suchintegrationsanforderungen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.

Rücksichtnahme	Details
Verwenden von Kafka-Endpunkten	Für Kafka-Endpunkte wird Mutual TLS nicht unterstützt. Wenn Sie also `ssl.client.auth` eingestellt auf `required` in Ihrer Kafka-Broker-Konfiguration kann es zu Problemen bei der Kafka-Endpunktkonfiguration kommen. Die Authentifizierung von Kafka-Endpunkten verwendet die folgenden Authentifizierungstypen. Diese Typen unterscheiden sich von denen, die für die Authentifizierung anderer Endpunkte wie Amazon SNS verwendet werden, und erfordern Anmeldeinformationen mit Benutzername und Kennwort. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Hinweis:** Konfigurierte Speicherproxyeinstellungen gelten nicht für Endpunkte der Kafka-Plattformdienste.

Überlegungen zur Verwendung des CloudMirror-Replikationsdienstes

Rücksichtnahme	Details
Replikationsstatus	StorageGRID unterstützt nicht die `x-amz-replication-status` Kopfzeile.
Objektgröße	Die maximale Größe für Objekte, die vom CloudMirror-Replikationsdienst in einen Ziel-Bucket repliziert werden können, beträgt 5 TiB, was der maximal *unterstützten* Objektgröße entspricht. **Hinweis**: Die maximal *empfohlene* Größe für einen einzelnen PutObject-Vorgang beträgt 5 GiB (5.368.709.120 Bytes). Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie stattdessen den mehrteiligen Upload.
Bucket-Versionierung und Versions-IDs	Wenn für den Quell-S3-Bucket in StorageGRID die Versionierung aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren. Beachten Sie bei der Verwendung der Versionierung, dass die Reihenfolge der Objektversionen im Ziel-Bucket nach bestem Wissen und Gewissen erfolgt und aufgrund von Einschränkungen im S3-Protokoll nicht vom CloudMirror-Dienst garantiert wird. **Hinweis**: Versions-IDs für den Quell-Bucket in StorageGRID stehen in keinem Zusammenhang mit den Versions-IDs für den Ziel-Bucket.

Rücksichtnahme	Details
Tagging für Objektversionen	Aufgrund von Einschränkungen im S3-Protokoll repliziert der CloudMirror-Dienst keine PutObjectTagging- oder DeleteObjectTagging-Anfragen, die eine Versions-ID bereitstellen. Da die Versions-IDs für Quelle und Ziel nicht miteinander verknüpft sind, kann nicht sichergestellt werden, dass eine Tag-Aktualisierung auf eine bestimmte Versions-ID repliziert wird. Im Gegensatz dazu repliziert der CloudMirror-Dienst PutObjectTagging-Anfragen oder DeleteObjectTagging-Anfragen, die keine Versions-ID angeben. Diese Anfragen aktualisieren die Tags für den neuesten Schlüssel (oder die neueste Version, wenn der Bucket versioniert ist). Normale Aufnahmen mit Tags (keine Tagging-Updates) werden ebenfalls repliziert.
Mehrteilige Uploads und `ETag` Werte	Beim Spiegeln von Objekten, die mit einem mehrteiligen Upload hochgeladen wurden, behält der CloudMirror-Dienst die Teile nicht bei. Infolgedessen `ETag` Wert für das gespiegelte Objekt wird anders sein als der `ETag` Wert des ursprünglichen Objekts.
Mit SSE-C verschlüsselte Objekte (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)	Der CloudMirror-Dienst unterstützt keine mit SSE-C verschlüsselten Objekte. Wenn Sie versuchen, ein Objekt in den Quell-Bucket für die CloudMirror-Replikation aufzunehmen und die Anforderung die SSE-C-Anforderungsheader enthält, schlägt der Vorgang fehl.
Bucket mit aktivierter S3-Objektsperre	Die Replikation wird für Quell- oder Ziel-Buckets mit aktivierter S3-Objektsperre nicht unterstützt.

Grundlegendes zum CloudMirror-Replikationsdienst

Sie können die CloudMirror-Replikation für einen S3-Bucket aktivieren, wenn StorageGRID bestimmte, dem Bucket hinzugefügte Objekte in einen oder mehrere externe Ziel-Buckets repliziert.

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 wird nicht unterstützt, wenn im Quell-Bucket S3 Object Lock aktiviert ist.

CloudMirror und ILM

Die CloudMirror-Replikation funktioniert unabhängig von den aktiven ILM-Richtlinien des Grids. Der CloudMirror-Dienst repliziert Objekte, sobald sie im Quell-Bucket gespeichert sind, und liefert sie so schnell wie möglich an den Ziel-Bucket. Die Bereitstellung replizierter Objekte wird ausgelöst, wenn die Objektaufnahme erfolgreich ist.

CloudMirror und Cross-Grid-Replikation

Die CloudMirror-Replikation weist wichtige Ähnlichkeiten und Unterschiede zur Cross-Grid-Replikationsfunktion auf. Weitere Informationen finden Sie unter "Vergleichen Sie Cross-Grid-Replikation und

CloudMirror-Replikation" .

CloudMirror und S3-Buckets

Die CloudMirror-Replikation ist normalerweise so konfiguriert, dass ein externer S3-Bucket als Ziel verwendet wird. Sie können die Replikation jedoch auch so konfigurieren, dass eine andere StorageGRID Bereitstellung oder ein beliebiger S3-kompatibler Dienst verwendet wird.

Vorhandene Eimer

Wenn Sie die CloudMirror-Replikation für einen vorhandenen Bucket aktivieren, werden nur die neuen Objekte repliziert, die diesem Bucket hinzugefügt werden. Alle vorhandenen Objekte im Bucket werden nicht repliziert. Um die Replikation vorhandener Objekte zu erzwingen, können Sie die Metadaten des vorhandenen Objekts aktualisieren, indem Sie eine Objektkopie durchführen.

> ⓘ Wenn Sie die CloudMirror-Replikation zum Kopieren von Objekten an ein Amazon S3-Ziel verwenden, beachten Sie, dass Amazon S3 die Größe benutzerdefinierter Metadaten in jedem PUT-Anforderungsheader auf 2 KB begrenzt. Wenn ein Objekt benutzerdefinierte Metadaten größer als 2 KB hat, wird dieses Objekt nicht repliziert.

Mehrere Ziel-Buckets

Um Objekte in einem einzelnen Bucket in mehrere Ziel-Buckets zu replizieren, geben Sie das Ziel für jede Regel in der XML-Replikationskonfiguration an. Sie können ein Objekt nicht gleichzeitig in mehr als einen Bucket replizieren.

Versionierte oder nicht versionierte Buckets

Sie können die CloudMirror-Replikation auf versionierten oder nicht versionierten Buckets konfigurieren. Die Ziel-Buckets können versioniert oder nicht versioniert sein. Sie können jede beliebige Kombination aus versionierten und nicht versionierten Buckets verwenden. Sie können beispielsweise einen versionierten Bucket als Ziel für einen nicht versionierten Quell-Bucket angeben oder umgekehrt. Sie können auch zwischen Buckets ohne Versionsnummer replizieren.

Löschung, Replikationsschleifen und Ereignisse

Löschverhalten

Entspricht dem Löschverhalten des Amazon S3-Dienstes Cross-Region Replication (CRR). Durch das Löschen eines Objekts in einem Quell-Bucket wird niemals ein repliziertes Objekt im Ziel gelöscht. Wenn sowohl Quell- als auch Ziel-Buckets versioniert sind, wird die Löschmarkierung repliziert. Wenn der Ziel-Bucket nicht versioniert ist, wird beim Löschen eines Objekts im Quell-Bucket weder die Löschmarkierung in den Ziel-Bucket repliziert noch das Zielobjekt gelöscht.

Schutz vor Replikationsschleifen

Wenn Objekte in den Ziel-Bucket repliziert werden, markiert StorageGRID sie als „Replikate“. Ein StorageGRID Ziel-Bucket repliziert als Replikate markierte Objekte nicht erneut und schützt Sie so vor versehentlichen Replikationsschleifen. Diese Replikatmarkierung erfolgt intern für StorageGRID und hindert Sie nicht daran, AWS CRR zu nutzen, wenn Sie einen Amazon S3-Bucket als Ziel verwenden.

> ⓘ Der benutzerdefinierte Header, der zum Markieren einer Replik verwendet wird, ist `x-ntap-sg-replica` . Diese Markierung verhindert einen Kaskadenspiegel. StorageGRID unterstützt einen bidirektionalen CloudMirror zwischen zwei Grids.

Ereignisse im Ziel-Bucket

Die Eindeutigkeit und Reihenfolge der Ereignisse im Ziel-Bucket sind nicht garantiert. Aufgrund von Vorgängen, die zur Gewährleistung einer erfolgreichen Zustellung durchgeführt werden, kann es vorkommen, dass mehrere identische Kopien eines Quellobjekts an das Ziel übermittelt werden. In seltenen Fällen, wenn dasselbe Objekt gleichzeitig von zwei oder mehr verschiedenen StorageGRID Sites aktualisiert wird, stimmt die Reihenfolge der Vorgänge im Ziel-Bucket möglicherweise nicht mit der Reihenfolge der Ereignisse im Quell-Bucket überein.

Benachrichtigungen für Buckets verstehen

Sie können die Ereignisbenachrichtigung für einen S3-Bucket aktivieren, wenn StorageGRID Benachrichtigungen über bestimmte Ereignisse an einen Kafka-Zielcluster oder Amazon Simple Notification Service senden soll.

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.

Ereignisbenachrichtigungen werden im Quell-Bucket wie in der Benachrichtigungskonfiguration angegeben erstellt und an das Ziel übermittelt. Wenn ein mit einem Objekt verknüpftes Ereignis erfolgreich ist, wird eine Benachrichtigung über dieses Ereignis erstellt und zur Übermittlung in die Warteschlange gestellt.

Die Eindeutigkeit und Reihenfolge der Benachrichtigungen sind nicht garantiert. Aufgrund von Vorgängen, die zur Gewährleistung einer erfolgreichen Zustellung durchgeführt werden, kann es sein, dass mehrere Benachrichtigungen zu einem Ereignis an das Ziel übermittelt werden. Und da die Übermittlung asynchron erfolgt, kann nicht garantiert werden, dass die zeitliche Reihenfolge der Benachrichtigungen am Ziel mit der Reihenfolge der Ereignisse im Quell-Bucket übereinstimmt, insbesondere bei Vorgängen, die von verschiedenen StorageGRID Sites stammen. Sie können die `sequencer` Geben Sie in der Ereignisnachricht den Schlüssel ein, um die Reihenfolge der Ereignisse für ein bestimmtes Objekt zu bestimmen, wie in der Amazon S3-Dokumentation beschrieben.

StorageGRID Ereignisbenachrichtigungen folgen mit einigen Einschränkungen der Amazon S3-API.

- Die folgenden Ereignistypen werden unterstützt:
  - s3:Objekt erstellt:
  - s3:ObjektErstellt:Put
  - s3:ObjektErstellt:Post
  - s3:ObjektErstellt:Kopie
  - s3:Objekterstellt:MehrteiligerUpload abgeschlossen
  - s3:Objekt entfernt:
  - s3:Objekt entfernt:Löschen
  - s3:Objekt entfernt:DeleteMarker erstellt
  - s3:ObjectRestore:Post
- Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das standardmäßige JSON-Format, enthalten jedoch einige Schlüssel nicht und verwenden für andere bestimmte Werte, wie in der Tabelle gezeigt:

Schlüsselname	StorageGRID -Wert
Ereignisquelle	`sgws:s3`
awsRegion	*nicht enthalten*
x-amz-id-2	*nicht enthalten*
arn	`urn:sgws:s3:::bucket_name`

Verstehen Sie den Suchintegrationsdienst

Sie können die Suchintegration für einen S3-Bucket aktivieren, wenn Sie einen externen Such- und Datenanalysedienst für Ihre Objektmetadaten verwenden möchten.

Der Suchintegrationsdienst ist ein benutzerdefinierter StorageGRID Dienst, der automatisch und asynchron S3-Objektmetadaten an einen Zielendpunkt sendet, wenn ein Objekt erstellt oder gelöscht wird oder seine Metadaten oder Tags aktualisiert werden. Sie können dann die vom Zieldienst bereitgestellten ausgefeilten Such-, Datenanalyse-, Visualisierungs- oder maschinellen Lerntools verwenden, um Ihre Objektdaten zu durchsuchen, zu analysieren und Erkenntnisse daraus zu gewinnen.

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-Objektsperre konfiguriert werden kann, werden die S3-Objektsperre-Metadaten (einschließlich „Aufbewahrungsdatum“ und „Legal Hold“-Status) der Objekte nicht in die an Elasticsearch gesendeten Metadaten aufgenommen.

> ⓘ Da der Suchintegrationsdienst das Senden von Objektmetadaten an ein Ziel veranlasst, wird sein Konfigurations-XML als „*Metadaten*-Benachrichtigungskonfigurations-XML“ bezeichnet. Dieses Konfigurations-XML unterscheidet sich vom „Benachrichtigungskonfigurations-XML“, das zum Aktivieren von *Ereignis*-Benachrichtigungen verwendet wird.

Suchintegration und S3-Buckets

Sie können den Suchintegrationsdienst für jeden versionierten oder nicht versionierten Bucket aktivieren. Die Suchintegration wird konfiguriert, indem die XML-Konfigurationsdatei für Metadatenbenachrichtigungen mit dem Bucket verknüpft wird, der angibt, auf welche Objekte reagiert werden soll und das Ziel für die Objektmetadaten ist.

Metadatenbenachrichtigungen werden in Form eines JSON-Dokuments generiert, das den Bucket-Namen, den Objektnamen und die Versions-ID (sofern vorhanden) enthält. Jede Metadatenbenachrichtigung enthält zusätzlich zu allen Tags und Benutzermetadaten des Objekts einen Standardsatz von Systemmetadaten für das Objekt.

Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur Zuordnung von Datumsformaten. Sie müssen die dynamischen Feldzuordnungen im Index aktivieren, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Suchbenachrichtigungen

Metadatenbenachrichtigungen werden generiert und zur Zustellung in die Warteschlange gestellt, wenn:

- Ein Objekt wird erstellt.
- Ein Objekt wird gelöscht, auch wenn Objekte aufgrund der Ausführung der ILM-Richtlinie des Grids gelöscht werden.
- Objektmetadaten oder Tags werden hinzugefügt, aktualisiert oder gelöscht. Beim Update wird immer der komplette Satz an Metadaten und Tags gesendet – nicht nur die geänderten Werte.

Nachdem Sie einem Bucket XML-Metadatenbenachrichtigungskonfigurations-XML hinzugefügt haben, werden Benachrichtigungen für alle neuen Objekte gesendet, die Sie erstellen, und für alle Objekte, die Sie durch Aktualisieren der Daten, Benutzermetadaten oder Tags ändern. Es werden jedoch keine Benachrichtigungen für Objekte gesendet, die sich bereits im Bucket befanden. Um sicherzustellen, dass die Objektmetadaten für alle Objekte im Bucket an das Ziel gesendet werden, sollten Sie einen der folgenden Schritte ausführen:

- Konfigurieren Sie den Suchintegrationsdienst unmittelbar nach dem Erstellen des Buckets und vor dem Hinzufügen von Objekten.
- Führen Sie für alle Objekte, die sich bereits im Bucket befinden, eine Aktion aus, die das Senden einer Metadatenbenachrichtigung an das Ziel auslöst.

Suchintegrationsdienst und Elasticsearch

Der Suchintegrationsdienst StorageGRID unterstützt einen Elasticsearch-Cluster als Ziel. Wie bei den anderen Plattformdiensten wird das Ziel im Endpunkt angegeben, dessen URN im Konfigurations-XML für den Dienst verwendet wird. Verwenden Sie die "NetApp Interoperabilitätsmatrix-Tool" um die unterstützten Versionen von Elasticsearch zu ermitteln.

Verwalten von Plattformdienst-Endpunkten

Konfigurieren von Plattformdienstendpunkten

Bevor Sie einen Plattformdienst für einen Bucket konfigurieren können, müssen Sie mindestens einen Endpunkt als Ziel für den Plattformdienst konfigurieren.

Der Zugriff auf Plattformdienste wird pro Mandant von einem StorageGRID -Administrator aktiviert. Um einen Plattformdienst-Endpunkt zu erstellen oder zu verwenden, müssen Sie ein Mandantenbenutzer mit der Berechtigung „Endpunkte verwalten“ oder „Root-Zugriff“ in einem Grid sein, dessen Netzwerk so konfiguriert wurde, dass Speicherknoten auf externe Endpunktressourcen zugreifen können. Für einen einzelnen Mandanten können Sie maximal 500 Plattformdienst-Endpunkte konfigurieren. Wenden Sie sich für weitere Informationen an Ihren StorageGRID Administrator.

Was ist ein Plattformdienst-Endpunkt?

Ein Plattformdienst-Endpunkt gibt die Informationen an, die StorageGRID für den Zugriff auf das externe Ziel benötigt.

Wenn Sie beispielsweise Objekte aus einem StorageGRID Bucket in einen Amazon S3-Bucket replizieren möchten, erstellen Sie einen Plattformdienst-Endpunkt, der die Informationen und Anmeldeinformationen enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket bei Amazon benötigt.

Jeder Plattformdiensttyp erfordert einen eigenen Endpunkt. Sie müssen daher für jeden Plattformdienst, den Sie verwenden möchten, mindestens einen Endpunkt konfigurieren. Nachdem Sie einen Plattformdienst-Endpunkt definiert haben, verwenden Sie die URN des Endpunkts als Ziel in der Konfigurations-XML, die zum Aktivieren des Dienstes verwendet wird.

Sie können denselben Endpunkt als Ziel für mehr als einen Quell-Bucket verwenden. Sie können beispielsweise mehrere Quell-Buckets so konfigurieren, dass sie Objektmetadaten an denselben Suchintegrationsendpunkt senden, sodass Sie Suchvorgänge über mehrere Buckets hinweg durchführen können. Sie können einen Quell-Bucket auch so konfigurieren, dass er mehr als einen Endpunkt als Ziel verwendet. Dadurch können Sie beispielsweise Benachrichtigungen über die Objekterstellung an ein Amazon Simple Notification Service (Amazon SNS)-Thema und Benachrichtigungen über die Objektlöschung an ein zweites Amazon SNS-Thema senden.

Endpunkte für die CloudMirror-Replikation

StorageGRID unterstützt Replikationsendpunkte, die S3-Buckets darstellen. Diese Buckets können auf Amazon Web Services, derselben oder einer Remote- StorageGRID Bereitstellung oder einem anderen Dienst gehostet werden.

Endpunkte für Benachrichtigungen

StorageGRID unterstützt Amazon SNS- und Kafka-Endpunkte. Simple Queue Service (SQS) oder AWS Lambda-Endpunkte werden nicht unterstützt.

Für Kafka-Endpunkte wird Mutual TLS nicht unterstützt. Wenn Sie also `ssl.client.auth` eingestellt auf `required` in Ihrer Kafka-Broker-Konfiguration kann es zu Problemen bei der Kafka-Endpunktkonfiguration kommen.

Endpunkte für den Suchintegrationsdienst

StorageGRID unterstützt Suchintegrationsendpunkte, die Elasticsearch-Cluster darstellen. Diese Elasticsearch-Cluster können sich in einem lokalen Rechenzentrum befinden oder in einer AWS-Cloud oder anderswo gehostet werden.

Der Endpunkt der Suchintegration bezieht sich auf einen bestimmten Elasticsearch-Index und -Typ. Sie müssen den Index in Elasticsearch erstellen, bevor Sie den Endpunkt in StorageGRID erstellen, sonst schlägt die Endpunkterstellung fehl. Sie müssen den Typ nicht erstellen, bevor Sie den Endpunkt erstellen. StorageGRID erstellt den Typ bei Bedarf, wenn es Objektmetadaten an den Endpunkt sendet.

Ähnliche Informationen

"StorageGRID verwalten"

Geben Sie die URN für den Plattformdienst-Endpunkt an

Wenn Sie einen Plattformdienste-Endpunkt erstellen, müssen Sie einen eindeutigen

Ressourcennamen (URN) angeben. Sie verwenden die URN, um auf den Endpunkt zu verweisen, wenn Sie eine XML-Konfiguration für den Plattformdienst erstellen. Die URN für jeden Endpunkt muss eindeutig sein.

StorageGRID validiert die Endpunkte der Plattformdienste, während Sie sie erstellen. Bevor Sie einen Plattformdienste-Endpunkt erstellen, bestätigen Sie, dass die im Endpunkt angegebene Ressource vorhanden und erreichbar ist.

URN-Elemente

Die URN für einen Plattformdienst-Endpunkt muss mit einem der folgenden Zeichen beginnen: `arn:aws` oder `urn:mysite` , wie folgt:

- Wenn der Dienst auf Amazon Web Services (AWS) gehostet wird, verwenden Sie `arn:aws`
- Wenn der Dienst auf der Google Cloud Platform (GCP) gehostet wird, verwenden Sie `arn:aws`
- Wenn der Dienst lokal gehostet wird, verwenden Sie `urn:mysite`

Wenn Sie beispielsweise die URN für einen CloudMirror-Endpunkt angeben, der auf StorageGRID gehostet wird, könnte die URN mit beginnen `urn:sgws` .

Das nächste Element der URN gibt den Typ des Plattformdienstes wie folgt an:

Service	Typ
CloudMirror-Replikation	`s3`
Benachrichtigungen	`sns`oder `kafka`
Suchintegration	`es`

Um beispielsweise weiterhin die URN für einen CloudMirror-Endpunkt anzugeben, der auf StorageGRID gehostet wird, würden Sie hinzufügen `s3` zu bekommen `urn:sgws:s3` .

Das letzte Element der URN identifiziert die spezifische Zielressource an der Ziel-URI.

Service	Spezifische Ressource
CloudMirror-Replikation	`bucket-name`
Benachrichtigungen	`sns-topic-name`oder `kafka-topic-name`
Suchintegration	`domain-name/index-name/type-name` **Hinweis:** Wenn der Elasticsearch-Cluster **nicht** für die automatische Erstellung von Indizes konfiguriert ist, müssen Sie den Index manuell erstellen, bevor Sie den Endpunkt erstellen.

URNs für auf AWS und GCP gehostete Dienste

Für AWS- und GCP-Entitäten ist die vollständige URN eine gültige AWS-ARN. Beispiel:

- CloudMirror-Replikation:

```
arn:aws:s3:::bucket-name
```

- Benachrichtigungen:

```
arn:aws:sns:region:account-id:topic-name
```

- Suchintegration:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> Für einen AWS-Suchintegrationsendpunkt ist der `domain-name` muss die Literalzeichenfolge enthalten `domain/` , wie hier gezeigt.

URNs für lokal gehostete Dienste

Wenn Sie lokal gehostete Dienste anstelle von Cloud-Diensten verwenden, können Sie die URN auf jede beliebige Weise angeben, die eine gültige und eindeutige URN erstellt, solange die URN die erforderlichen Elemente an der dritten und letzten Stelle enthält. Sie können die optional angegebenen Elemente leer lassen oder sie auf eine beliebige Weise angeben, die Ihnen bei der Identifizierung der Ressource hilft und die URN eindeutig macht. Beispiel:

- CloudMirror-Replikation:

```
urn:mysite:s3:optional:optional:bucket-name
```

  Für einen CloudMirror-Endpunkt, der auf StorageGRID gehostet wird, können Sie eine gültige URN angeben, die mit beginnt `urn:sgws` :

```
urn:sgws:s3:optional:optional:bucket-name
```

- Benachrichtigungen:

  Geben Sie einen Amazon Simple Notification Service-Endpunkt an:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

  Geben Sie einen Kafka-Endpunkt an:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- Suchintegration:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> Für lokal gehostete Suchintegrationsendpunkte gilt: `domain-name` Das Element kann eine beliebige Zeichenfolge sein, solange die URN des Endpunkts eindeutig ist.

Plattformdienst-Endpunkt erstellen

Sie müssen mindestens einen Endpunkt des richtigen Typs erstellen, bevor Sie einen Plattformdienst aktivieren können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .
- Die vom Plattformdienst-Endpunkt referenzierte Ressource wurde erstellt:
  - CloudMirror-Replikation: S3-Bucket
  - Ereignisbenachrichtigung: Amazon Simple Notification Service (Amazon SNS) oder Kafka-Thema
  - Suchbenachrichtigung: Elasticsearch-Index, wenn der Zielcluster nicht für die automatische Erstellung von Indizes konfiguriert ist.
- Sie verfügen über die Informationen zur Zielressource:
  - Host und Port für den Uniform Resource Identifier (URI)

    > Wenn Sie einen auf einem StorageGRID -System gehosteten Bucket als Endpunkt für die CloudMirror-Replikation verwenden möchten, wenden Sie sich an den Grid-Administrator, um die einzugebenden Werte zu ermitteln.

  - Eindeutiger Ressourcenname (URN)

    "Geben Sie die URN für den Plattformdienst-Endpunkt an"

  - Authentifizierungsdaten (falls erforderlich):

Suchintegrationsendpunkte

Für Suchintegrationsendpunkte können Sie die folgenden Anmeldeinformationen verwenden:

- Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
- Grundlegendes HTTP: Benutzername und Passwort

CloudMirror-Replikationsendpunkte

Für CloudMirror-Replikationsendpunkte können Sie die folgenden Anmeldeinformationen verwenden:

- Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
- CAP (C2S Access Portal): URL für temporäre Anmeldeinformationen, Server- und Client-Zertifikate, Client-Schlüssel und eine optionale Passphrase für den privaten Client-Schlüssel.

Amazon SNS-Endpunkte

Für Amazon SNS-Endpunkte können Sie die folgenden Anmeldeinformationen verwenden:

- Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel

Kafka-Endpunkte

Für Kafka-Endpunkte können Sie die folgenden Anmeldeinformationen verwenden:

- SASL/PLAIN: Benutzername und Passwort
- SASL/SCRAM-SHA-256: Benutzername und Passwort
- SASL/SCRAM-SHA-512: Benutzername und Passwort

    - Sicherheitszertifikat (bei Verwendung eines benutzerdefinierten CA-Zertifikats)

- Wenn die Elasticsearch-Sicherheitsfunktionen aktiviert sind, verfügen Sie über die Berechtigung zum Überwachen des Clusters für Konnektivitätstests und entweder über die Berechtigung zum Schreiben des Index oder über die Berechtigung zum Indexieren und Löschen des Index für Dokumentaktualisierungen.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**. Die Seite „Plattformdienst-Endpunkte“ wird angezeigt.
2. Wählen Sie **Endpunkt erstellen**.
3. Geben Sie einen Anzeigenamen ein, um den Endpunkt und seinen Zweck kurz zu beschreiben.

   Der Typ des Plattformdienstes, den der Endpunkt unterstützt, wird neben dem Endpunktnamen angezeigt, wenn dieser auf der Seite „Endpunkte“ aufgeführt ist. Sie müssen diese Information also nicht in den Namen aufnehmen.

4. Geben Sie im Feld **URI** den Unique Resource Identifier (URI) des Endpunkts an.

   Verwenden Sie eines der folgenden Formate:

```
https://host:port
http://host:port
```

Wenn Sie keinen Port angeben, werden die folgenden Standardports verwendet:

- Port 443 für HTTPS-URIs und Port 80 für HTTP-URIs (die meisten Endpunkte)
- Port 9092 für HTTPS und HTTP-URIs (nur Kafka-Endpunkte)

Beispielsweise könnte die URI für einen auf StorageGRID gehosteten Bucket wie folgt lauten:

```
https://s3.example.com:10443
```

In diesem Beispiel `s3.example.com` stellt den DNS-Eintrag für die virtuelle IP (VIP) der StorageGRID Hochverfügbarkeitsgruppe (HA) dar und `10443` stellt den im Load Balancer-Endpunkt definierten Port dar.

> Wenn möglich, sollten Sie eine Verbindung zu einer HA-Gruppe von Lastausgleichsknoten herstellen, um einen einzelnen Fehlerpunkt zu vermeiden.

Ähnlich könnte die URI für einen auf AWS gehosteten Bucket lauten:

```
https://s3-aws-region.amazonaws.com
```

> Wenn der Endpunkt für den CloudMirror-Replikationsdienst verwendet wird, schließen Sie den Bucket-Namen nicht in die URI ein. Sie geben den Bucket-Namen in das Feld **URN** ein.

5. Geben Sie den eindeutigen Ressourcennamen (URN) für den Endpunkt ein.

> Sie können die URN eines Endpunkts nicht mehr ändern, nachdem der Endpunkt erstellt wurde.

6. Wählen Sie **Weiter**.
7. Wählen Sie einen Wert für **Authentifizierungstyp**.

Suchintegrationsendpunkte

Geben Sie die Anmeldeinformationen für einen Suchintegrationsendpunkt ein oder laden Sie sie hoch.

Die von Ihnen angegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
Grundlegendes HTTP	Verwendet einen Benutzernamen und ein Kennwort, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort

CloudMirror-Replikationsendpunkte

Geben Sie die Anmeldeinformationen für einen CloudMirror-Replikationsendpunkt ein oder laden Sie sie hoch.

Die von Ihnen angegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
CAP (C2S-Zugangsportal)	Verwendet Zertifikate und Schlüssel, um Verbindungen zum Ziel zu authentifizieren.	• URL für temporäre Anmeldeinformationen • Server-CA-Zertifikat (PEM-Datei-Upload) • Client-Zertifikat (PEM-Datei-Upload) • Privater Clientschlüssel (PEM-Dateiupload, verschlüsseltes OpenSSL-Format oder unverschlüsseltes privates Schlüsselformat) • Passphrase für den privaten Clientschlüssel (optional)

Amazon SNS-Endpunkte

Geben Sie die Anmeldeinformationen für einen Amazon SNS-Endpunkt ein oder laden Sie sie hoch.

Die von Ihnen angegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

Kafka-Endpunkte

Geben Sie die Anmeldeinformationen für einen Kafka-Endpunkt ein oder laden Sie sie hoch.

Die von Ihnen angegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
SASL/PLAIN	Verwendet einen Benutzernamen und ein Kennwort im Klartext, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort
SASL/SCRAM-SHA-256	Verwendet einen Benutzernamen und ein Kennwort unter Verwendung eines Challenge-Response-Protokolls und SHA-256-Hashing, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort
SASL/SCRAM-SHA-512	Verwendet einen Benutzernamen und ein Kennwort unter Verwendung eines Challenge-Response-Protokolls und SHA-512-Hashing, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort

Wählen Sie **Authentifizierung über Delegation verwenden**, wenn Benutzername und Kennwort von einem Delegationstoken abgeleitet sind, das von einem Kafka-Cluster abgerufen wurde.

8. Wählen Sie **Weiter**.
9. Wählen Sie ein Optionsfeld für **Server überprüfen** aus, um auszuwählen, wie die TLS-Verbindung zum Endpunkt überprüft wird.

Art der Zertifikatsprüfung	Beschreibung
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.
CA-Zertifikat des Betriebssystems verwenden	Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
Zertifikat nicht überprüfen	Das für die TLS-Verbindung verwendete Zertifikat wird nicht überprüft. Diese Option ist nicht sicher.

10. Wählen Sie **Endpunkt testen und erstellen**.
    - Wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann, wird eine Erfolgsmeldung angezeigt. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.
    - Wenn die Endpunktvalidierung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn Sie den Endpunkt ändern müssen, um den Fehler zu beheben, wählen Sie **Zurück zu den Endpunktdetails** und aktualisieren Sie die Informationen. Wählen Sie dann **Testen und Endpunkt erstellen**.

Die Endpunkterstellung schlägt fehl, wenn Plattformdienste für Ihr Mandantenkonto nicht aktiviert sind. Wenden Sie sich an Ihren StorageGRID Administrator.

Nachdem Sie einen Endpunkt konfiguriert haben, können Sie dessen URN verwenden, um einen Plattformdienst zu konfigurieren.

Ähnliche Informationen

- "Geben Sie die URN für den Plattformdienst-Endpunkt an"
- "Konfigurieren der CloudMirror-Replikation"
- "Konfigurieren von Ereignisbenachrichtigungen"
- "Suchintegrationsdienst konfigurieren"

Testen Sie die Verbindung für den Plattformdienst-Endpunkt

Wenn sich die Verbindung zu einem Plattformdienst geändert hat, können Sie die Verbindung für den Endpunkt testen, um zu überprüfen, ob die Zielressource vorhanden ist und mit den von Ihnen angegebenen Anmeldeinformationen erreicht werden kann.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

StorageGRID überprüft nicht, ob die Anmeldeinformationen über die richtigen Berechtigungen verfügen.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**.

   Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

2. Wählen Sie den Endpunkt aus, dessen Verbindung Sie testen möchten.

   Die Seite mit den Endpunktdetails wird angezeigt.

3. Wählen Sie **Verbindung testen**.
   - Wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann, wird eine Erfolgsmeldung angezeigt. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.
   - Wenn die Endpunktvalidierung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn Sie den Endpunkt ändern müssen, um den Fehler zu beheben, wählen Sie **Konfiguration** und aktualisieren Sie die Informationen. Wählen Sie dann **Testen und Änderungen speichern**.

Plattformdienst-Endpunkt bearbeiten

Sie können die Konfiguration für einen Plattformdienst-Endpunkt bearbeiten, um dessen Namen, URI oder andere Details zu ändern. Beispielsweise müssen Sie möglicherweise abgelaufene Anmeldeinformationen aktualisieren oder die URI ändern, damit sie für das

Failover auf einen Backup-Elasticsearch-Index verweist. Sie können die URN für einen Plattformdienst-Endpunkt nicht ändern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**.

   Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

2. Wählen Sie den Endpunkt aus, den Sie bearbeiten möchten.

   Die Seite mit den Endpunktdetails wird angezeigt.

3. Wählen Sie **Konfiguration**.
4. Ändern Sie bei Bedarf die Konfiguration des Endpunkts.

   Sie können die URN eines Endpunkts nicht mehr ändern, nachdem der Endpunkt erstellt wurde.

   a. Um den Anzeigenamen für den Endpunkt zu ändern, wählen Sie das Bearbeitungssymbol .
   b. Ändern Sie die URI nach Bedarf.
   c. Ändern Sie bei Bedarf den Authentifizierungstyp.
      - Ändern Sie für die Zugriffsschlüsselauthentifizierung den Schlüssel nach Bedarf, indem Sie **S3-Schlüssel bearbeiten** auswählen und eine neue Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel einfügen. Wenn Sie Ihre Änderungen abbrechen müssen, wählen Sie **S3-Schlüsselbearbeitung rückgängig machen**.
      - Ändern Sie für die CAP-Authentifizierung (C2S Access Portal) die URL der temporären Anmeldeinformationen oder die optionale Passphrase für den privaten Clientschlüssel und laden Sie bei Bedarf neue Zertifikats- und Schlüsseldateien hoch.

        Der private Schlüssel des Clients muss im verschlüsselten OpenSSL-Format oder im unverschlüsselten privaten Schlüsselformat vorliegen.

   d. Ändern Sie bei Bedarf die Methode zur Überprüfung des Servers.
5. Wählen Sie **Testen und Änderungen speichern**.
   - Wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann, wird eine Erfolgsmeldung angezeigt. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort überprüft.
   - Wenn die Endpunktvalidierung fehlschlägt, wird eine Fehlermeldung angezeigt. Ändern Sie den Endpunkt, um den Fehler zu beheben, und wählen Sie dann **Testen und Änderungen speichern** aus.

Plattformdienst-Endpunkt löschen

Sie können einen Endpunkt löschen, wenn Sie den zugehörigen Plattformdienst nicht

mehr verwenden möchten.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**.

   Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

2. Aktivieren Sie das Kontrollkästchen für jeden Endpunkt, den Sie löschen möchten.

   Wenn Sie einen verwendeten Plattformdienst-Endpunkt löschen, wird der zugehörige Plattformdienst für alle Buckets deaktiviert, die den Endpunkt verwenden. Alle noch nicht abgeschlossenen Anfragen werden gelöscht. Alle neuen Anfragen werden weiterhin generiert, bis Sie Ihre Bucket-Konfiguration so ändern, dass sie nicht mehr auf die gelöschte URN verweist. StorageGRID meldet diese Anfragen als nicht behebbare Fehler.

3. Wählen Sie **Aktionen** > **Endpunkt löschen**.

   Es wird eine Bestätigungsmeldung angezeigt.

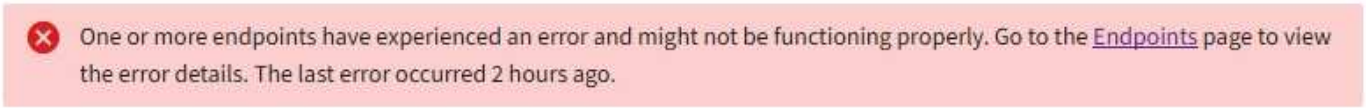
4. Wählen Sie **Endpunkt löschen**.

Beheben von Fehlern bei Plattformdienst-Endpunkten

Wenn beim Versuch von StorageGRID , mit einem Plattformdienst-Endpunkt zu kommunizieren, ein Fehler auftritt, wird auf dem Dashboard eine Meldung angezeigt. Auf der Seite „Plattformdienst-Endpunkte“ gibt die Spalte „Letzter Fehler“ an, wie lange der Fehler her ist. Es wird kein Fehler angezeigt, wenn die mit den Anmeldeinformationen eines Endpunkts verknüpften Berechtigungen falsch sind.

Feststellen, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Fehler am Endpunkt der Plattformdienste aufgetreten sind, wird im Tenant Manager-Dashboard eine Warnmeldung angezeigt. Weitere Einzelheiten zum Fehler finden Sie auf der Seite „Plattformdienst-Endpunkte“.



Derselbe Fehler, der auf dem Dashboard angezeigt wird, erscheint auch oben auf der Seite „Plattformdienst-Endpunkte“. So zeigen Sie eine ausführlichere Fehlermeldung an:

Schritte

1. Wählen Sie aus der Liste der Endpunkte den Endpunkt aus, bei dem der Fehler auftritt.
2. Wählen Sie auf der Seite mit den Endpunktdetails **Verbindung** aus. Auf dieser Registerkarte wird nur der

letzte Fehler für einen Endpunkt angezeigt und es wird angegeben, wie lange der Fehler her ist. Fehler, die das rote X-Symbol enthalten  innerhalb der letzten 7 Tage aufgetreten ist.

Prüfen, ob der Fehler noch aktuell ist

Einige Fehler werden möglicherweise auch nach ihrer Behebung weiterhin in der Spalte **Letzter Fehler** angezeigt. So können Sie feststellen, ob ein Fehler aktuell ist, oder das Entfernen eines behobenen Fehlers aus der Tabelle erzwingen:

Schritte

1. Wählen Sie den Endpunkt aus.

   Die Seite mit den Endpunktdetails wird angezeigt.

2. Wählen Sie **Verbindung** > **Verbindung testen**.

Wenn Sie **Verbindung testen** auswählen, überprüft StorageGRID , ob der Endpunkt der Plattformdienste vorhanden ist und mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Beheben von Endpunktfehlern

Mithilfe der Meldung „Letzter Fehler“ auf der Seite mit den Endpunktdetails können Sie die Fehlerursache ermitteln. Bei einigen Fehlern müssen Sie möglicherweise den Endpunkt bearbeiten, um das Problem zu beheben. Beispielsweise kann ein CloudMirroring-Fehler auftreten, wenn StorageGRID nicht auf den Ziel-S3-Bucket zugreifen kann, weil es nicht über die richtigen Zugriffsberechtigungen verfügt oder der Zugriffsschlüssel abgelaufen ist. Die Meldung lautet: „Entweder müssen die Endpunktanmeldeinformationen oder der Zielzugriff aktualisiert werden“, und die Details lauten „AccessDenied“ oder „InvalidAccessKeyId“.

Wenn Sie den Endpunkt bearbeiten müssen, um einen Fehler zu beheben, führt die Auswahl von **Testen und Änderungen speichern** dazu, dass StorageGRID den aktualisierten Endpunkt validiert und bestätigt, dass er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Schritte

1. Wählen Sie den Endpunkt aus.
2. Wählen Sie auf der Seite mit den Endpunktdetails **Konfiguration** aus.
3. Bearbeiten Sie die Endpunktkonfiguration nach Bedarf.
4. Wählen Sie **Verbindung** > **Verbindung testen**.

Endpunktanmeldeinformationen mit unzureichenden Berechtigungen

Wenn StorageGRID einen Plattformdienst-Endpunkt validiert, bestätigt es, dass die Anmeldeinformationen des Endpunkts zum Kontaktieren der Zielressource verwendet werden können, und führt eine grundlegende Berechtigungsprüfung durch. StorageGRID validiert jedoch nicht alle Berechtigungen, die für bestimmte Vorgänge der Plattformdienste erforderlich sind. Wenn Sie beim Versuch, einen Plattformdienst zu verwenden, eine Fehlermeldung erhalten (z. B. „403 Forbidden“), überprüfen Sie daher die mit den Anmeldeinformationen des Endpunkts verknüpften Berechtigungen.

Ähnliche Informationen

- **StorageGRID verwalten › Fehlerbehebung bei Plattformdiensten**

- "Plattformdienst-Endpunkt erstellen"
- "Testen Sie die Verbindung für den Plattformdienst-Endpunkt"
- "Plattformdienst-Endpunkt bearbeiten"

Konfigurieren der CloudMirror-Replikation

Um die CloudMirror-Replikation für einen Bucket zu aktivieren, erstellen und wenden Sie eine gültige XML-Konfiguration für die Bucket-Replikation an.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Replikationsquelle fungiert.
- Der Endpunkt, den Sie als Ziel für die CloudMirror-Replikation verwenden möchten, ist bereits vorhanden und Sie verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

Die CloudMirror-Replikation kopiert Objekte aus einem Quell-Bucket in einen Ziel-Bucket, der in einem Endpunkt angegeben ist.

Allgemeine Informationen zur Bucket-Replikation und ihrer Konfiguration finden Sie unter "Amazon Simple Storage Service (S3)-Dokumentation: Objekte replizieren" . Informationen zur Implementierung von GetBucketReplication, DeleteBucketReplication und PutBucketReplication StorageGRID finden Sie im"Operationen an Buckets" .

> Die CloudMirror-Replikation weist wichtige Ähnlichkeiten und Unterschiede zur Cross-Grid-Replikationsfunktion auf. Weitere Informationen finden Sie unter"Vergleichen Sie Cross-Grid-Replikation und CloudMirror-Replikation" .

Beachten Sie beim Konfigurieren der CloudMirror-Replikation die folgenden Anforderungen und Merkmale:

- Wenn Sie eine gültige XML-Konfiguration für die Bucket-Replikation erstellen und anwenden, muss diese für jedes Ziel die URN eines S3-Bucket-Endpunkts verwenden.
- Die Replikation wird für Quell- oder Ziel-Buckets mit aktivierter S3-Objektsperre nicht unterstützt.
- Wenn Sie die CloudMirror-Replikation für einen Bucket aktivieren, der Objekte enthält, werden dem Bucket neu hinzugefügte Objekte repliziert, die vorhandenen Objekte im Bucket werden jedoch nicht repliziert. Sie müssen vorhandene Objekte aktualisieren, um die Replikation auszulösen.
- Wenn Sie in der XML-Replikationskonfiguration eine Speicherklasse angeben, verwendet StorageGRID diese Klasse beim Ausführen von Vorgängen am Ziel-S3-Endpunkt. Der Zielendpunkt muss auch die angegebene Speicherklasse unterstützen. Befolgen Sie unbedingt alle Empfehlungen des Zielsystemanbieters.

Schritte

1. Aktivieren Sie die Replikation für Ihren Quell-Bucket:
   - Verwenden Sie einen Texteditor, um die zum Aktivieren der Replikation erforderliche XML-Replikationskonfiguration zu erstellen, wie in der S3-Replikations-API angegeben.

- Beim Konfigurieren des XML:
  - Beachten Sie, dass StorageGRID nur V1 der Replikationskonfiguration unterstützt. Dies bedeutet, dass StorageGRID die Verwendung des `Filter` Element für Regeln und befolgt V1-Konventionen zum Löschen von Objektversionen. Weitere Informationen finden Sie in der Amazon-Dokumentation zur Replikationskonfiguration.
  - Verwenden Sie die URN eines S3-Bucket-Endpunkts als Ziel.
  - Optional fügen Sie die `<StorageClass>` Element und geben Sie eine der folgenden Optionen an:
    - `STANDARD`: Die Standardspeicherklasse. Wenn Sie beim Hochladen eines Objekts keine Speicherklasse angeben, `STANDARD` Speicherklasse wird verwendet.
    - `STANDARD_IA`: (Standard – seltener Zugriff.) Verwenden Sie diese Speicherklasse für Daten, auf die weniger häufig zugegriffen wird, die aber dennoch bei Bedarf einen schnellen Zugriff erfordern.
    - `REDUCED_REDUNDANCY`: Verwenden Sie diese Speicherklasse für nicht kritische, reproduzierbare Daten, die mit weniger Redundanz gespeichert werden können als die `STANDARD` Speicherklasse.
  - Wenn Sie eine `Role` im Konfigurations-XML wird es ignoriert. Dieser Wert wird von StorageGRID nicht verwendet.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
3. Wählen Sie den Namen des Quell-Buckets aus.

   Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie **Plattformdienste** > **Replikation**.
5. Aktivieren Sie das Kontrollkästchen **Replikation aktivieren**.
6. Fügen Sie die XML-Replikationskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

   Plattformdienste müssen für jedes Mandantenkonto von einem StorageGRID Administrator mithilfe des Grid Managers oder der Grid Management-API aktiviert werden. Wenden Sie sich an Ihren StorageGRID -Administrator, wenn beim Speichern der XML-Konfiguration ein Fehler auftritt.

7. Überprüfen Sie, ob die Replikation richtig konfiguriert ist:

a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die in der Replikationskonfiguration angegebenen Anforderungen für die Replikation erfüllt.

   Im zuvor gezeigten Beispiel werden Objekte repliziert, die mit dem Präfix „2020“ übereinstimmen.

b. Bestätigen Sie, dass das Objekt in den Ziel-Bucket repliziert wurde.

   Bei kleinen Objekten erfolgt die Replikation schnell.

Ähnliche Informationen

"Plattformdienst-Endpunkt erstellen"

Konfigurieren von Ereignisbenachrichtigungen

Sie aktivieren Benachrichtigungen für einen Bucket, indem Sie eine XML-Benachrichtigungskonfiguration erstellen und den Tenant Manager verwenden, um die XML auf einen Bucket anzuwenden.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Benachrichtigungsquelle dient.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, ist bereits vorhanden und Sie verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

Sie konfigurieren Ereignisbenachrichtigungen, indem Sie die Benachrichtigungskonfigurations-XML mit einem Quell-Bucket verknüpfen. Die XML-Benachrichtigungskonfiguration folgt den S3-Konventionen zum Konfigurieren von Bucket-Benachrichtigungen, wobei das Zielthema Kafka oder Amazon SNS als URN eines Endpunkts angegeben ist.

Allgemeine Informationen zu Ereignisbenachrichtigungen und deren Konfiguration finden Sie im "Amazon-Dokumentation" . Informationen zur Implementierung der S3-Bucket-Benachrichtigungskonfigurations-API durch StorageGRID finden Sie im"Anweisungen zur Implementierung von S3-Clientanwendungen" .

Beachten Sie beim Konfigurieren von Ereignisbenachrichtigungen für einen Bucket die folgenden Anforderungen und Merkmale:

- Wenn Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden, muss für jedes Ziel die URN eines Endpunkts für Ereignisbenachrichtigungen verwendet werden.
- 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.
- Nachdem Sie Ereignisbenachrichtigungen konfiguriert haben, wird jedes Mal, wenn ein bestimmtes Ereignis für ein Objekt im Quell-Bucket eintritt, eine Benachrichtigung generiert und an das als Zielendpunkt verwendete Amazon SNS- oder Kafka-Thema gesendet.
- Wenn Sie Ereignisbenachrichtigungen für einen Bucket aktivieren, der Objekte enthält, werden Benachrichtigungen nur für Aktionen gesendet, die nach dem Speichern der

Benachrichtigungskonfiguration ausgeführt werden.

Schritte

1. Aktivieren Sie Benachrichtigungen für Ihren Quell-Bucket:
   - Verwenden Sie einen Texteditor, um die zum Aktivieren von Ereignisbenachrichtigungen erforderliche XML-Benachrichtigungskonfiguration zu erstellen, wie in der S3-Benachrichtigungs-API angegeben.
   - Verwenden Sie beim Konfigurieren des XML die URN eines Endpunkts für Ereignisbenachrichtigungen als Zielthema.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. Wählen Sie im Mandanten-Manager **STORAGE (S3)** > **Buckets**.
3. Wählen Sie den Namen des Quell-Buckets aus.

   Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie **Plattformdienste** > **Ereignisbenachrichtigungen**.
5. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigungen aktivieren**.
6. Fügen Sie die XML-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

   Plattformdienste müssen für jedes Mandantenkonto von einem StorageGRID Administrator mithilfe des Grid Managers oder der Grid Management-API aktiviert werden. Wenden Sie sich an Ihren StorageGRID -Administrator, wenn beim Speichern der XML-Konfiguration ein Fehler auftritt.

7. Überprüfen Sie, ob die Ereignisbenachrichtigungen richtig konfiguriert sind:
   a. Führen Sie eine Aktion für ein Objekt im Quell-Bucket aus, das die Anforderungen zum Auslösen einer Benachrichtigung erfüllt, wie in der Konfigurations-XML konfiguriert.

      Im Beispiel wird eine Ereignisbenachrichtigung gesendet, wenn ein Objekt mit dem `images/` Präfix.

b. Bestätigen Sie, dass eine Benachrichtigung an das Zielthema Amazon SNS oder Kafka übermittelt wurde.

   Wenn Ihr Zielthema beispielsweise auf Amazon SNS gehostet wird, können Sie den Dienst so konfigurieren, dass er Ihnen eine E-Mail sendet, wenn die Benachrichtigung zugestellt wird.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+
Wenn die Benachrichtigung beim Zielthema empfangen wird, haben Sie Ihren Quell-Bucket erfolgreich für StorageGRID -Benachrichtigungen konfiguriert.

Ähnliche Informationen

"Benachrichtigungen für Buckets verstehen"

"Verwenden Sie die S3 REST-API"

"Plattformdienst-Endpunkt erstellen"

Konfigurieren des Suchintegrationsdienstes

Sie aktivieren die Suchintegration für einen Bucket, indem Sie XML für die Suchintegration erstellen und den Tenant Manager verwenden, um das XML auf den Bucket anzuwenden.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie haben bereits einen S3-Bucket erstellt, dessen Inhalt Sie indizieren möchten.
- Der Endpunkt, den Sie als Ziel für den Suchintegrationsdienst verwenden möchten, ist bereits vorhanden und Sie verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

Nachdem Sie den Suchintegrationsdienst für einen Quell-Bucket konfiguriert haben, löst das Erstellen eines Objekts oder das Aktualisieren der Metadaten oder Tags eines Objekts das Senden von Objektmetadaten an den Zielendpunkt aus.

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, der bereits Objekte enthält, werden für vorhandene Objekte nicht automatisch Metadatenbenachrichtigungen gesendet. Aktualisieren Sie diese vorhandenen Objekte, um sicherzustellen, dass ihre Metadaten zum Zielsuchindex hinzugefügt werden.

Schritte

1. Aktivieren Sie die Suchintegration für einen Bucket:
    - Verwenden Sie einen Texteditor, um die XML-Metadatenbenachrichtigung zu erstellen, die zum Aktivieren der Suchintegration erforderlich ist.
    - Verwenden Sie beim Konfigurieren des XML die URN eines Suchintegrationsendpunkts als Ziel.

      Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise könnten Sie Metadaten für Objekte mit dem Präfix `images` zu einem Ziel und Metadaten für Objekte mit dem Präfix `videos` zu einem anderen. Konfigurationen mit überlappenden Präfixen sind ungültig und werden bei der Übermittlung abgelehnt. Beispielsweise eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` und eine zweite Regel für Objekte mit dem Präfix `test2` ist nicht erlaubt.

      Bei Bedarf finden Sie weitere Informationen imBeispiele für die Metadatenkonfigurations-XML .

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Elemente in der XML-Konfiguration der Metadatenbenachrichtigung:

Name	Beschreibung	Erforderlich
Metadatenbenachrichtigungskonfiguration	Container-Tag für Regeln, die zum Angeben der Objekte und des Ziels für Metadatenbenachrichtigungen verwendet werden. Enthält ein oder mehrere Regelelemente.	Ja
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten einem angegebenen Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration-Element enthalten.	Ja
AUSWEIS	Eindeutige Kennung für die Regel. Im Regelelement enthalten.	Nein
Status	Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen. Im Regelelement enthalten.	Ja
Präfix	Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet. Um alle Objekte abzugleichen, geben Sie ein leeres Präfix an. Im Regelelement enthalten.	Ja
Ziel	Container-Tag für das Ziel einer Regel. Im Regelelement enthalten.	Ja

Name	Beschreibung	Erforderlich
Urne	URN des Ziels, an das die Objektmetadaten gesendet werden. Muss die URN eines StorageGRID -Endpunkts mit den folgenden Eigenschaften sein: • `es`muss das dritte Element sein. • Die URN muss mit dem Index und Typ enden, in dem die Metadaten gespeichert sind, in der Form `domain-name/myindex/mytype` . Endpunkte werden mithilfe des Tenant Managers oder der Tenant Management API konfiguriert. Sie haben folgende Form: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML übermittelt wird, andernfalls schlägt die Konfiguration mit einem 404-Fehler fehl. URN ist im Zielelement enthalten.	Ja

2. Wählen Sie im Tenant Manager **STORAGE (S3)** > **Buckets**.
3. Wählen Sie den Namen des Quell-Buckets aus.

   Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie **Plattformdienste** > **Suchintegration**
5. Aktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
6. Fügen Sie die Metadaten-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

   Plattformdienste müssen für jedes Mandantenkonto von einem StorageGRID Administrator mithilfe des Grid Managers oder der Management-API aktiviert werden. Wenden Sie sich an Ihren StorageGRID -Administrator, wenn beim Speichern der XML-Konfiguration ein Fehler auftritt.

7. Überprüfen Sie, ob der Suchintegrationsdienst richtig konfiguriert ist:
   a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die Anforderungen zum Auslösen einer Metadatenbenachrichtigung erfüllt, wie im Konfigurations-XML angegeben.

      Im zuvor gezeigten Beispiel lösen alle zum Bucket hinzugefügten Objekte eine Metadatenbenachrichtigung aus.

   b. Bestätigen Sie, dass dem im Endpunkt angegebenen Suchindex ein JSON-Dokument hinzugefügt wurde, das die Metadaten und Tags des Objekts enthält.

Nach Abschluss

Bei Bedarf können Sie die Suchintegration für einen Bucket mit einer der folgenden Methoden deaktivieren:

- Wählen Sie **STORAGE (S3)** > **Buckets** und deaktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
- Wenn Sie die S3-API direkt verwenden, verwenden Sie eine Benachrichtigungsanforderung zum Löschen von Bucket-Metadaten. Siehe die Anweisungen zum Implementieren von S3-Clientanwendungen.

Beispiel: Metadaten-Benachrichtigungskonfiguration, die für alle Objekte gilt

In diesem Beispiel werden die Objektmetadaten für alle Objekte an dasselbe Ziel gesendet.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Beispiel: Konfiguration der Metadatenbenachrichtigung mit zwei Regeln

In diesem Beispiel werden Objektmetadaten für Objekte verwendet, die mit dem Präfix `/images` wird an ein Ziel gesendet, während Objektmetadaten für Objekte, die dem Präfix entsprechen `/videos` wird an ein zweites Ziel gesendet.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Metadaten-Benachrichtigungsformat

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, wird jedes Mal, wenn Objektmetadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden, ein JSON-Dokument generiert und an den Zielendpunkt gesendet.

Dieses Beispiel zeigt ein Beispiel des JSON, das generiert werden könnte, wenn ein Objekt mit dem Schlüssel `SGWS/Tagging.txt` wird in einem Bucket namens erstellt `test` . Der `test` Bucket ist nicht versioniert, also die `versionId` -Tag ist leer.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Im JSON-Dokument enthaltene Felder

Der Dokumentname umfasst den Bucket-Namen, den Objektnamen und die Versions-ID, falls vorhanden.

Bucket- und Objektinformationen

`bucket`: Name des Buckets

`key`: Objektschlüsselname

`versionID`: Objektversion, für Objekte in versionierten Buckets

`region`: Bucket-Bereich, zum Beispiel `us-east-1`

Systemmetadaten

`size`: Objektgröße (in Bytes), wie sie für einen HTTP-Client sichtbar ist

`md5`: Objekt-Hash

Benutzermetadaten

`metadata`: Alle Benutzermetadaten für das Objekt als Schlüssel-Wert-Paare

`key:value`

Schlagwörter

`tags`: Alle für das Objekt definierten Objekt-Tags als Schlüssel-Wert-Paare

`key:value`

So zeigen Sie Ergebnisse in Elasticsearch an

Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen

als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur Zuordnung von Datumsformaten. Aktivieren Sie die dynamischen Feldzuordnungen im Index, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Verwenden Sie die S3 REST-API

Unterstützte Versionen und Updates der S3 REST API

StorageGRID unterstützt die Simple Storage Service (S3)-API, die als Satz von Representational State Transfer (REST)-Webdiensten implementiert ist.

Durch die Unterstützung der S3 REST API können Sie serviceorientierte Anwendungen, die für S3-Webdienste entwickelt wurden, mit lokalem Objektspeicher verbinden, der das StorageGRID -System verwendet. Es sind nur minimale Änderungen an der aktuellen Verwendung von S3 REST-API-Aufrufen durch eine Clientanwendung erforderlich.

Unterstützte Versionen

StorageGRID unterstützt die folgenden spezifischen Versionen von S3 und HTTP.

Artikel	Version
S3-API-Spezifikation	"Amazon Web Services (AWS)-Dokumentation: Amazon Simple Storage Service API-Referenz"
HTTP	1,1 Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35). "IETF RFC 2616: Hypertext Transfer Protocol (HTTP/1.1)" **Hinweis**: StorageGRID unterstützt kein HTTP/1.1-Pipelining.

Aktualisierungen der S3 REST API-Unterstützung

Freigeben	Kommentare
11,9	• Unterstützung für vorberechnete SHA-256-Prüfsummenwerte für die folgenden Anfragen und unterstützten Header hinzugefügt. Mit dieser Funktion können Sie die Integrität hochgeladener Objekte überprüfen: ◦ CompleteMultipartUpload: `x-amz-checksum-sha256` ◦ CreateMultipartUpload: `x-amz-checksum-algorithm` ◦ GetObject: `x-amz-checksum-mode` ◦ Kopfobjekt: `x-amz-checksum-mode` ◦ Teileliste ◦ PutObject: `x-amz-checksum-sha256` ◦ UploadPart: `x-amz-checksum-sha256` • Dem Grid-Administrator wurde die Möglichkeit hinzugefügt, die Aufbewahrungs- und Compliance-Einstellungen auf Mandantenebene zu steuern. Diese Einstellungen wirken sich auf die S3 Object Lock-Einstellungen aus. ◦ Standardaufbewahrungsmodus für Buckets und Objektaufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen. ◦ Standardaufbewahrungszeitraum des Buckets und Aufbewahrungsdatum des Objekts: Muss kleiner oder gleich dem zulässigen maximalen Aufbewahrungszeitraum sein, der vom Grid-Administrator festgelegt wurde. • Verbesserte Unterstützung für `aws-chunked` Inhaltskodierung und Streaming `x-amz-content-sha256` Werte. Einschränkungen: ◦ Falls vorhanden, `chunk-signature` ist optional und nicht validiert ◦ Falls vorhanden, `x-amz-trailer` Inhalt wird ignoriert
11,8	Die Namen der S3-Operationen wurden aktualisiert, damit sie mit den Namen übereinstimmen, die in der "Amazon Web Services (AWS)-Dokumentation: Amazon Simple Storage Service API-Referenz" .
11,7	• Hinzugefügt"Kurzreferenz: Unterstützte S3-API-Anfragen" . • Unterstützung für die Verwendung des GOVERNANCE-Modus mit S3 Object Lock hinzugefügt. • Unterstützung für das StorageGRID-spezifische `x-ntap-sg-cgr-replication-status` Antwortheader für GET Object- und HEAD Object-Anfragen. Dieser Header gibt den Replikationsstatus eines Objekts für die Cross-Grid-Replikation an. • SelectObjectContent-Anfragen unterstützen jetzt Parquet-Objekte.

Freigeben	Kommentare
11,6	• Unterstützung für die Verwendung von hinzugefügt `partNumber` Anforderungsparameter in GET-Objekt- und HEAD-Objektanforderungen. • Unterstützung für einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer auf Bucket-Ebene für S3 Object Lock hinzugefügt. • Zusätzliche Unterstützung für die `s3:object-lock-remaining-retention-days` Richtlinienbedingungsschlüssel, um den Bereich der zulässigen Aufbewahrungszeiträume für Ihre Objekte festzulegen. • Die maximal *empfohlene* Größe für einen einzelnen PUT-Objektvorgang wurde auf 5 GiB (5.368.709.120 Bytes) geändert. Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie stattdessen den mehrteiligen Upload.
11,5	• Unterstützung für die Verwaltung der Bucket-Verschlüsselung hinzugefügt. • Unterstützung für S3 Object Lock und veraltete Compliance-Anfragen hinzugefügt. • Unterstützung für die Verwendung von DELETE Multiple Objects bei versionierten Buckets hinzugefügt. • Der `Content-MD5` Der Anforderungsheader wird jetzt korrekt unterstützt.
11,4	• Unterstützung für DELETE-Bucket-Tagging, GET-Bucket-Tagging und PUT-Bucket-Tagging hinzugefügt. Kostenzuordnungs-Tags werden nicht unterstützt. • Für in StorageGRID 11.4 erstellte Buckets ist die Einschränkung von Objektschlüsselnamen zur Einhaltung der Best Practices für die Leistung nicht mehr erforderlich. • Unterstützung für Bucket-Benachrichtigungen hinzugefügt auf der `s3:ObjectRestore:Post` Ereignistyp. • AWS-Größenbeschränkungen für mehrteilige Teile werden jetzt erzwungen. Jeder Teil eines mehrteiligen Uploads muss zwischen 5 MiB und 5 GiB groß sein. Der letzte Teil kann kleiner als 5 MiB sein. • Unterstützung für TLS 1.3 hinzugefügt
11,3	• Unterstützung für die serverseitige Verschlüsselung von Objektdaten mit vom Kunden bereitgestellten Schlüsseln (SSE-C) hinzugefügt. • Unterstützung für DELETE-, GET- und PUT-Bucket-Lebenszyklusoperationen (nur Ablaufaktion) und für die `x-amz-expiration` Antwortheader. • PUT-Objekt, PUT-Objekt – Kopieren und mehrteiliger Upload aktualisiert, um die Auswirkungen von ILM-Regeln zu beschreiben, die eine synchrone Platzierung bei der Aufnahme verwenden. • TLS 1.1-Chiffren werden nicht mehr unterstützt.

Freigeben	Kommentare
11,2	Unterstützung für die POST-Objektwiederherstellung zur Verwendung mit Cloud-Speicherpools hinzugefügt. Unterstützung für die Verwendung der AWS-Syntax für ARN, Richtlinienbedingungsschlüssel und Richtlinienvariablen in Gruppen- und Bucket-Richtlinien hinzugefügt. Vorhandene Gruppen- und Bucket-Richtlinien, die die StorageGRID Syntax verwenden, werden weiterhin unterstützt. **Hinweis:** Die Verwendung von ARN/URN in anderen JSON/XML-Konfigurationen, einschließlich der in benutzerdefinierten StorageGRID -Funktionen verwendeten, hat sich nicht geändert.
11,1	Unterstützung für Cross-Origin Resource Sharing (CORS), HTTP für S3-Clientverbindungen zu Grid-Knoten und Compliance-Einstellungen für Buckets hinzugefügt.
11,0	Unterstützung für die Konfiguration von Plattformdiensten (CloudMirror-Replikation, Benachrichtigungen und Elasticsearch-Suchintegration) für Buckets hinzugefügt. Außerdem wurde Unterstützung für die Objektmarkierung, Standortbeschränkungen für Buckets und die verfügbare Konsistenz hinzugefügt.
10,4	Unterstützung für ILM-Scan-Änderungen an der Versionierung, Aktualisierungen der Seite „Endpoint Domain Names“, Bedingungen und Variablen in Richtlinien, Richtlinienbeispielen und der Berechtigung „PutOverwriteObject“ hinzugefügt.
10,3	Unterstützung für Versionierung hinzugefügt.
10,2	Unterstützung für Gruppen- und Bucket-Zugriffsrichtlinien sowie für mehrteilige Kopien (Upload-Teil – Kopie) hinzugefügt.
10,1	Unterstützung für mehrteilige Uploads, Anfragen im virtuellen gehosteten Stil und v4-Authentifizierung hinzugefügt.
10,0	Erste Unterstützung der S3 REST API durch das StorageGRID -System. Die aktuell unterstützte Version der *Simple Storage Service API Reference* ist der 01.03.2006.

Kurzreferenz: Unterstützte S3-API-Anfragen

Auf dieser Seite wird zusammengefasst, wie StorageGRID die APIs des Amazon Simple Storage Service (S3) unterstützt.

Diese Seite enthält nur die S3-Operationen, die von StorageGRID unterstützt werden.

Um die AWS-Dokumentation für jeden Vorgang anzuzeigen, wählen Sie den Link in der Überschrift aus.

Allgemeine URI-Abfrageparameter und Anforderungsheader

Sofern nicht anders angegeben, werden die folgenden allgemeinen URI-Abfrageparameter unterstützt:

- `versionId`(wie für Objektoperationen erforderlich)

Sofern nicht anders angegeben, werden die folgenden allgemeinen Anforderungsheader unterstützt:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Ähnliche Informationen

- "Details zur S3 REST API-Implementierung"
- "Amazon Simple Storage Service API-Referenz: Allgemeine Anforderungsheader"

"AbortMultipartUpload"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diesen zusätzlichen URI-Abfrageparameter:

- `uploadId`

Anforderungstext

Keine

StorageGRID -Dokumentation

"Vorgänge für mehrteilige Uploads"

"CompleteMultipartUpload"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diesen zusätzlichen URI-Abfrageparameter:

- `uploadId`
- `x-amz-checksum-sha256`

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- `ChecksumSHA256`
- `CompleteMultipartUpload`

- `ETag`
- `Part`
- `PartNumber`

StorageGRID -Dokumentation

"CompleteMultipartUpload"

"Objekt kopieren"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Header:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Anforderungstext

Keine

StorageGRID -Dokumentation

"Objekt kopieren"

"Bucket erstellen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Header:

- `x-amz-bucket-object-lock-enabled`

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Operationen an Buckets"

"CreateMultipartUpload"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Header:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Anforderungstext

Keine

StorageGRID -Dokumentation

"CreateMultipartUpload"

"Bucket löschen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage.

StorageGRID -Dokumentation

"Operationen an Buckets"

"BucketCors löschen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"DeleteBucketEncryption"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"DeleteBucketLifecycle"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

- "Operationen an Buckets"
- "Erstellen einer S3-Lebenszykluskonfiguration"

"DeleteBucketPolicy"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"DeleteBucketReplication"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"BucketTagging löschen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"Objekt löschen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diesen zusätzlichen Anfrageheader:

- `x-amz-bypass-governance-retention`

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Objekten"

"Objekte löschen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diesen zusätzlichen Anfrageheader:

- `x-amz-bypass-governance-retention`

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Operationen an Objekten"

"DeleteObjectTagging"

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Objekten"

"GetBucketAcl"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketCors"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketEncryption"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketLifecycleConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

- "Operationen an Buckets"
- "Erstellen einer S3-Lebenszykluskonfiguration"

"BucketLocation abrufen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketNotificationConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketPolicy"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketReplication"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketVersioning"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen URI-Abfrageparameter:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Und diese zusätzlichen Anforderungsheader:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Anforderungstext

Keine

StorageGRID -Dokumentation

"GetObject"

"GetObjectAcl"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Objekten"

"GetObjectLegalHold"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

"GetObjectLockConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

"GetObjectRetention"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

"GetObjectTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Objekten"

"Kopfeimer"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"HeadObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alleallgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Header:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Anforderungstext

Keine

StorageGRID -Dokumentation

"HeadObject"

"Buckets auflisten"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

Operationen auf dem Dienst › ListBuckets

"ListMultipartUploads"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Parameter:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Anforderungstext

Keine

StorageGRID -Dokumentation

"ListMultipartUploads"

"ListObjects"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Parameter:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"ListObjectsV2"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Parameter:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"ListObjectVersions"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Parameter:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"Teileliste"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Parameter:

- `max-parts`

- `part-number-marker`
- `uploadId`

Anforderungstext

Keine

StorageGRID -Dokumentation

"ListMultipartUploads"

"PutBucketCors"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketEncryption"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketLifecycleConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- `And`
- `Days`
- `Expiration`

- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

StorageGRID -Dokumentation

- "Operationen an Buckets"
- "Erstellen einer S3-Lebenszykluskonfiguration"

"PutBucketNotificationConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketPolicy"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Einzelheiten zu den unterstützten JSON-Body-Feldern finden Sie unter"Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien" .

"PutBucketReplication"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

XML-Tags des Anforderungstexts

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketVersioning"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstextparameter

StorageGRID unterstützt die folgenden Anforderungstextparameter:

- `VersioningConfiguration`
- `Status`

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen Header:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Anforderungstext

- Binärdaten des Objekts

StorageGRID -Dokumentation

"PutObject"

"PutObjectLegalHold"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

"PutObjectLockConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

"PutObjectRetention"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage, plus diesen zusätzlichen Header:

- `x-amz-bypass-governance-retention`

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

"PutObjectTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Operationen an Objekten"

"RestoreObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allgemeine Parameter und Header für diese Anfrage.

Anforderungstext

Einzelheiten zu den unterstützten Body-Feldern finden Sie unter"RestoreObject" .

"SelectObjectContent"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage.

Anforderungstext

Einzelheiten zu den unterstützten Textfeldern finden Sie hier:

- "Verwenden Sie S3 Select"
- "SelectObjectContent"

"UploadPart"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen URI-Abfrageparameter:

- `partNumber`
- `uploadId`

Und diese zusätzlichen Anforderungsheader:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Anforderungstext

- Binärdaten des Teils

StorageGRID -Dokumentation

"UploadPart"

"UploadPartCopy"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt allegemeine Parameter und Header für diese Anfrage, plus diese zusätzlichen URI-Abfrageparameter:

- `partNumber`
- `uploadId`

Und diese zusätzlichen Anforderungsheader:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Anforderungstext

Keine

StorageGRID -Dokumentation

"UploadPartCopy"

Testen der S3 REST API-Konfiguration

Sie können die Amazon Web Services Command Line Interface (AWS CLI) verwenden, um Ihre Verbindung zum System zu testen und zu überprüfen, ob Sie Objekte lesen und schreiben können.

Bevor Sie beginnen

- Sie haben die AWS CLI von heruntergeladen und installiert "aws.amazon.com/cli" .
- Optional haben Sie"einen Load Balancer-Endpunkt erstellt" . Andernfalls kennen Sie die IP-Adresse des Speicherknotens, mit dem Sie eine Verbindung herstellen möchten, und die zu verwendende Portnummer. Sehen "IP-Adressen und Ports für Clientverbindungen" .
- Du hast"ein S3-Mandantenkonto erstellt" .
- Sie haben sich beim Mandanten angemeldet und"einen Zugriffsschlüssel erstellt" .

Einzelheiten zu diesen Schritten finden Sie unter"Konfigurieren von Clientverbindungen" .

Schritte

1. Konfigurieren Sie die AWS CLI-Einstellungen, um das Konto zu verwenden, das Sie im StorageGRID -System erstellt haben:
   a. Wechseln Sie in den Konfigurationsmodus: `aws configure`
   b. Geben Sie die Zugriffsschlüssel-ID für das von Ihnen erstellte Konto ein.
   c. Geben Sie den geheimen Zugriffsschlüssel für das von Ihnen erstellte Konto ein.
   d. Geben Sie die zu verwendende Standardregion ein. Beispiel: `us-east-1` .
   e. Geben Sie das zu verwendende Standardausgabeformat ein oder drücken Sie die Eingabetaste, um JSON auszuwählen.
2. Erstellen Sie einen Bucket.

   In diesem Beispiel wird davon ausgegangen, dass Sie einen Load Balancer-Endpunkt für die Verwendung der IP-Adresse 10.96.101.17 und des Ports 10443 konfiguriert haben.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Wenn der Bucket erfolgreich erstellt wurde, wird der Speicherort des Buckets zurückgegeben, wie im folgenden Beispiel zu sehen ist:

```
"Location": "/testbucket"
```

3. Laden Sie ein Objekt hoch.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Wenn das Objekt erfolgreich hochgeladen wurde, wird ein Etag zurückgegeben, der ein Hash der Objektdaten ist.

4. Listen Sie den Inhalt des Buckets auf, um zu überprüfen, ob das Objekt hochgeladen wurde.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Löschen Sie das Objekt.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Löschen Sie den Bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

So implementiert StorageGRID die S3 REST API

Widersprüchliche Clientanforderungen

Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst.

Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.

Konsistenzwerte

Konsistenz sorgt für ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Standorte hinweg. Sie können die Konsistenz je nach Anwendungsfall ändern.

Standardmäßig garantiert StorageGRID die Lese-nach-Schreib-Konsistenz für neu erstellte Objekte. Jeder GET nach einem erfolgreich abgeschlossenen PUT kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und Löschungen sind letztendlich konsistent. Die Ausbreitung von Überschreibungen dauert im Allgemeinen Sekunden oder Minuten, kann aber bis zu 15 Tage dauern.

Wenn Sie Objektoperationen mit einer anderen Konsistenz durchführen möchten, können Sie:

- Geben Sie eine Konsistenz fürjeder Eimer .
- Geben Sie eine Konsistenz fürjede API-Operation .
- Ändern Sie die standardmäßige rasterweite Konsistenz, indem Sie eine der folgenden Aufgaben ausführen:
  - Gehen Sie im Grid Manager zu **KONFIGURATION** > **System** > **Speichereinstellungen** > **Standardkonsistenz**.
  - .

> Eine Änderung der rasterweiten Konsistenz gilt nur für Buckets, die nach der Änderung der Einstellung erstellt wurden. Um die Details einer Änderung zu ermitteln, sehen Sie sich das Audit-Protokoll an unter `/var/local/log` (Suche nach **Konsistenzebene**).

Konsistenzwerte

Die Konsistenz wirkt sich darauf aus, wie die Metadaten, die StorageGRID zum Verfolgen von Objekten verwendet, zwischen Knoten verteilt werden und somit auf die Verfügbarkeit von Objekten für Clientanforderungen.

Sie können die Konsistenz für einen Bucket oder eine API-Operation auf einen der folgenden Werte festlegen:

- **Alle**: Alle Knoten erhalten die Daten sofort, andernfalls schlägt die Anfrage fehl.
- **Stark global**: Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites.
- **Strong-Site**: Garantiert die Lese-nach-Schreib-Konsistenz für alle Clientanforderungen innerhalb einer Site.
- **Lesen nach neuem Schreiben**: (Standard) Bietet Lese-nach-Schreib-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
- **Verfügbar**: Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

Verwenden Sie die Konsistenz „Lesen nach neuem Schreiben“ und „Verfügbar“.

Wenn ein HEAD- oder GET-Vorgang die Konsistenz „Lesen nach neuem Schreiben“ verwendet, führt StorageGRID die Suche in mehreren Schritten wie folgt durch:

- Es sucht zunächst mit geringer Konsistenz nach dem Objekt.
- Wenn diese Suche fehlschlägt, wird die Suche beim nächsten Konsistenzwert wiederholt, bis eine Konsistenz erreicht wird, die dem Verhalten für „stark global“ entspricht.

Wenn ein HEAD- oder GET-Vorgang die Konsistenz „Lesen nach neuem Schreiben“ verwendet, das Objekt jedoch nicht vorhanden ist, erreicht die Objektsuche immer eine Konsistenz, die dem Verhalten für „Strong-Global“ entspricht. Da für diese Konsistenz mehrere Kopien der Objektmetadaten an jedem Standort verfügbar sein müssen, kann es zu einer hohen Anzahl interner Serverfehler vom Typ 500 kommen, wenn zwei oder mehr Speicherknoten am selben Standort nicht verfügbar sind.

Sofern Sie keine Konsistenzgarantien ähnlich denen von Amazon S3 benötigen, können Sie diese Fehler bei HEAD- und GET-Vorgängen verhindern, indem Sie die Konsistenz auf „Verfügbar“ setzen. Wenn ein HEAD- oder GET-Vorgang die Konsistenz „Verfügbar“ verwendet, bietet StorageGRID nur die letztendliche Konsistenz. Ein fehlgeschlagener Vorgang wird bei zunehmender Konsistenz nicht wiederholt, sodass es nicht erforderlich ist, dass mehrere Kopien der Objektmetadaten verfügbar sind.

Konsistenz für API-Operation angeben

Um die Konsistenz für eine einzelne API-Operation festzulegen, müssen die Konsistenzwerte für die Operation unterstützt werden und Sie müssen die Konsistenz im Anforderungsheader angeben. In diesem Beispiel wird die Konsistenz für einen GetObject-Vorgang auf „Strong-Site“ festgelegt.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

Sie müssen für die PutObject- und GetObject-Vorgänge dieselbe Konsistenz verwenden.

Konsistenz für Bucket angeben

Um die Konsistenz für den Bucket festzulegen, können Sie das StorageGRID verwenden"PUT Bucket-Konsistenz" Anfrage. Oder Sie können"die Konsistenz eines Eimers ändern" vom Mieterverwalter.

Beachten Sie beim Festlegen der Konsistenz für einen Bucket Folgendes:

- Durch das Festlegen der Konsistenz für einen Bucket wird bestimmt, welche Konsistenz für S3-Operationen verwendet wird, die an den Objekten im Bucket oder an der Bucket-Konfiguration ausgeführt werden. Es hat keine Auswirkungen auf Vorgänge am Bucket selbst.
- Die Konsistenz für einen einzelnen API-Vorgang überschreibt die Konsistenz für den Bucket.
- Im Allgemeinen sollten Buckets die Standardkonsistenz „Lesen nach neuem Schreiben“ verwenden. Wenn Anfragen nicht richtig funktionieren, ändern Sie nach Möglichkeit das Verhalten des Anwendungsclients. Oder konfigurieren Sie den Client so, dass die Konsistenz für jede API-Anforderung angegeben wird. Stellen Sie die Konsistenz auf Eimerebene nur als letztes Mittel ein.

[[Wie Konsistenzkontrollen und ILM-Regeln zusammenwirken]]Wie Konsistenz- und ILM-Regeln den Datenschutz beeinflussen

Sowohl Ihre Wahl der Konsistenz als auch Ihre ILM-Regel wirken sich darauf aus, wie Objekte geschützt werden. Diese Einstellungen können interagieren.

Beispielsweise wirkt sich die beim Speichern eines Objekts verwendete Konsistenz auf die anfängliche Platzierung der Objektmetadaten aus, während das für die ILM-Regel ausgewählte Aufnahmeverhalten die anfängliche Platzierung der Objektkopien beeinflusst. Da StorageGRID zur Erfüllung von Clientanforderungen Zugriff auf die Metadaten und Daten eines Objekts benötigt, kann die Auswahl passender Schutzebenen für Konsistenz und Aufnahmeverhalten einen besseren anfänglichen Datenschutz und vorhersehbarere Systemreaktionen bieten.

Die folgende"Aufnahmeoptionen" stehen für ILM-Regeln zur Verfügung:

Doppeltes Commit

StorageGRID erstellt sofort Zwischenkopien des Objekts und meldet dem Client den Erfolg. Wenn möglich, werden die in der ILM-Regel angegebenen Kopien erstellt.

Strikt

Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor dem Client der Erfolg gemeldet wird.

Ausgewogen

StorageGRID versucht, bei der Aufnahme alle in der ILM-Regel angegebenen Kopien zu erstellen. Wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg wird an den Client zurückgegeben. Die in der ILM-Regel angegebenen Kopien werden nach Möglichkeit erstellt.

Beispiel für die Interaktion zwischen Konsistenz- und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Sites mit der folgenden ILM-Regel und der folgenden Konsistenz:

- **ILM-Regel**: Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem Remote-Standort. Verwenden Sie ein striktes Aufnahmeverhalten.
- **Konsistenz**: Stark global (Objektmetadaten werden sofort an alle Sites verteilt).

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID Kopien beider Objekte und verteilt Metadaten an beide Sites, bevor dem Client die Erfolgsmeldung zurückgegeben wird.

Zum Zeitpunkt der erfolgreichen Aufnahme der Nachricht ist das Objekt vollständig vor Verlust geschützt. Wenn beispielsweise die lokale Site kurz nach der Aufnahme verloren geht, sind am Remote-Standort weiterhin Kopien der Objektdaten und der Objektmetadaten vorhanden. Das Objekt ist vollständig abrufbar.

Wenn Sie stattdessen dieselbe ILM-Regel und die starke Site-Konsistenz verwenden, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten auf die Remote-Site repliziert wurden, aber bevor die Objektmetadaten dorthin verteilt werden. In diesem Fall entspricht das Schutzniveau der Objektmetadaten nicht dem Schutzniveau der Objektdaten. Wenn die lokale Site kurz nach der Aufnahme verloren geht, gehen die Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenz und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp , wenn Sie Hilfe benötigen.

Objektversionierung

Sie können den Versionsstatus eines Buckets festlegen, wenn Sie mehrere Versionen jedes Objekts behalten möchten. Durch Aktivieren der Versionierung für einen Bucket können Sie vor dem versehentlichen Löschen von Objekten schützen und frühere Versionen eines Objekts abrufen und wiederherstellen.

Das StorageGRID -System implementiert Versionierung mit Unterstützung für die meisten Funktionen und mit einigen Einschränkungen. StorageGRID unterstützt bis zu 10.000 Versionen jedes Objekts.

Die Objektversionierung kann mit StorageGRID Information Lifecycle Management (ILM) oder mit der S3-Bucket-Lebenszykluskonfiguration kombiniert werden. Sie müssen die Versionierung für jeden Bucket explizit aktivieren. Wenn die Versionierung für einen Bucket aktiviert ist, wird jedem dem Bucket hinzugefügten Objekt eine Versions-ID zugewiesen, die vom StorageGRID -System generiert wird.

Die Verwendung von MFA (Multi-Faktor-Authentifizierung) zum Löschen wird nicht unterstützt.

> Die Versionierung kann nur für Buckets aktiviert werden, die mit StorageGRID Version 10.3 oder höher erstellt wurden.

ILM und Versionierung

ILM-Richtlinien werden auf jede Version eines Objekts angewendet. Ein ILM-Scanprozess scannt kontinuierlich alle Objekte und wertet sie anhand der aktuellen ILM-Richtlinie neu aus. Alle Änderungen, die Sie an ILM-Richtlinien vornehmen, werden auf alle zuvor aufgenommenen Objekte angewendet. Dies schließt zuvor aufgenommene Versionen ein, wenn die Versionierung aktiviert ist. Beim ILM-Scannen werden neue ILM-Änderungen auf zuvor aufgenommene Objekte angewendet.

Für S3-Objekte in Buckets mit aktivierter Versionierung können Sie mit der Versionierungsunterstützung ILM-Regeln erstellen, die „Nicht aktuelle Zeit“ als Referenzzeit verwenden (wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ in"Schritt 1 des Assistenten „ILM-Regel erstellen““). Wenn ein Objekt aktualisiert wird, werden seine vorherigen Versionen nicht mehr aktuell. Mithilfe eines Filters „Nicht aktuelle Zeit“ können Sie Richtlinien erstellen, die die Speicherauswirkungen früherer Objektversionen reduzieren.

> Wenn Sie eine neue Version eines Objekts mithilfe eines mehrteiligen Uploadvorgangs hochladen, gibt die nicht aktuelle Zeit für die ursprüngliche Version des Objekts an, wann der mehrteilige Upload für die neue Version erstellt wurde, und nicht, wann der mehrteilige Upload abgeschlossen wurde. In seltenen Fällen kann die nicht aktuelle Zeit der Originalversion Stunden oder Tage vor der Zeit der aktuellen Version liegen.

Ähnliche Informationen

- "So werden versionierte S3-Objekte gelöscht"
- "ILM-Regeln und -Richtlinien für versionierte S3-Objekte (Beispiel 4)" .

Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren

Wenn die globale S3-Objektsperre-Einstellung für Ihr StorageGRID System aktiviert ist, können Sie Buckets mit aktivierter S3-Objektsperre erstellen. Sie können die Standardaufbewahrung für jeden Bucket oder Aufbewahrungseinstellungen für jede Objektversion angeben.

So aktivieren Sie die S3-Objektsperre für einen Bucket

Wenn die globale S3-Objektsperre-Einstellung für Ihr StorageGRID System aktiviert ist, können Sie die S3-Objektsperre optional aktivieren, wenn Sie jeden Bucket erstellen.

S3 Object Lock ist eine permanente Einstellung, die nur aktiviert werden kann, wenn Sie einen Bucket erstellen. Sie können die S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt

wurde.

Um die S3-Objektsperre für einen Bucket zu aktivieren, verwenden Sie eine der folgenden Methoden:

- Erstellen Sie den Bucket mit dem Tenant Manager. Sehen "S3-Bucket erstellen" .
- Erstellen Sie den Bucket mithilfe einer CreateBucket-Anforderung mit dem `x-amz-bucket-object-lock-enabled` Anforderungsheader. Sehen "Operationen an Buckets" .

S3 Object Lock erfordert eine Bucket-Versionierung, die beim Erstellen des Buckets automatisch aktiviert wird. Sie können die Versionsverwaltung für den Bucket nicht aussetzen. Sehen "Objektversionierung" .

Standardaufbewahrungseinstellungen für einen Bucket

Wenn S3 Object Lock für einen Bucket aktiviert ist, können Sie optional die Standardaufbewahrung für den Bucket aktivieren und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer angeben.

Standardaufbewahrungsmodus

- Im COMPLIANCE-Modus:
  - Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
  - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
  - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im GOVERNANCE-Modus:
  - Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung kann die `x-amz-bypass-governance-retention: true` Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen.
  - Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.
  - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Standardaufbewahrungsdauer

Für jeden Bucket kann eine Standardaufbewahrungsdauer in Jahren oder Tagen angegeben werden.

So legen Sie die Standardaufbewahrung für einen Bucket fest

Um die Standardaufbewahrung für einen Bucket festzulegen, verwenden Sie eine der folgenden Methoden:

- Verwalten Sie die Bucket-Einstellungen über den Tenant Manager. Sehen"Erstellen eines S3-Buckets" Und"Standardaufbewahrung für S3 Object Lock aktualisieren" .
- Geben Sie eine PutObjectLockConfiguration-Anforderung für den Bucket aus, um den Standardmodus und die Standardanzahl von Tagen oder Jahren anzugeben.

PutObjectLockConfiguration

Mit der PutObjectLockConfiguration-Anforderung können Sie den Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer für einen Bucket festlegen und ändern, bei dem S3 Object Lock aktiviert ist. Sie können auch zuvor konfigurierte Standardaufbewahrungseinstellungen entfernen.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der Standardaufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` Und `x-amz-object-lock-retain-until-date` sind nicht angegeben. Die Standardaufbewahrungsfrist wird zur Berechnung des Aufbewahrungs-bis-Datums

verwendet, wenn `x-amz-object-lock-retain-until-date` ist nicht angegeben.

Wenn die Standardaufbewahrungsfrist nach der Aufnahme einer Objektversion geändert wird, bleibt das Aufbewahrungsdatum der Objektversion gleich und wird nicht anhand der neuen Standardaufbewahrungsfrist neu berechnet.

Sie müssen über die `s3:PutBucketObjectLockConfiguration` Berechtigung oder Root-Konto sein, um diesen Vorgang abzuschließen.

Der `Content-MD5` Der Anforderungsheader muss in der PUT-Anforderung angegeben werden.

Anforderungsbeispiel

Dieses Beispiel aktiviert S3 Object Lock für einen Bucket und legt den Standardaufbewahrungsmodus auf COMPLIANCE und die Standardaufbewahrungsdauer auf 6 Jahre fest.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

So bestimmen Sie die Standardaufbewahrung für einen Bucket

Um festzustellen, ob S3 Object Lock für einen Bucket aktiviert ist, und um den Standardaufbewahrungsmodus und die Aufbewahrungsdauer anzuzeigen, verwenden Sie eine der folgenden Methoden:

- Zeigen Sie den Bucket im Mandanten-Manager an. Sehen "S3-Buckets anzeigen" .
- Geben Sie eine GetObjectLockConfiguration-Anforderung aus.

GetObjectLockConfiguration

Mit der GetObjectLockConfiguration-Anforderung können Sie feststellen, ob die S3-Objektsperre für einen Bucket aktiviert ist. Wenn dies der Fall ist, können Sie prüfen, ob für den Bucket ein Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer konfiguriert sind.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der Standardaufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` ist nicht angegeben. Die Standardaufbewahrungsfrist wird zur Berechnung des Aufbewahrungs-bis-Datums verwendet, wenn `x-amz-object-lock-retain-until-date` ist nicht angegeben.

Sie müssen über die `s3:GetBucketObjectLockConfiguration` Berechtigung oder Root-Konto sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Antwortbeispiel

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

So legen Sie Aufbewahrungseinstellungen für ein Objekt fest

Ein Bucket mit aktivierter S3 Object Lock kann eine Kombination aus Objekten mit und ohne S3 Object Lock-Aufbewahrungseinstellungen enthalten.

Aufbewahrungseinstellungen auf Objektebene werden mithilfe der S3 REST-API angegeben. Die Aufbewahrungseinstellungen für ein Objekt überschreiben alle Standardaufbewahrungseinstellungen für den Bucket.

Sie können für jedes Objekt die folgenden Einstellungen festlegen:

- **Aufbewahrungsmodus**: Entweder COMPLIANCE oder GOVERNANCE.
- **Aufbewahrungsdatum**: Ein Datum, das angibt, wie lange die Objektversion von StorageGRID aufbewahrt werden muss.
  - Wenn das Aufbewahrungsdatum im COMPLIANCE-Modus in der Zukunft liegt, kann das Objekt zwar abgerufen, aber nicht geändert oder gelöscht werden. Das Aufbewahrungsdatum kann verlängert werden, es kann jedoch nicht verkürzt oder entfernt werden.
  - Im GOVERNANCE-Modus können Benutzer mit Sonderberechtigung die Einstellung „Aufbewahren bis Datum“ umgehen. Sie können eine Objektversion löschen, bevor ihre Aufbewahrungsfrist abgelaufen ist. Sie können das Aufbewahrungsdatum auch verlängern, verkürzen oder sogar entfernen.
- **Rechtliche Sperre**: Durch Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise müssen Sie möglicherweise ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht, rechtlich sperren. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie ausdrücklich aufgehoben wird.

  Die Einstellung für die rechtliche Aufbewahrung eines Objekts ist unabhängig vom Aufbewahrungsmodus und dem Aufbewahrungsdatum. Wenn eine Objektversion einer rechtlichen Sperre unterliegt, kann niemand diese Version löschen.

Um S3 Object Lock-Einstellungen anzugeben, wenn Sie einem Bucket eine Objektversion hinzufügen, führen Sie einen"PutObject" ,"Objekt kopieren" , oder"CreateMultipartUpload" Anfrage.

Sie können Folgendes verwenden:

- `x-amz-object-lock-mode`, wobei COMPLIANCE oder GOVERNANCE (Groß-/Kleinschreibung beachten) lauten kann.

  > Wenn Sie angeben `x-amz-object-lock-mode` müssen Sie außerdem angeben `x-amz-object-lock-retain-until-date` .

- `x-amz-object-lock-retain-until-date`
  - Der Wert für das Retain-until-Datum muss das Format haben `2020-08-10T21:46:00Z` . Sekundenbruchteile sind zulässig, es bleiben jedoch nur 3 Dezimalstellen erhalten (Millisekundengenauigkeit). Andere ISO 8601-Formate sind nicht zulässig.
  - Das Aufbewahrungsdatum muss in der Zukunft liegen.
- `x-amz-object-lock-legal-hold`

  Wenn die rechtliche Sperre aktiviert ist (Groß-/Kleinschreibung beachten), wird das Objekt einer rechtlichen Sperre unterzogen. Wenn die rechtliche Sperre deaktiviert ist, wird keine rechtliche Sperre verhängt. Jeder andere Wert führt zu einem 400 Bad Request (InvalidArgument)-Fehler.

Wenn Sie einen dieser Anforderungsheader verwenden, beachten Sie die folgenden Einschränkungen:

- Der `Content-MD5` Anforderungsheader ist erforderlich, falls vorhanden `x-amz-object-lock-*` Der Anforderungsheader ist in der PutObject-Anforderung vorhanden. `Content-MD5` ist für CopyObject oder

CreateMultipartUpload nicht erforderlich.

- Wenn für den Bucket die S3-Objektsperre nicht aktiviert ist und ein `x-amz-object-lock-*` Wenn kein Anforderungsheader vorhanden ist, wird der Fehler „400 Bad Request (InvalidRequest)“ zurückgegeben.
- Die PutObject-Anforderung unterstützt die Verwendung von `x-amz-storage-class: REDUCED_REDUNDANCY` um dem AWS-Verhalten zu entsprechen. Wenn jedoch ein Objekt in einen Bucket mit aktivierter S3-Objektsperre aufgenommen wird, führt StorageGRID immer eine Aufnahme mit doppeltem Commit durch.
- Eine nachfolgende GET- oder HeadObject-Versionsantwort enthält die Header `x-amz-object-lock-mode` , `x-amz-object-lock-retain-until-date` , Und `x-amz-object-lock-legal-hold` , sofern konfiguriert und der Absender der Anfrage über die richtige `s3:Get*` Berechtigungen.

Sie können die `s3:object-lock-remaining-retention-days` Richtlinienbedingungsschlüssel, um die minimal und maximal zulässigen Aufbewahrungsfristen für Ihre Objekte zu begrenzen.

So aktualisieren Sie die Aufbewahrungseinstellungen für ein Objekt

Wenn Sie die Einstellungen für die gesetzliche Aufbewahrungspflicht oder die Aufbewahrungsdauer für eine vorhandene Objektversion aktualisieren müssen, können Sie die folgenden Vorgänge für die Objektunterressource ausführen:

- `PutObjectLegalHold`

  Wenn der neue Wert für die rechtliche Sperre EIN ist, wird das Objekt einer rechtlichen Sperre unterzogen. Wenn der Legal-Hold-Wert auf „AUS“ gesetzt ist, wird der Legal Hold aufgehoben.

- `PutObjectRetention`
  - Der Moduswert kann COMPLIANCE oder GOVERNANCE sein (Groß-/Kleinschreibung beachten).
  - Der Wert für das Retain-until-Datum muss das Format haben `2020-08-10T21:46:00Z` . Sekundenbruchteile sind zulässig, es bleiben jedoch nur 3 Dezimalstellen erhalten (Millisekundengenauigkeit). Andere ISO 8601-Formate sind nicht zulässig.
  - Wenn für eine Objektversion ein vorhandenes Aufbewahrungsdatum vorhanden ist, können Sie dieses nur erhöhen. Der neue Wert muss in der Zukunft liegen.

So verwenden Sie den GOVERNANCE-Modus

Benutzer mit der `s3:BypassGovernanceRetention` Die Berechtigung kann die aktiven Aufbewahrungseinstellungen eines Objekts umgehen, das den GOVERNANCE-Modus verwendet. Alle DELETE- oder PutObjectRetention-Vorgänge müssen Folgendes enthalten: `x-amz-bypass-governance-retention:true` Anforderungsheader. Diese Benutzer können die folgenden zusätzlichen Vorgänge ausführen:

- Führen Sie die Vorgänge „DeleteObject“ oder „DeleteObjects“ aus, um eine Objektversion zu löschen, bevor ihre Aufbewahrungsfrist abgelaufen ist.

  Objekte, die einer rechtlichen Sperre unterliegen, können nicht gelöscht werden. Die rechtliche Sperre muss deaktiviert sein.

- Führen Sie PutObjectRetention-Vorgänge durch, die den Modus einer Objektversion von GOVERNANCE in COMPLIANCE ändern, bevor die Aufbewahrungsfrist des Objekts abgelaufen ist.

  Ein Wechsel des Modus von COMPLIANCE zu GOVERNANCE ist niemals zulässig.

- Führen Sie PutObjectRetention-Vorgänge durch, um die Aufbewahrungsdauer einer Objektversion zu erhöhen, zu verringern oder zu entfernen.

Ähnliche Informationen

- "Verwalten von Objekten mit S3 Object Lock"
- "Verwenden Sie S3 Object Lock, um Objekte beizubehalten"
- "Amazon Simple Storage Service-Benutzerhandbuch: Sperren von Objekten"

Erstellen einer S3-Lebenszykluskonfiguration

Sie können eine S3-Lebenszykluskonfiguration erstellen, um zu steuern, wann bestimmte Objekte aus dem StorageGRID System gelöscht werden.

Das einfache Beispiel in diesem Abschnitt veranschaulicht, wie eine S3-Lebenszykluskonfiguration steuern kann, wann bestimmte Objekte aus bestimmten S3-Buckets gelöscht werden (ablaufen). Das Beispiel in diesem Abschnitt dient nur zur Veranschaulichung. Ausführliche Informationen zum Erstellen von S3-Lebenszykluskonfigurationen finden Sie unter "Amazon Simple Storage Service-Benutzerhandbuch: Objekt-Lebenszyklusverwaltung" . Beachten Sie, dass StorageGRID nur Ablaufaktionen unterstützt, keine Übergangsaktionen.

Was ist eine Lebenszykluskonfiguration?

Eine Lebenszykluskonfiguration ist ein Satz von Regeln, die auf die Objekte in bestimmten S3-Buckets angewendet werden. Jede Regel gibt an, welche Objekte betroffen sind und wann diese Objekte ablaufen (an einem bestimmten Datum oder nach einer bestimmten Anzahl von Tagen).

StorageGRID unterstützt bis zu 1.000 Lebenszyklusregeln in einer Lebenszykluskonfiguration. Jede Regel kann die folgenden XML-Elemente enthalten:

- Ablauf: Löschen Sie ein Objekt, wenn ein bestimmtes Datum erreicht ist oder wenn eine bestimmte Anzahl von Tagen ab dem Zeitpunkt der Aufnahme des Objekts abgelaufen ist.
- NoncurrentVersionExpiration: Löschen Sie ein Objekt, wenn eine angegebene Anzahl von Tagen erreicht ist, beginnend mit dem Zeitpunkt, an dem das Objekt nicht mehr aktuell ist.
- Filter (Präfix, Tag)
- Status
- AUSWEIS

Jedes Objekt folgt den Aufbewahrungseinstellungen entweder eines S3-Bucket-Lebenszyklus oder einer ILM-Richtlinie. Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Aktionen zum Ablauf des Lebenszyklus die ILM-Richtlinie für Objekte, die dem Bucket-Lebenszyklusfilter entsprechen. Objekte, die nicht dem Bucket-Lebenszyklusfilter entsprechen, verwenden die Aufbewahrungseinstellungen der ILM-Richtlinie. Wenn ein Objekt einem Bucket-Lebenszyklusfilter entspricht und keine Ablaufaktionen explizit angegeben sind, werden die Aufbewahrungseinstellungen der ILM-Richtlinie nicht verwendet und es wird davon ausgegangen, dass Objektversionen für immer aufbewahrt werden. Sehen "Beispielprioritäten für den S3-Bucket-Lebenszyklus und die ILM-Richtlinie" .

Dies kann dazu führen, dass ein Objekt aus dem Raster entfernt wird, obwohl die Platzierungsanweisungen in einer ILM-Regel weiterhin für das Objekt gelten. Oder ein Objekt kann auf dem Raster verbleiben, auch wenn alle ILM-Platzierungsanweisungen für das Objekt abgelaufen sind. Weitere Informationen finden Sie unter "Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts" .

Die Bucket-Lebenszykluskonfiguration kann mit Buckets verwendet werden, bei denen S3 Object Lock aktiviert ist. Für ältere konforme Buckets wird die Bucket-Lebenszykluskonfiguration jedoch nicht unterstützt.

StorageGRID unterstützt die Verwendung der folgenden Bucket-Operationen zur Verwaltung von Lebenszykluskonfigurationen:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Lebenszykluskonfiguration erstellen

Als ersten Schritt beim Erstellen einer Lebenszykluskonfiguration erstellen Sie eine JSON-Datei, die eine oder mehrere Regeln enthält. Diese JSON-Datei enthält beispielsweise die folgenden drei Regeln:

1. Regel 1 gilt nur für Objekte, die dem Präfix entsprechen `category1` / und die haben eine `key2` Wert von `tag2` . Der `Expiration` Der Parameter gibt an, dass Objekte, die dem Filter entsprechen, am 22. August 2020 um Mitternacht ablaufen.
2. Regel 2 gilt nur für Objekte, die dem Präfix entsprechen `category2` /. Der `Expiration` Der Parameter gibt an, dass Objekte, die dem Filter entsprechen, 100 Tage nach ihrer Aufnahme ablaufen.

   Regeln, die eine Anzahl von Tagen angeben, beziehen sich auf den Zeitpunkt der Aufnahme des Objekts. Wenn das aktuelle Datum das Aufnahmedatum plus die Anzahl der Tage überschreitet, werden einige Objekte möglicherweise aus dem Bucket entfernt, sobald die Lebenszykluskonfiguration angewendet wird.

3. Regel 3 gilt nur für Objekte, die dem Präfix entsprechen `category3` /. Der `Expiration` Der Parameter gibt an, dass alle nicht aktuellen Versionen übereinstimmender Objekte 50 Tage, nachdem sie nicht mehr aktuell sind, ablaufen.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Lebenszykluskonfiguration auf Bucket anwenden

Nachdem Sie die Lebenszyklus-Konfigurationsdatei erstellt haben, wenden Sie sie auf einen Bucket an, indem Sie eine PutBucketLifecycleConfiguration-Anforderung senden.

Diese Anfrage wendet die Lebenszykluskonfiguration in der Beispieldatei auf Objekte in einem Bucket namens `testbucket` .

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Um zu überprüfen, ob eine Lebenszykluskonfiguration erfolgreich auf den Bucket angewendet wurde, senden Sie eine GetBucketLifecycleConfiguration-Anforderung. Beispiel:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Eine erfolgreiche Antwort listet die Lebenszykluskonfiguration auf, die Sie gerade angewendet haben.

Überprüfen Sie, ob das Ablaufdatum des Bucket-Lebenszyklus für das Objekt gilt

Sie können beim Ausgeben einer PutObject-, HeadObject- oder GetObject-Anforderung feststellen, ob eine Ablaufregel in der Lebenszykluskonfiguration auf ein bestimmtes Objekt zutrifft. Wenn eine Regel zutrifft, enthält die Antwort eine `Expiration` Parameter, der angibt, wann das Objekt abläuft und welche Ablaufregel erfüllt wurde.

> Da der Bucket-Lebenszyklus ILM außer Kraft setzt, `expiry-date` angezeigt wird das tatsächliche Datum, an dem das Objekt gelöscht wird. Weitere Informationen finden Sie unter "So wird die Objektaufbewahrung bestimmt" .

Beispielsweise wurde diese PutObject-Anforderung am 22. Juni 2020 ausgegeben und platziert ein Objekt in der `testbucket` Eimer.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

Die Erfolgsantwort gibt an, dass das Objekt in 100 Tagen (01. Oktober 2020) abläuft und dass es Regel 2 der Lebenszykluskonfiguration entspricht.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Beispielsweise wurde diese HeadObject-Anforderung verwendet, um Metadaten für dasselbe Objekt im Testbucket-Bucket abzurufen.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

Die Erfolgsantwort enthält die Metadaten des Objekts und gibt an, dass das Objekt in 100 Tagen abläuft und Regel 2 entspricht.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Für Buckets mit aktivierter Versionierung gilt: `x-amz-expiration` Der Antwortheader gilt nur für aktuelle Versionen von Objekten.

Empfehlungen zur Implementierung der S3 REST API

Sie sollten diese Empfehlungen befolgen, wenn Sie die S3 REST-API zur Verwendung mit StorageGRID implementieren.

Empfehlungen für HEADs zu nicht vorhandenen Objekten

Wenn Ihre Anwendung routinemäßig prüft, ob ein Objekt an einem Pfad existiert, an dem Sie das Objekt nicht erwarten, sollten Sie die Option "Verfügbar" verwenden."Konsistenz" . Sie sollten beispielsweise die Konsistenz „Verfügbar“ verwenden, wenn Ihre Anwendung einen HEAD für einen Speicherort vor dem PUT anwendet.

Andernfalls kann es vorkommen, dass Sie, wenn der HEAD-Vorgang das Objekt nicht findet, eine große Anzahl interner Serverfehler vom Typ 500 erhalten, wenn zwei oder mehr Speicherknoten am selben Standort nicht verfügbar sind oder ein Remote-Standort nicht erreichbar ist.

Sie können die "Verfügbare" Konsistenz für jeden Bucket mithilfe der"PUT Bucket-Konsistenz" Anfrage, oder

Sie können die Konsistenz im Anfrageheader für eine einzelne API-Operation angeben.

Empfehlungen für Objektschlüssel

Befolgen Sie diese Empfehlungen für Objektschlüsselnamen, basierend auf dem Zeitpunkt der ersten Erstellung des Buckets.

Buckets, die in StorageGRID 11.4 oder früher erstellt wurden

- Verwenden Sie keine zufälligen Werte als die ersten vier Zeichen der Objektschlüssel. Dies steht im Gegensatz zur früheren AWS-Empfehlung für Schlüsselpräfixe. Verwenden Sie stattdessen nicht zufällige, nicht eindeutige Präfixe, wie etwa `image` .
- Wenn Sie der früheren AWS-Empfehlung folgen, zufällige und eindeutige Zeichen in Schlüsselpräfixen zu verwenden, stellen Sie den Objektschlüsseln einen Verzeichnisnamen voran. Das heißt, verwenden Sie dieses Format:

  `mybucket/mydir/f8e3-image3132.jpg`

  Anstelle dieses Formats:

  `mybucket/f8e3-image3132.jpg`

In StorageGRID 11.4 oder höher erstellte Buckets

Eine Einschränkung der Objektschlüsselnamen zur Einhaltung der Best Practices für die Leistung ist nicht erforderlich. In den meisten Fällen können Sie für die ersten vier Zeichen von Objektschlüsselnamen zufällige Werte verwenden.

Eine Ausnahme hiervon stellt ein S3-Workload dar, der kontinuierlich alle Objekte nach kurzer Zeit entfernt. Um die Auswirkungen auf die Leistung in diesem Anwendungsfall zu minimieren, variieren Sie alle paar tausend Objekte einen führenden Teil des Schlüsselnamens mit etwas wie dem Datum. Nehmen wir beispielsweise an, dass ein S3-Client normalerweise 2.000 Objekte/Sekunde schreibt und die ILM- oder Bucket-Lebenszyklusrichtlinie alle Objekte nach drei Tagen entfernt. Um die Auswirkungen auf die Leistung zu minimieren, können Sie Schlüssel nach einem Muster wie diesem benennen: `/mybucket/mydir/`*`yyyymmddhhmmss-random_UUID`*`.jpg`

Empfehlungen für „Range Reads“

Wenn die"globale Option zum Komprimieren gespeicherter Objekte" aktiviert 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.

Unterstützung für Amazon S3 REST API

Details zur S3 REST API-Implementierung

Das StorageGRID -System implementiert die Simple Storage Service API (API-Version 2006-03-01) mit Unterstützung für die meisten Vorgänge und mit einigen Einschränkungen. Sie müssen die Implementierungsdetails verstehen, wenn Sie S3 REST API-Clientanwendungen integrieren.

Das StorageGRID -System unterstützt sowohl Anfragen im virtuellen gehosteten Stil als auch Anfragen im Pfadstil.

Datumsverarbeitung

Die StorageGRID -Implementierung der S3 REST API unterstützt nur gültige HTTP-Datumsformate.

Das StorageGRID -System unterstützt nur gültige HTTP-Datumsformate für Header, die Datumswerte akzeptieren. Der Zeitanteil des Datums kann im Format Greenwich Mean Time (GMT) oder im Format Universal Coordinated Time (UTC) ohne Zeitzonenverschiebung angegeben werden (+0000 muss angegeben werden). Wenn Sie die `x-amz-date` Header in Ihrer Anfrage, überschreibt es alle im Date-Anforderungsheader angegebenen Werte. Bei Verwendung von AWS Signature Version 4 ist die `x-amz-date` Der Header muss in der signierten Anfrage vorhanden sein, da der Datumsheader nicht unterstützt wird.

Allgemeine Anforderungsheader

Das StorageGRID -System unterstützt die gemeinsamen Anforderungsheader, die definiert sind durch "Amazon Simple Storage Service API-Referenz: Allgemeine Anforderungsheader" , mit einer Ausnahme.

Anforderungsheader	Durchführung
Genehmigung	Volle Unterstützung für AWS Signature Version 2 Unterstützung für AWS Signature Version 4, mit folgenden Ausnahmen: • Wenn Sie den tatsächlichen Nutzlastprüfsummenwert in `x-amz-content-sha256` wird der Wert ohne Validierung akzeptiert, als ob der Wert `UNSIGNED-PAYLOAD` für den Header vorgesehen war. Wenn Sie eine `x-amz-content-sha256` Header-Wert, der impliziert `aws-chunked` Streaming (z. B. STREAMING-AWS4-HMAC-SHA256-PAYLOAD), werden die Chunk-Signaturen nicht anhand der Chunk-Daten überprüft.
x-amz-Sicherheitstoken	Nicht implementiert. Rückgaben `XNotImplemented` .

Allgemeine Antwortheader

Das StorageGRID -System unterstützt alle gängigen Antwortheader, die in der *Simple Storage Service API Reference* definiert sind, mit einer Ausnahme.

Antwortheader	Durchführung
x-amz-id-2	Nicht verwendet

Authentifizieren von Anfragen

Das StorageGRID -System unterstützt sowohl authentifizierten als auch anonymen Zugriff auf Objekte mithilfe der S3-API.

Die S3-API unterstützt Signature Version 2 und Signature Version 4 zur Authentifizierung von S3-API-Anfragen.

Authentifizierte Anfragen müssen mit Ihrer Zugriffsschlüssel-ID und Ihrem geheimen Zugriffsschlüssel signiert werden.

Das StorageGRID -System unterstützt zwei Authentifizierungsmethoden: HTTP `Authorization` Header und Verwendung von Abfrageparametern.

Verwenden Sie den HTTP-Autorisierungsheader

Das HTTP `Authorization` Der Header wird von allen S3-API-Operationen verwendet, außer von anonymen Anfragen, sofern dies durch die Bucket-Richtlinie zulässig ist. Der `Authorization` Der Header enthält alle erforderlichen Signaturinformationen zur Authentifizierung einer Anfrage.

Verwenden von Abfrageparametern

Sie können Abfrageparameter verwenden, um einer URL Authentifizierungsinformationen hinzuzufügen. Dies wird als Vorsignierung der URL bezeichnet und kann verwendet werden, um vorübergehenden Zugriff auf bestimmte Ressourcen zu gewähren. Benutzer mit der vorsignierten URL müssen den geheimen Zugriffsschlüssel nicht kennen, um auf die Ressource zuzugreifen. Dadurch können Sie Dritten eingeschränkten Zugriff auf eine Ressource gewähren.

Vorgänge für den Dienst

Das StorageGRID -System unterstützt die folgenden Vorgänge für den Dienst.

Betrieb	Durchführung
Buckets auflisten (früher GET-Dienst genannt)	Implementiert mit dem gesamten Amazon S3 REST API-Verhalten. Änderungen vorbehalten.
GET-Speichernutzung	Das StorageGRID"GET-Speichernutzung" Die Anfrage gibt Auskunft über die Gesamtmenge des von einem Konto und jedem mit dem Konto verknüpften Bucket verwendeten Speichers. Dies ist eine Operation für den Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter(`?x-ntap-sg-usage`) hinzugefügt.

Betrieb	Durchführung
OPTIONEN /	Clientanwendungen können `OPTIONS /` Anfragen an den S3-Port eines Speicherknotens, ohne S3-Authentifizierungsdaten anzugeben, um festzustellen, ob der Speicherknoten verfügbar ist. Sie können diese Anfrage zur Überwachung verwenden oder um externen Lastenausgleichsmodulen zu ermöglichen, zu erkennen, wenn ein Speicherknoten ausgefallen ist.

Operationen an Buckets

Das StorageGRID -System unterstützt maximal 5.000 Buckets für jedes S3-Mandantenkonto.

Jedes Raster kann maximal 100.000 Buckets enthalten.

Um 5.000 Buckets zu unterstützen, muss jeder Speicherknoten im Grid über mindestens 64 GB RAM verfügen.

Die Einschränkungen für Bucket-Namen folgen den regionalen Einschränkungen des AWS-US-Standards, Sie sollten sie jedoch zusätzlich auf DNS-Namenskonventionen beschränken, um Anfragen im virtuellen S3-Hosting-Stil zu unterstützen.

Weitere Informationen finden Sie im Folgenden:

- "Amazon Simple Storage Service-Benutzerhandbuch: Bucket-Kontingente, Einschränkungen und Begrenzungen"
- "Konfigurieren von S3-Endpunktdomänennamen"

Die Operationen ListObjects (GET Bucket) und ListObjectVersions (GET Bucket-Objektversionen) unterstützen StorageGRID"Konsistenzwerte" .

Sie können überprüfen, ob Aktualisierungen der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind. Sehen "GET Bucket – Letzte Zugriffszeit" .

Die folgende Tabelle beschreibt, wie StorageGRID S3 REST API-Bucket-Operationen implementiert. Um diese Vorgänge auszuführen, müssen die erforderlichen Zugangsdaten für das Konto angegeben werden.

Betrieb	Durchführung
Bucket erstellen	Erstellt einen neuen Bucket. Indem Sie den Bucket erstellen, werden Sie zum Bucket-Eigentümer. • Bucket-Namen müssen den folgenden Regeln entsprechen: ◦ Muss in jedem StorageGRID -System eindeutig sein (nicht nur innerhalb des Mandantenkontos). ◦ Muss DNS-kompatibel sein. ◦ Muss mindestens 3 und darf nicht mehr als 63 Zeichen enthalten. ◦ Kann eine Reihe von einem oder mehreren Labels sein, wobei benachbarte Labels durch einen Punkt getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten. ◦ Darf nicht wie eine IP-Adresse im Textformat aussehen. ◦ In Anfragen im virtuell gehosteten Stil sollten keine Punkte verwendet werden. Punkte verursachen Probleme bei der Überprüfung des Platzhalterzertifikats des Servers. • Standardmäßig werden Buckets im `us-east-1` Region; Sie können jedoch die `LocationConstraint` Anforderungselement im Anforderungstext, um eine andere Region anzugeben. Bei Verwendung der `LocationConstraint` Element müssen Sie den genauen Namen einer Region angeben, die mit dem Grid Manager oder der Grid Management API definiert wurde. Wenden Sie sich an Ihren Systemadministrator, wenn Sie den zu verwendenden Regionsnamen nicht kennen. **Hinweis**: Es tritt ein Fehler auf, wenn Ihre CreateBucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde. • Sie können Folgendes einschließen: `x-amz-bucket-object-lock-enabled` Anforderungsheader zum Erstellen eines Buckets mit aktivierter S3-Objektsperre. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" . Sie müssen S3 Object Lock aktivieren, wenn Sie den Bucket erstellen. Sie können die S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde. S3 Object Lock erfordert eine Bucket-Versionierung, die automatisch aktiviert wird, wenn Sie den Bucket erstellen.
Bucket löschen	Löscht den Bucket.
BucketCors löschen	Löscht die CORS-Konfiguration für den Bucket.
DeleteBucketEncryption	Löscht die Standardverschlüsselung aus dem Bucket. Vorhandene verschlüsselte Objekte bleiben verschlüsselt, aber alle neuen Objekte, die dem Bucket hinzugefügt werden, werden nicht verschlüsselt.

Betrieb	Durchführung
DeleteBucketLifecycle	Löscht die Lebenszykluskonfiguration aus dem Bucket. Sehen "Erstellen einer S3-Lebenszykluskonfiguration" .
DeleteBucketPolicy	Löscht die an den Bucket angehängte Richtlinie.
DeleteBucketReplication	Löscht die an den Bucket angehängte Replikationskonfiguration.
BucketTagging löschen	Verwendet die `tagging` Unterressource zum Entfernen aller Tags aus einem Bucket. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag mit einem ihm zugewiesenen Wert. Geben Sie keine DeleteBucketTagging-Anforderung aus, wenn ein `NTAP-SG-ILM-BUCKET-TAG` Eimer-Tag. Senden Sie stattdessen eine PutBucketTagging-Anfrage mit nur dem `NTAP-SG-ILM-BUCKET-TAG` Tag und sein zugewiesener Wert, um alle anderen Tags aus dem Bucket zu entfernen. Verändern oder entfernen Sie nicht die `NTAP-SG-ILM-BUCKET-TAG` Eimer-Tag.
GetBucketAcl	Gibt eine positive Antwort sowie die ID, den Anzeigenamen und die Berechtigung des Bucket-Eigentümers zurück und gibt damit an, dass der Eigentümer vollen Zugriff auf den Bucket hat.
GetBucketCors	Gibt den `cors` Konfiguration für den Bucket.
GetBucketEncryption	Gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.
GetBucketLifecycleConfiguration (früher GET Bucket-Lebenszyklus genannt)	Gibt die Lebenszykluskonfiguration für den Bucket zurück. Sehen "Erstellen einer S3-Lebenszykluskonfiguration" .
BucketLocation abrufen	Gibt die Region zurück, die mit dem `LocationConstraint` Element in der CreateBucket-Anforderung. Wenn die Region des Buckets `us-east-1` , wird für die Region eine leere Zeichenfolge zurückgegeben.
GetBucketNotificationConfiguration (früher „GET Bucket-Benachrichtigung“ genannt)	Gibt die dem Bucket zugeordnete Benachrichtigungskonfiguration zurück.
GetBucketPolicy	Gibt die dem Bucket zugeordnete Richtlinie zurück.
GetBucketReplication	Gibt die dem Bucket zugeordnete Replikationskonfiguration zurück.

Betrieb	Durchführung
GetBucketTagging	Verwendet die `tagging` Unterressource, um alle Tags für einen Bucket zurückzugeben. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag mit einem ihm zugewiesenen Wert. Ändern oder entfernen Sie dieses Tag nicht.
GetBucketVersioning	Diese Implementierung verwendet die `versioning` Unterressource, um den Versionsstatus eines Buckets zurückzugeben. • *blank*: Die Versionierung wurde nie aktiviert (Bucket ist „Unversioned“) • Aktiviert: Versionierung ist aktiviert • Ausgesetzt: Die Versionsverwaltung war zuvor aktiviert und ist ausgesetzt
GetObjectLockConfiguration	Gibt den Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer des Buckets zurück, sofern konfiguriert. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .
Kopfeimer	Stellt fest, ob ein Bucket vorhanden ist und Sie über die Berechtigung verfügen, darauf zuzugreifen. Dieser Vorgang gibt Folgendes zurück: • `x-ntap-sg-bucket-id`: Die UUID des Buckets im UUID-Format. • `x-ntap-sg-trace-id`: Die eindeutige Trace-ID der zugehörigen Anfrage.
ListObjects und ListObjectsV2 (früher GET Bucket genannt)	Gibt einige oder alle (bis zu 1.000) Objekte in einem Bucket zurück. Die Speicherklasse für Objekte kann einen von zwei Werten haben, auch wenn das Objekt mit dem `REDUCED_REDUNDANCY` Speicherklassenoption: • `STANDARD`, was darauf hinweist, dass das Objekt in einem Speicherpool gespeichert ist, der aus Speicherknoten besteht. • `GLACIER`, was darauf hinweist, dass das Objekt in den vom Cloud Storage Pool angegebenen externen Bucket verschoben wurde. Wenn der Bucket eine große Anzahl gelöschter Schlüssel mit demselben Präfix enthält, kann die Antwort einige `CommonPrefixes` die keine Schlüssel enthalten.
ListObjectVersions (zuvor GET Bucket Object-Versionen genannt)	Mit Lesezugriff auf einen Bucket kann dieser Vorgang mit dem `versions` Die Unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.

Betrieb	Durchführung
PutBucketCors	Legt die CORS-Konfiguration für einen Bucket fest, sodass der Bucket Cross-Origin-Anfragen verarbeiten kann. Cross-Origin Resource Sharing (CORS) ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, Sie verwenden einen S3-Bucket namens `images` zum Speichern von Grafiken. Durch Festlegen der CORS-Konfiguration für die `images` Bucket, können Sie die Anzeige der Bilder in diesem Bucket auf der Website zulassen `http://www.example.com` .
PutBucketEncryption	Legt den Standardverschlüsselungsstatus eines vorhandenen Buckets fest. Wenn die Verschlüsselung auf Bucket-Ebene aktiviert ist, werden alle neuen Objekte, die dem Bucket hinzugefügt werden, verschlüsselt. StorageGRID unterstützt serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln. Wenn Sie die serverseitige Verschlüsselungskonfigurationsregel angeben, legen Sie die `SSEAlgorithm` Parameter auf `AES256` und verwenden Sie nicht die `KMSMasterKeyID` Parameter. Die Standardverschlüsselungskonfiguration des Buckets wird ignoriert, wenn die Objekt-Upload-Anforderung bereits eine Verschlüsselung angibt (d. h. wenn die Anforderung die `x-amz-server-side-encryption-*` Anforderungsheader).
PutBucketLifecycleConfiguration (früher PUT Bucket-Lebenszyklus genannt)	Erstellt eine neue Lebenszykluskonfiguration für den Bucket oder ersetzt eine vorhandene Lebenszykluskonfiguration. StorageGRID unterstützt bis zu 1.000 Lebenszyklusregeln in einer Lebenszykluskonfiguration. Jede Regel kann die folgenden XML-Elemente enthalten: • Ablauf (Tage, Datum, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filter (Präfix, Tag) • Status • AUSWEIS StorageGRID unterstützt diese Aktionen nicht: • AbbruchUnvollständigMehrteiliger Upload • Übergang Sehen "Erstellen einer S3-Lebenszykluskonfiguration" . Informationen dazu, wie die Ablaufaktion in einem Bucket-Lebenszyklus mit ILM-Platzierungsanweisungen interagiert, finden Sie unter"Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts" . **Hinweis**: Die Bucket-Lebenszykluskonfiguration kann mit Buckets verwendet werden, bei denen S3 Object Lock aktiviert ist, die Bucket-Lebenszykluskonfiguration wird jedoch für ältere konforme Buckets nicht unterstützt.

Betrieb	Durchführung

PutBucketNotificationConfiguration
 	
(früher PUT Bucket-Benachrichtigung genannt)
	Konfiguriert Benachrichtigungen für den Bucket mithilfe der im Anforderungstext enthaltenen Benachrichtigungskonfigurations-XML. Sie sollten sich der folgenden Implementierungsdetails bewusst sein:
	
	• StorageGRID unterstützt Amazon Simple Notification Service (Amazon SNS) oder Kafka-Themen als Ziele. Simple Queue Service (SQS) oder Amazon Lambda-Endpunkte werden nicht unterstützt.
	• Das Ziel für Benachrichtigungen muss als URN eines StorageGRID Endpunkts angegeben werden. Endpunkte können mit dem Tenant Manager oder der Tenant Management API erstellt werden.
	
	Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ist. Wenn der Endpunkt nicht existiert, wird ein `400 Bad Request` Fehler wird mit dem Code zurückgegeben `InvalidArgument` .
	
	• Für die folgenden Ereignistypen können Sie keine Benachrichtigung konfigurieren. Diese Ereignistypen werden **nicht** unterstützt.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das standardmäßige JSON-Format, mit der Ausnahme, dass sie einige Schlüssel nicht enthalten und für andere bestimmte Werte verwenden, wie in der folgenden Liste gezeigt:
	◦ **Ereignisquelle**
	`sgws:s3`
	◦ **awsRegion**
	nicht enthalten
	◦ **x-amz-id-2**
	nicht enthalten
	◦ **arn**
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Legt die dem Bucket zugeordnete Richtlinie fest. Sehen "Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien" .

Betrieb	Durchführung
PutBucketReplication	Konfiguriert"StorageGRID CloudMirror-Replikation" für den Bucket unter Verwendung der im Anforderungstext bereitgestellten XML-Replikationskonfiguration. Bei der CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten: • StorageGRID unterstützt nur V1 der Replikationskonfiguration. Dies bedeutet, dass StorageGRID die Verwendung des `Filter` Element für Regeln und befolgt V1-Konventionen zum Löschen von Objektversionen. Weitere Einzelheiten finden Sie unter "Amazon Simple Storage Service-Benutzerhandbuch: Replikationskonfiguration" . • Die Bucket-Replikation kann für versionierte oder nicht versionierte Buckets konfiguriert werden. • Sie können in jeder Regel der XML-Replikationskonfiguration einen anderen Ziel-Bucket angeben. Ein Quell-Bucket kann in mehr als einen Ziel-Bucket repliziert werden. • Ziel-Buckets müssen als URN von StorageGRID -Endpunkten angegeben werden, wie im Tenant Manager oder der Tenant Management API angegeben. Sehen "Konfigurieren der CloudMirror-Replikation" . Der Endpunkt muss vorhanden sein, damit die Replikationskonfiguration erfolgreich ist. Wenn der Endpunkt nicht existiert, schlägt die Anfrage fehl, da `400 Bad Request` Die Fehlermeldung lautet: `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • Sie müssen kein `Role` im Konfigurations-XML. Dieser Wert wird von StorageGRID nicht verwendet und wird ignoriert, wenn er übermittelt wird. • Wenn Sie die Speicherklasse aus der Konfigurations-XML weglassen, verwendet StorageGRID die `STANDARD` Speicherklasse standardmäßig. • Wenn Sie ein Objekt aus dem Quell-Bucket oder den Quell-Bucket selbst löschen, ist das regionsübergreifende Replikationsverhalten wie folgt: ◦ Wenn Sie das Objekt oder den Bucket löschen, bevor es repliziert wurde, wird das Objekt/der Bucket nicht repliziert und Sie werden nicht benachrichtigt. ◦ Wenn Sie das Objekt oder den Bucket nach der Replikation löschen, folgt StorageGRID dem standardmäßigen Löschverhalten von Amazon S3 für V1 der regionsübergreifenden Replikation.

Betrieb	Durchführung
PutBucketTagging	Verwendet die `tagging` Unterressource zum Hinzufügen oder Aktualisieren eines Satzes von Tags für einen Bucket. Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen: • Sowohl StorageGRID als auch Amazon S3 unterstützen bis zu 50 Tags für jeden Bucket. • Mit einem Bucket verknüpfte Tags müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein. • Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. • Bei Schlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag mit einem ihm zugewiesenen Wert. Stellen Sie sicher, dass die `NTAP-SG-ILM-BUCKET-TAG` Das Bucket-Tag ist mit dem zugewiesenen Wert in allen PutBucketTagging-Anfragen enthalten. Ändern oder entfernen Sie dieses Tag nicht. **Hinweis**: Dieser Vorgang überschreibt alle aktuellen Tags, die der Bucket bereits hat. Wenn vorhandene Tags aus dem Set weggelassen werden, werden diese Tags für den Bucket entfernt.
PutBucketVersioning	Verwendet die `versioning` Unterressource zum Festlegen des Versionsstatus eines vorhandenen Buckets. Sie können den Versionsstatus mit einem der folgenden Werte festlegen: • Aktiviert: Aktiviert die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Versions-ID. • Angehalten: Deaktiviert die Versionierung für die Objekte im Bucket. Alle zum Bucket hinzugefügten Objekte erhalten die Versions-ID `null` .
PutObjectLockConfiguration	Konfiguriert oder entfernt den Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer des Buckets. Wenn die Standardaufbewahrungsfrist geändert wird, bleibt das Aufbewahrungsdatum vorhandener Objektversionen gleich und wird nicht anhand der neuen Standardaufbewahrungsfrist neu berechnet. Sehen"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" für detaillierte Informationen.

Operationen an Objekten

Operationen an Objekten

In diesem Abschnitt wird beschrieben, wie das StorageGRID -System S3 REST-API-Operationen für Objekte implementiert.

Für alle Objektoperationen gelten folgende Bedingungen:

- StorageGRID"Konsistenzwerte" werden von allen Operationen an Objekten unterstützt, mit Ausnahme der folgenden:
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelectObjectContent
- Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.
- Alle Objekte in einem StorageGRID Bucket sind Eigentum des Bucket-Eigentümers, einschließlich der von einem anonymen Benutzer oder einem anderen Konto erstellten Objekte.
- Auf Datenobjekte, die über Swift in das StorageGRID System aufgenommen werden, kann nicht über S3 zugegriffen werden.

Die folgende Tabelle beschreibt, wie StorageGRID S3 REST API-Objektoperationen implementiert.

Betrieb	Durchführung
Objekt löschen	Multi-Faktor-Authentifizierung (MFA) und der Antwortheader `x-amz-mfa` werden nicht unterstützt. Bei der Verarbeitung einer DeleteObject-Anforderung versucht StorageGRID , alle Kopien des Objekts sofort von allen gespeicherten Standorten zu entfernen. Bei Erfolg gibt StorageGRID sofort eine Antwort an den Client zurück. Wenn nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Speicherort vorübergehend nicht verfügbar ist), stellt StorageGRID die Kopien zur Entfernung in die Warteschlange und zeigt dem Client anschließend den Erfolg an. **Versionierung** Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und die `versionId` Unterressource. Durch die Verwendung dieser Unterressource wird die Version dauerhaft gelöscht. Wenn die `versionId` entspricht einem Löschmarker, der Antwortheader `x-amz-delete-marker` wird zurückgegeben auf `true` . • Wenn ein Objekt gelöscht wird, ohne dass `versionId` Unterressource auf einem Bucket mit aktivierter Versionierung, führt dies zur Generierung einer Löschmarkierung. Der `versionId` für die Löschmarkierung wird mit dem `x-amz-version-id` Antwortheader und der `x-amz-delete-marker` Der Antwortheader wird auf `true` . • Wenn ein Objekt gelöscht wird, ohne dass `versionId` Unterressource auf einem Bucket mit ausgesetzter Versionierung, führt dies zu einer dauerhaften Löschung einer bereits vorhandenen „Null“-Version oder eines „Null“-Löschmarkers und zur Generierung eines neuen „Null“-Löschmarkers. Der `x-amz-delete-marker` Der Antwortheader wird auf `true` . **Hinweis**: In bestimmten Fällen können für ein Objekt mehrere Löschmarkierungen vorhanden sein. Sehen"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" um zu erfahren, wie Sie Objektversionen im GOVERNANCE-Modus löschen.

Betrieb	Durchführung
Objekte löschen (früher „DELETE Multiple Objects“ genannt)	Multi-Faktor-Authentifizierung (MFA) und der Antwortheader `x-amz-mfa` werden nicht unterstützt. In derselben Anforderungsnachricht können mehrere Objekte gelöscht werden. Sehen"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" um zu erfahren, wie Sie Objektversionen im GOVERNANCE-Modus löschen.
DeleteObjectTagging	Verwendet die `tagging` Unterressource zum Entfernen aller Tags von einem Objekt. **Versionierung** Wenn die `versionId` Wenn in der Anforderung kein Abfrageparameter angegeben ist, löscht der Vorgang alle Tags aus der aktuellsten Version des Objekts in einem versionierten Bucket. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "MethodNotAllowed" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .
GetObject	"GetObject"
GetObjectAcl	Wenn die erforderlichen Zugriffsberechtigungen für das Konto bereitgestellt werden, gibt der Vorgang eine positive Antwort sowie die ID, den Anzeigenamen und die Berechtigung des Objektbesitzers zurück, was darauf hinweist, dass der Besitzer vollen Zugriff auf das Objekt hat.
GetObjectLegalHold	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
GetObjectRetention	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
GetObjectTagging	Verwendet die `tagging` Unterressource, um alle Tags für ein Objekt zurückzugeben. **Versionierung** Wenn die `versionId` Wenn in der Anforderung kein Abfrageparameter angegeben ist, gibt der Vorgang alle Tags aus der aktuellsten Version des Objekts in einem versionierten Bucket zurück. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "MethodNotAllowed" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"

Betrieb	Durchführung
PutObject	"PutObject"
Objekt kopieren (früher PUT-Objekt – Kopieren genannt)	"Objekt kopieren"
PutObjectLegalHold	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
PutObjectRetention	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

Betrieb	Durchführung
PutObjectTagging	Verwendet die `tagging` Unterressource zum Hinzufügen einer Reihe von Tags zu einem vorhandenen Objekt. **Objekt-Tag-Grenzwerte** Sie können neuen Objekten beim Hochladen Tags hinzufügen oder Sie können sie vorhandenen Objekten hinzufügen. Sowohl StorageGRID als auch Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Mit einem Objekt verknüpfte Tags müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei Schlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden. **Tag-Updates und Aufnahmeverhalten** Wenn Sie PutObjectTagging verwenden, um die Tags eines Objekts zu aktualisieren, nimmt StorageGRID das Objekt nicht erneut auf. Dies bedeutet, dass die in der entsprechenden ILM-Regel angegebene Option für das Aufnahmeverhalten nicht verwendet wird. Alle durch die Aktualisierung ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Hintergrundprozesse neu ausgewertet wird. Dies bedeutet, dass keine Aktion ausgeführt wird, wenn die ILM-Regel die Option „Streng“ für das Aufnahmeverhalten verwendet und die erforderlichen Objektplatzierungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist. **Konflikte lösen** Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen. **Versionierung** Wenn die `versionId` Wenn in der Anforderung kein Abfrageparameter angegeben ist, fügt der Vorgang der aktuellsten Version des Objekts in einem versionierten Bucket Tags hinzu. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "MethodNotAllowed" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .
SelectObjectContent	"SelectObjectContent"

Verwenden Sie S3 Select

StorageGRID unterstützt die folgenden Amazon S3 Select-Klauseln, Datentypen und

Operatoren für die"SelectObjectContent-Befehl" .

Nicht aufgeführte Artikel werden nicht unterstützt.

Informationen zur Syntax finden Sie unter"SelectObjectContent" . Weitere Informationen zu S3 Select finden Sie im "AWS-Dokumentation für S3 Select" .

Nur Mandantenkonten, bei denen S3 Select aktiviert ist, können SelectObjectContent-Abfragen ausgeben. Siehe die"Überlegungen und Anforderungen zur Verwendung von S3 Select" .

Klauseln

- SELECT-Liste
- FROM-Klausel
- WHERE-Klausel
- LIMIT-Klausel

Datentypen

- bool
- ganze Zahl
- Schnur
- schweben
- Dezimal, numerisch
- Zeitstempel

Betreiber

Logische Operatoren

- UND
- NICHT
- ODER

Vergleichsoperatoren

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- ZWISCHEN

- IN

Mustervergleichsoperatoren

- WIE
- _
- %

Unitäre Operatoren

- IST NULL
- IST NICHT NULL

Mathematische Operatoren

- +
- -
- *
- /
- %

StorageGRID folgt der Priorität des Amazon S3 Select-Operators.

Aggregatfunktionen

- AVG()
- ZÄHLEN(*)
- MAX()
- MIN()
- SUMME()

Bedingte Funktionen

- FALL
- VERSCHMELZEN
- NULLIF

Konvertierungsfunktionen

- CAST (für unterstützten Datentyp)

Datumsfunktionen

- DATE_ADD
- DATE_DIFF
- EXTRAKT
- TO_STRING

- TO_TIMESTAMP
- UTCNOW

Zeichenfolgenfunktionen

- CHAR_LENGTH, CHARACTER_LENGTH
- UNTERE
- TEILZEICHENKETTE
- TRIMMEN
- OBERE

Verwenden Sie serverseitige Verschlüsselung

Durch die serverseitige Verschlüsselung können Sie Ihre ruhenden Objektdaten schützen. StorageGRID verschlüsselt die Daten beim Schreiben des Objekts und entschlüsselt die Daten, wenn Sie auf das Objekt zugreifen.

Wenn Sie serverseitige Verschlüsselung verwenden möchten, können Sie je nach Verwaltung der Verschlüsselungsschlüssel zwischen zwei sich gegenseitig ausschließenden Optionen wählen:

- **SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln)**: Wenn Sie eine S3-Anfrage zum Speichern eines Objekts stellen, verschlüsselt StorageGRID das Objekt mit einem eindeutigen Schlüssel. Wenn Sie eine S3-Anforderung zum Abrufen des Objekts stellen, verwendet StorageGRID den gespeicherten Schlüssel zum Entschlüsseln des Objekts.
- **SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)**: Wenn Sie eine S3-Anfrage zum Speichern eines Objekts stellen, geben Sie Ihren eigenen Verschlüsselungsschlüssel an. Wenn Sie ein Objekt abrufen, geben Sie im Rahmen Ihrer Anfrage denselben Verschlüsselungsschlüssel an. Wenn die beiden Verschlüsselungsschlüssel übereinstimmen, wird das Objekt entschlüsselt und Ihre Objektdaten werden zurückgegeben.

  Während StorageGRID alle Objektverschlüsselungs- und -entschlüsselungsvorgänge verwaltet, müssen Sie die von Ihnen bereitgestellten Verschlüsselungsschlüssel verwalten.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.

> Wenn ein Objekt mit SSE oder SSE-C verschlüsselt ist, werden alle Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

Verwenden Sie SSE

Um ein Objekt mit einem eindeutigen, von StorageGRID verwalteten Schlüssel zu verschlüsseln, verwenden Sie den folgenden Anforderungsheader:

```
x-amz-server-side-encryption
```

Der SSE-Anforderungsheader wird von den folgenden Objektoperationen unterstützt:

- "PutObject"
- "Objekt kopieren"
- "CreateMultipartUpload"

Verwenden Sie SSE-C

Um ein Objekt mit einem eindeutigen Schlüssel zu verschlüsseln, den Sie verwalten, verwenden Sie drei Anforderungsheader:

Anforderungsheader	Beschreibung
`x-amz-server-side-encryption-customer-algorithm`	Geben Sie den Verschlüsselungsalgorithmus an. Der Headerwert muss `AES256`.
`x-amz-server-side-encryption-customer-key`	Geben Sie den Verschlüsselungsschlüssel an, der zum Verschlüsseln oder Entschlüsseln des Objekts verwendet wird. Der Wert für den Schlüssel muss 256 Bit lang und base64-codiert sein.
`x-amz-server-side-encryption-customer-key-MD5`	Geben Sie den MD5-Digest des Verschlüsselungsschlüssels gemäß RFC 1321 an, der verwendet wird, um sicherzustellen, dass der Verschlüsselungsschlüssel fehlerfrei übertragen wurde. Der Wert für den MD5-Digest muss base64-codiert und 128 Bit lang sein.

Die SSE-C-Anforderungsheader werden von den folgenden Objektoperationen unterstützt:

- "GetObject"
- "HeadObject"
- "PutObject"
- "Objekt kopieren"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Überlegungen zur Verwendung der serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)

Beachten Sie vor der Verwendung von SSE-C die folgenden Hinweise:

- Sie müssen https verwenden.

> ⚠ StorageGRID lehnt bei Verwendung von SSE-C alle über HTTP gestellten Anfragen ab. Aus Sicherheitsgründen sollten Sie jeden versehentlich über HTTP gesendeten Schlüssel als gefährdet betrachten. Entsorgen Sie den Schlüssel und drehen Sie ihn entsprechend.

- Der ETag in der Antwort ist nicht der MD5 der Objektdaten.
- Sie müssen die Zuordnung von Verschlüsselungsschlüsseln zu Objekten verwalten. StorageGRID speichert keine Verschlüsselungsschlüssel. Sie sind für die Nachverfolgung des

Verschlüsselungsschlüssels verantwortlich, den Sie für jedes Objekt bereitstellen.

- Wenn für Ihren Bucket die Versionierung aktiviert ist, sollte jede Objektversion über einen eigenen Verschlüsselungsschlüssel verfügen. Sie sind für die Nachverfolgung des für jede Objektversion verwendeten Verschlüsselungsschlüssels verantwortlich.
- Da Sie die Verschlüsselungsschlüssel auf der Clientseite verwalten, müssen Sie auch alle zusätzlichen Sicherheitsvorkehrungen, wie etwa die Schlüsselrotation, auf der Clientseite verwalten.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.

- Wenn für den Bucket eine Cross-Grid-Replikation oder eine CloudMirror-Replikation konfiguriert ist, können Sie keine SSE-C-Objekte aufnehmen. Der Aufnahmevorgang schlägt fehl.

Ähnliche Informationen

"Amazon S3-Benutzerhandbuch: Verwenden der serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)"

Objekt kopieren

Mit der S3 CopyObject-Anforderung können Sie eine Kopie eines Objekts erstellen, das bereits in S3 gespeichert ist. Ein CopyObject-Vorgang ist dasselbe wie die Ausführung von GetObject gefolgt von PutObject.

Konflikte lösen

Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.

Objektgröße

Die maximal *empfohlene* Größe für einen einzelnen PutObject-Vorgang beträgt 5 GiB (5.368.709.120 Bytes). Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie"mehrteiliger Upload" stattdessen.

Die maximal *unterstützte* Größe für einen einzelnen PutObject-Vorgang beträgt 5 TiB (5.497.558.138.880 Bytes).

> Wenn Sie ein Upgrade von StorageGRID 11.6 oder früher durchgeführt haben, wird die Warnung „S3 PUT-Objektgröße zu groß“ ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das 5 GiB überschreitet. Wenn Sie eine Neuinstallation von StorageGRID 11.7 oder 11.8 haben, wird der Alarm in diesem Fall nicht ausgelöst. Um jedoch dem AWS S3-Standard zu entsprechen, werden zukünftige Versionen von StorageGRID keine Uploads von Objekten unterstützen, die größer als 5 GiB sind.

UTF-8-Zeichen in Benutzermetadaten

Wenn eine Anfrage (nicht maskierte) UTF-8-Werte im Schlüsselnamen oder Wert benutzerdefinierter Metadaten enthält, ist das StorageGRID Verhalten undefiniert.

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen, die im Schlüsselnamen oder -wert

benutzerdefinierter Metadaten enthalten sind. Escape-UTF-8-Zeichen werden als ASCII-Zeichen behandelt:

- Anforderungen sind erfolgreich, wenn benutzerdefinierte Metadaten Escape-UTF-8-Zeichen enthalten.
- StorageGRID gibt nicht zurück `x-amz-missing-meta` Header, wenn der interpretierte Wert des Schlüsselnamens oder -werts nicht druckbare Zeichen enthält.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten
- `x-amz-metadata-directive`: Der Standardwert ist `COPY` , wodurch Sie das Objekt und die zugehörigen Metadaten kopieren können.

  Sie können angeben `REPLACE` um die vorhandenen Metadaten beim Kopieren des Objekts zu überschreiben oder die Objektmetadaten zu aktualisieren.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: Der Standardwert ist `COPY` , wodurch Sie das Objekt und alle Tags kopieren können.

  Sie können angeben `REPLACE` um die vorhandenen Tags beim Kopieren des Objekts zu überschreiben oder die Tags zu aktualisieren.

- S3 Object Lock-Anforderungsheader:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Wenn eine Anfrage ohne diese Header gestellt wird, werden die Bucket-Standardaufbewahrungseinstellungen verwendet, um den Objektversionsmodus und das Aufbewahrungsdatum zu berechnen. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .

- SSE-Anforderungsheader:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`

- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

  SehenAnforderungsheader für serverseitige Verschlüsselung

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Wenn Sie ein Objekt kopieren und das Quellobjekt eine Prüfsumme hat, kopiert StorageGRID diesen Prüfsummenwert nicht in das neue Objekt. Dieses Verhalten gilt unabhängig davon, ob Sie versuchen, `x-amz-checksum-algorithm` in der Objektanforderung.

- `x-amz-website-redirect-location`

Speicherklassenoptionen

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und beeinflusst, wie viele Objektkopien StorageGRID erstellt, wenn die entsprechende ILM-Regel Dual Commit oder Balanced verwendet."Aufnahmeoption" .

- `STANDARD`

  (Standard) Gibt einen Dual-Commit-Aufnahmevorgang an, wenn die ILM-Regel die Option „Dual Commit“ verwendet oder wenn die Option „Balanced“ auf die Erstellung von Zwischenkopien zurückgreift.

- `REDUCED_REDUNDANCY`

  Gibt einen Single-Commit-Ingest-Vorgang an, wenn die ILM-Regel die Option „Dual Commit“ verwendet oder wenn die Option „Balanced“ auf die Erstellung von Zwischenkopien zurückgreift.

> ⓘ Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperre aufnehmen, wird die `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-Compliant-Bucket aufnehmen, `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine Dual-Commit-Aufnahme durch, um sicherzustellen, dass die Compliance-Anforderungen erfüllt werden.

Verwenden von x-amz-copy-source in CopyObject

Wenn der Quell-Bucket und -Schlüssel, angegeben in `x-amz-copy-source` Header, unterscheiden sich vom Ziel-Bucket und -Schlüssel, eine Kopie der Quellobjektdaten wird in das Ziel geschrieben.

Wenn Quelle und Ziel übereinstimmen und die `x-amz-metadata-directive` Der Header wird wie folgt angegeben: `REPLACE` , werden die Metadaten des Objekts mit den in der Anfrage angegebenen Metadatenwerten aktualisiert. In diesem Fall nimmt StorageGRID das Objekt nicht erneut auf. Dies hat zwei wichtige Konsequenzen:

- Sie können CopyObject nicht verwenden, um ein vorhandenes Objekt vor Ort zu verschlüsseln oder die Verschlüsselung eines vorhandenen Objekts vor Ort zu ändern. Wenn Sie die `x-amz-server-side-encryption` Kopfzeile oder die `x-amz-server-side-encryption-customer-algorithm` Header, StorageGRID lehnt die Anfrage ab und gibt zurück `XNotImplemented` .
- Die in der entsprechenden ILM-Regel angegebene Option für das Aufnahmeverhalten wird nicht verwendet. Alle durch die Aktualisierung ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Hintergrundprozesse neu ausgewertet wird.

  Dies bedeutet, dass keine Aktion ausgeführt wird, wenn die ILM-Regel die Option „Streng“ für das Aufnahmeverhalten verwendet und die erforderlichen Objektplatzierungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist.

Anforderungsheader für serverseitige Verschlüsselung

Wenn du"Verwenden Sie serverseitige Verschlüsselung" , die von Ihnen bereitgestellten Anforderungsheader hängen davon ab, ob das Quellobjekt verschlüsselt ist und ob Sie das Zielobjekt verschlüsseln möchten.

- Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt ist, müssen Sie die folgenden drei Header in die CopyObject-Anforderung aufnehmen, damit das Objekt entschlüsselt und dann kopiert werden kann:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angeben `AES256` .
  - `x-amz-copy-source-server-side-encryption-customer-key`: Geben Sie den Verschlüsselungsschlüssel an, den Sie beim Erstellen des Quellobjekts angegeben haben.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest an, den Sie beim Erstellen des Quellobjekts angegeben haben.
- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten, schließen Sie die folgenden drei Header ein:
  - `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Geben Sie einen neuen Verschlüsselungsschlüssel für das Zielobjekt an.
  - `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des neuen Verschlüsselungsschlüssels an.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Überlegungen für"Verwendung serverseitiger Verschlüsselung" .

- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen, von StorageGRID (SSE) verwalteten Schlüssel verschlüsseln möchten, fügen Sie diesen Header in die CopyObject-Anforderung ein:
  - `x-amz-server-side-encryption`

> Der `server-side-encryption` Der Wert des Objekts kann nicht aktualisiert werden. Erstellen Sie stattdessen eine Kopie mit einem neuen `server-side-encryption` Wert mit `x-amz-metadata-directive` : `REPLACE` .

Versionierung

Wenn der Quell-Bucket versioniert ist, können Sie die `x-amz-copy-source` Header, um die neueste Version eines Objekts zu kopieren. Um eine bestimmte Version eines Objekts zu kopieren, müssen Sie die zu kopierende Version explizit angeben, indem Sie `versionId` Unterressource. Wenn der Ziel-Bucket versioniert ist, wird die generierte Version im `x-amz-version-id` Antwortheader. Wenn die Versionierung für den Ziel-Bucket ausgesetzt ist, dann `x-amz-version-id` gibt einen „Null“-Wert zurück.

GetObject

Sie können die S3 GetObject-Anforderung verwenden, um ein Objekt aus einem S3-Bucket abzurufen.

GetObject und mehrteilige Objekte

Sie können die `partNumber` Anforderungsparameter zum Abrufen eines bestimmten Teils eines mehrteiligen oder segmentierten Objekts. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, aus wie vielen Teilen das Objekt besteht.

Sie können einstellen `partNumber` auf 1 für segmentierte/mehrteilige Objekte und nicht-segmentierte/nicht-mehrteilige Objekte; jedoch `x-amz-mp-parts-count` Das Antwortelement wird nur für segmentierte oder mehrteilige Objekte zurückgegeben.

UTF-8-Zeichen in Benutzermetadaten

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten. GET-Anfragen für ein Objekt mit Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten geben nicht die `x-amz-missing-meta` Header, wenn der Schlüsselname oder -wert nicht druckbare Zeichen enthält.

Unterstützter Anforderungsheader

Der folgende Anforderungsheader wird unterstützt:

- `x-amz-checksum-mode`: Angeben `ENABLED`

  Der `Range` Header wird nicht unterstützt mit `x-amz-checksum-mode` für GetObject. Wenn Sie `Range` in der Anfrage mit `x-amz-checksum-mode` aktiviert ist, gibt StorageGRID in der Antwort keinen Prüfsummenwert zurück.

Nicht unterstützter Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt und gibt zurück `XNotImplemented` :

- `x-amz-website-redirect-location`

Versionierung

Wenn ein `versionId` Wenn keine Unterressource angegeben ist, ruft der Vorgang die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "Nicht gefunden" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .

Anforderungsheader für die serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)

Verwenden Sie alle drei Header, wenn das Objekt mit einem von Ihnen bereitgestellten eindeutigen Schlüssel verschlüsselt ist.

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des Objekts an.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in"Verwenden Sie serverseitige Verschlüsselung" .

Verhalten von GetObject für Cloud Storage Pool-Objekte

Wenn ein Objekt in einem"Cloud-Speicherpool" , das Verhalten einer GetObject-Anforderung hängt vom Status des Objekts ab. Sehen"HeadObject" für weitere Details.

> Wenn ein Objekt in einem Cloud-Speicherpool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Raster vorhanden sind, versuchen GetObject-Anfragen, Daten aus dem Raster abzurufen, bevor sie aus dem Cloud-Speicherpool abgerufen werden.

Zustand des Objekts	Verhalten von GetObject
In StorageGRID aufgenommenes, aber noch nicht von ILM ausgewertetes Objekt oder Objekt, das in einem herkömmlichen Speicherpool oder mithilfe von Erasure Coding gespeichert ist	`200 OK` Eine Kopie des Objekts wird abgerufen.
Objekt im Cloud-Speicherpool, aber noch nicht in einen nicht abrufbaren Zustand übergegangen	`200 OK` Eine Kopie des Objekts wird abgerufen.
Objekt in einen nicht abrufbaren Zustand überführt	`403 Forbidden` , `InvalidObjectState` Verwenden Sie ein"RestoreObject" Anforderung zum Wiederherstellen des Objekts in einen abrufbaren Zustand.

Zustand des Objekts	Verhalten von GetObject
Objekt wird gerade aus einem nicht abrufbaren Zustand wiederhergestellt	`403 Forbidden` , `InvalidObjectState` Warten Sie, bis die RestoreObject-Anforderung abgeschlossen ist.
Objekt vollständig im Cloud-Speicherpool wiederhergestellt	`200 OK` Eine Kopie des Objekts wird abgerufen.

Mehrteilige oder segmentierte Objekte in einem Cloud-Speicherpool

Wenn Sie ein mehrteiliges Objekt hochgeladen haben oder StorageGRID ein großes Objekt in Segmente aufgeteilt hat, ermittelt StorageGRID , ob das Objekt im Cloud Storage Pool verfügbar ist, indem es eine Teilmenge der Teile oder Segmente des Objekts auswählt. In einigen Fällen kann eine GetObject-Anforderung fälschlicherweise zurückgeben `200 OK` wenn einige Teile des Objekts bereits in einen nicht abrufbaren Zustand überführt wurden oder wenn einige Teile des Objekts noch nicht wiederhergestellt wurden.

In diesen Fällen:

- Die GetObject-Anforderung gibt möglicherweise einige Daten zurück, stoppt jedoch mitten in der Übertragung.
- Eine nachfolgende GetObject-Anforderung könnte `403 Forbidden` .

GetObject und Cross-Grid-Replikation

Wenn Sie"Netzverbund" Und"Cross-Grid-Replikation" für einen Bucket aktiviert ist, kann der S3-Client den Replikationsstatus eines Objekts überprüfen, indem er eine GetObject-Anforderung ausgibt. 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.

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

HeadObject

Sie können die S3 HeadObject-Anforderung verwenden, um Metadaten aus einem Objekt abzurufen, ohne das Objekt selbst zurückzugeben. Wenn das Objekt in einem Cloud-Speicherpool gespeichert ist, können Sie HeadObject verwenden, um den

Übergangszustand des Objekts zu bestimmen.

HeadObject und mehrteilige Objekte

Sie können die `partNumber` Anforderungsparameter zum Abrufen von Metadaten für einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, aus wie vielen Teilen das Objekt besteht.

Sie können einstellen `partNumber` auf 1 für segmentierte/mehrteilige Objekte und nicht-segmentierte/nicht-mehrteilige Objekte; jedoch `x-amz-mp-parts-count` Das Antwortelement wird nur für segmentierte oder mehrteilige Objekte zurückgegeben.

UTF-8-Zeichen in Benutzermetadaten

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten. HEAD-Anfragen für ein Objekt mit Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten geben nicht das `x-amz-missing-meta` Header, wenn der Schlüsselname oder -wert nicht druckbare Zeichen enthält.

Unterstützter Anforderungsheader

Der folgende Anforderungsheader wird unterstützt:

- `x-amz-checksum-mode`

  Der `partNumber` Parameter und `Range` Header werden nicht unterstützt mit `x-amz-checksum-mode` für HeadObject. Wenn Sie sie in die Anfrage aufnehmen mit `x-amz-checksum-mode` aktiviert ist, gibt StorageGRID in der Antwort keinen Prüfsummenwert zurück.

Nicht unterstützter Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt und gibt zurück `XNotImplemented` :

- `x-amz-website-redirect-location`

Versionierung

Wenn ein `versionId` Wenn keine Unterressource angegeben ist, ruft der Vorgang die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "Nicht gefunden" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .

Anforderungsheader für die serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)

Verwenden Sie alle drei Header, wenn das Objekt mit einem von Ihnen bereitgestellten eindeutigen Schlüssel verschlüsselt ist.

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des Objekts an.

Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in"Verwenden Sie serverseitige Verschlüsselung" .

HeadObject-Antworten für Cloud Storage Pool-Objekte

Wenn das Objekt in einem"Cloud-Speicherpool" werden die folgenden Antwortheader zurückgegeben:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Die Antwortheader liefern Informationen über den Status eines Objekts, wenn es in einen Cloud-Speicherpool verschoben, optional in einen nicht abrufbaren Status versetzt und wiederhergestellt wird.

Zustand des Objekts	Antwort auf HeadObject
In StorageGRID aufgenommenes, aber noch nicht von ILM ausgewertetes Objekt oder Objekt, das in einem herkömmlichen Speicherpool oder mithilfe von Erasure Coding gespeichert ist	`200 OK`(Es wird kein spezieller Antwortheader zurückgegeben.)

Objekt im Cloud-Speicherpool, aber noch nicht in einen nicht abrufbaren Zustand übergegangen	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Bis das Objekt in einen nicht abrufbaren Zustand überführt wird, ist der Wert für `expiry-date` ist auf einen fernen Zeitpunkt in der Zukunft festgelegt. Der genaue Zeitpunkt des Übergangs wird vom StorageGRID -System nicht gesteuert.

Zustand des Objekts	Antwort auf HeadObject

Das Objekt ist in den nicht abrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Raster vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Der Wert für `expiry-date` ist auf einen fernen Zeitpunkt in der Zukunft festgelegt.
	
	Hinweis: Wenn die Kopie im Grid nicht verfügbar ist (z. B. weil ein Storage Node ausgefallen ist), müssen Sie eine"RestoreObject" Fordern Sie die Wiederherstellung der Kopie aus dem Cloud-Speicherpool an, bevor Sie das Objekt erfolgreich abrufen können.

Das Objekt ist in einen nicht abrufbaren Zustand übergegangen und es ist keine Kopie im Raster vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objekt wird gerade aus einem nicht abrufbaren Zustand wiederhergestellt	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Objekt vollständig im Cloud-Speicherpool wiederhergestellt	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	Der `expiry-date` gibt an, wann das Objekt im Cloud-Speicherpool in einen nicht abrufbaren Zustand zurückversetzt wird.

Mehrteilige oder segmentierte Objekte im Cloud Storage Pool

Wenn Sie ein mehrteiliges Objekt hochgeladen haben oder StorageGRID ein großes Objekt in Segmente aufgeteilt hat, ermittelt StorageGRID , ob das Objekt im Cloud Storage Pool verfügbar ist, indem es eine Teilmenge der Teile oder Segmente des Objekts auswählt. In einigen Fällen kann eine HeadObject-Anforderung fälschlicherweise zurückgeben `x-amz-restore: ongoing-request="false"` wenn einige Teile des Objekts bereits in einen nicht abrufbaren Zustand überführt wurden oder wenn einige Teile des Objekts noch nicht wiederhergestellt wurden.

HeadObject und Cross-Grid-Replikation

Wenn Sie"Netzverbund" Und"Cross-Grid-Replikation" für einen Bucket aktiviert ist, kann der S3-Client den Replikationsstatus eines Objekts überprüfen, indem er eine HeadObject-Anforderung ausgibt. 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.

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

PutObject

Sie können die S3 PutObject-Anforderung verwenden, um einem Bucket ein Objekt hinzuzufügen.

Konflikte lösen

Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.

Objektgröße

Die maximal *empfohlene* Größe für einen einzelnen PutObject-Vorgang beträgt 5 GiB (5.368.709.120 Bytes). Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie"mehrteiliger Upload" stattdessen.

Die maximal *unterstützte* Größe für einen einzelnen PutObject-Vorgang beträgt 5 TiB (5.497.558.138.880 Bytes).

Wenn Sie ein Upgrade von StorageGRID 11.6 oder früher durchgeführt haben, wird die Warnung „S3 PUT-Objektgröße zu groß“ ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das 5 GiB überschreitet. Wenn Sie eine Neuinstallation von StorageGRID 11.7 oder 11.8 haben, wird der Alarm in diesem Fall nicht ausgelöst. Um jedoch dem AWS S3-Standard zu entsprechen, werden zukünftige Versionen von StorageGRID keine Uploads von Objekten unterstützen, die größer als 5 GiB sind.

Größe der Benutzermetadaten

Amazon S3 begrenzt die Größe benutzerdefinierter Metadaten innerhalb jedes PUT-Anforderungsheaders auf 2 KB. StorageGRID begrenzt Benutzermetadaten auf 24 KiB. Die Größe benutzerdefinierter Metadaten wird gemessen, indem die Summe der Anzahl der Bytes in der UTF-8-Kodierung jedes Schlüssels und Werts

berechnet wird.

UTF-8-Zeichen in Benutzermetadaten

Wenn eine Anfrage (nicht maskierte) UTF-8-Werte im Schlüsselnamen oder Wert benutzerdefinierter Metadaten enthält, ist das StorageGRID Verhalten undefiniert.

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen, die im Schlüsselnamen oder -wert benutzerdefinierter Metadaten enthalten sind. Escape-UTF-8-Zeichen werden als ASCII-Zeichen behandelt:

- PutObject-, CopyObject-, GetObject- und HeadObject-Anfragen sind erfolgreich, wenn benutzerdefinierte Metadaten Escape-UTF-8-Zeichen enthalten.
- StorageGRID gibt nicht zurück `x-amz-missing-meta` Header, wenn der interpretierte Wert des Schlüsselnamens oder -werts nicht druckbare Zeichen enthält.

Objekt-Tag-Grenzwerte

Sie können neuen Objekten beim Hochladen Tags hinzufügen oder Sie können sie vorhandenen Objekten hinzufügen. Sowohl StorageGRID als auch Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Mit einem Objekt verknüpfte Tags müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei Schlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden.

Objektbesitz

In StorageGRID sind alle Objekte Eigentum des Bucket-Eigentümerkontos, einschließlich der Objekte, die von einem Nicht-Eigentümerkonto oder einem anonymen Benutzer erstellt wurden.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Wenn Sie angeben `aws-chunked` für`Content-Encoding` StorageGRID überprüft die folgenden Punkte nicht:

  - StorageGRID überprüft nicht die `chunk-signature` gegen die Chunk-Daten.
  - StorageGRID überprüft den Wert, den Sie angeben, nicht für `x-amz-decoded-content-length` gegen das Objekt.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

Chunked Transfer Encoding wird unterstützt, wenn `aws-chunked` Außerdem wird eine Nutzlastsignatur verwendet.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten.

  Verwenden Sie beim Angeben des Name-Wert-Paares für benutzerdefinierte Metadaten dieses allgemeine Format:

  ```
  x-amz-meta-name: value
  ```

  Wenn Sie die Option **Benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie `creation-time` als Name der Metadaten, die aufzeichnen, wann das Objekt erstellt wurde. Beispiel:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  Der Wert für `creation-time` wird seit dem 1. Januar 1970 in Sekunden ausgewertet.

  > Eine ILM-Regel kann nicht sowohl eine **benutzerdefinierte Erstellungszeit** für die Referenzzeit als auch die Aufnahmeoption „Ausgewogen“ oder „Streng“ verwenden. Beim Erstellen der ILM-Regel wird ein Fehler zurückgegeben.

- `x-amz-tagging`
- S3 Object Lock-Anforderungsheader
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Wenn eine Anfrage ohne diese Header gestellt wird, werden die Bucket-Standardaufbewahrungseinstellungen verwendet, um den Objektversionsmodus und das Aufbewahrungsdatum zu berechnen. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .
- SSE-Anforderungsheader:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    SehenAnforderungsheader für serverseitige Verschlüsselung

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  Der `x-amz-website-redirect-location` Header-Returns `XNotImplemented` .

Speicherklassenoptionen

Der `x-amz-storage-class` Anforderungsheader wird unterstützt. Der übermittelte Wert für `x-amz-storage-class` beeinflusst, wie StorageGRID Objektdaten während der Aufnahme schützt, und nicht, wie viele persistente Kopien des Objekts im StorageGRID -System gespeichert werden (was durch ILM bestimmt wird).

Wenn die ILM-Regel, die einem aufgenommenen Objekt entspricht, die Option „Strenge Aufnahme“ verwendet, `x-amz-storage-class` Header hat keine Wirkung.

Folgende Werte können verwendet werden für `x-amz-storage-class` :

- `STANDARD`(Standard)
  - **Dual Commit**: Wenn die ILM-Regel die Option „Dual Commit“ für das Aufnahmeverhalten angibt, wird, sobald ein Objekt aufgenommen wird, eine zweite Kopie dieses Objekts erstellt und an einen anderen Speicherknoten verteilt (Dual Commit). Bei der Auswertung des ILM ermittelt StorageGRID , ob diese ersten Zwischenkopien die Platzierungsanweisungen in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an anderen Orten erstellt und die ersten Zwischenkopien gelöscht werden.
  - **Ausgeglichen**: Wenn die ILM-Regel die Option „Ausgeglichen“ angibt und StorageGRID nicht sofort alle in der Regel angegebenen Kopien erstellen kann, erstellt StorageGRID zwei Zwischenkopien auf verschiedenen Speicherknoten.

    Wenn StorageGRID alle in der ILM-Regel angegebenen Objektkopien sofort erstellen kann (synchrone Platzierung), `x-amz-storage-class` Header hat keine Wirkung.

- `REDUCED_REDUNDANCY`
  - **Dual Commit**: Wenn die ILM-Regel die Option „Dual Commit“ für das Aufnahmeverhalten angibt, erstellt StorageGRID beim Aufnehmen des Objekts eine einzelne Zwischenkopie (Single Commit).
  - **Ausgeglichen**: Wenn die ILM-Regel die Option „Ausgeglichen“ angibt, erstellt StorageGRID nur dann eine einzelne Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat dieser Header keine Wirkung. Der `REDUCED_REDUNDANCY` Die Option wird am besten verwendet, wenn die ILM-Regel, die dem Objekt entspricht, eine einzelne replizierte Kopie erstellt. In diesem Fall mit `REDUCED_REDUNDANCY` vermeidet das unnötige Erstellen und Löschen einer zusätzlichen Objektkopie für jeden Aufnahmevorgang.

  Verwenden des `REDUCED_REDUNDANCY` Unter anderen Umständen wird diese Option nicht empfohlen. `REDUCED_REDUNDANCY` erhöht das Risiko eines Objektdatenverlusts während der Aufnahme.

Beispielsweise können Daten verloren gehen, wenn die einzelne Kopie zunächst auf einem Speicherknoten gespeichert wird, der ausfällt, bevor die ILM-Auswertung erfolgen kann.

> Wenn für einen bestimmten Zeitraum nur eine Kopie vorhanden ist, besteht die Gefahr eines dauerhaften Datenverlusts. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

Festlegen `REDUCED_REDUNDANCY` wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Es hat keinen Einfluss darauf, wie viele Kopien des Objekts erstellt werden, wenn das Objekt von den aktiven ILM-Richtlinien ausgewertet wird, und führt nicht dazu, dass Daten im StorageGRID System auf niedrigeren Redundanzebenen gespeichert werden.

> Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperre aufnehmen, wird die `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-Compliant-Bucket aufnehmen, `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine Dual-Commit-Aufnahme durch, um sicherzustellen, dass die Compliance-Anforderungen erfüllt werden.

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein Objekt mit serverseitiger Verschlüsselung zu verschlüsseln. Die Optionen SSE und SSE-C schließen sich gegenseitig aus.

- **SSE**: Verwenden Sie den folgenden Header, wenn Sie das Objekt mit einem eindeutigen, von StorageGRID verwalteten Schlüssel verschlüsseln möchten.
  - `x-amz-server-side-encryption`

    Wenn die `x-amz-server-side-encryption` Header ist nicht in der PutObject-Anforderung enthalten, der rasterweite"Einstellung für die Verschlüsselung gespeicherter Objekte" wird aus der PutObject-Antwort weggelassen.

- **SSE-C**: Verwenden Sie alle drei Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
  - `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.
  - `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Überlegungen für"Verwendung serverseitiger Verschlüsselung" .

> Wenn ein Objekt mit SSE oder SSE-C verschlüsselt ist, werden alle Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

Versionierung

Wenn die Versionierung für einen Bucket aktiviert ist, `versionId` wird automatisch für die Version des gespeicherten Objekts generiert. Das `versionId` wird auch in der Antwort zurückgegeben, indem der `x-amz-version-id` Antwortheader.

Wenn die Versionierung ausgesetzt ist, wird die Objektversion mit einem Nullwert gespeichert. `versionId` und wenn bereits eine Nullversion vorhanden ist, wird diese überschrieben.

Signaturberechnungen für den Autorisierungsheader

Bei Verwendung der `Authorization` Header zur Authentifizierung von Anfragen. StorageGRID unterscheidet sich in folgenden Punkten von AWS:

- StorageGRID erfordert nicht `host` Header, die in `CanonicalHeaders` .
- StorageGRID erfordert nicht `Content-Type` eingeschlossen sein in `CanonicalHeaders` .
- StorageGRID erfordert nicht `x-amz-*` Header, die in `CanonicalHeaders` .

> Als allgemeine Best Practice sollten Sie diese Header immer in `CanonicalHeaders` um sicherzustellen, dass sie überprüft werden. Wenn Sie diese Header jedoch ausschließen, gibt StorageGRID keinen Fehler zurück.

Weitere Einzelheiten finden Sie unter "Signaturberechnungen für den Autorisierungsheader: Übertragen der Nutzlast in einem einzigen Block (AWS-Signaturversion 4)" .

Ähnliche Informationen

- "Objekte mit ILM verwalten"
- "Amazon Simple Storage Service API-Referenz: PutObject"

RestoreObject

Sie können die S3 RestoreObject-Anforderung verwenden, um ein Objekt wiederherzustellen, das in einem Cloud-Speicherpool gespeichert ist.

Unterstützter Anfragetyp

StorageGRID unterstützt nur RestoreObject-Anfragen zum Wiederherstellen eines Objekts. Es unterstützt nicht die `SELECT` Art der Restaurierung. Wählen Sie Anfragen zurück `XNotImplemented` .

Versionierung

Geben Sie optional an `versionId` um eine bestimmte Version eines Objekts in einem versionierten Bucket wiederherzustellen. Wenn Sie nicht angeben `versionId` wird die aktuellste Version des Objekts wiederhergestellt

Verhalten von RestoreObject bei Cloud Storage Pool-Objekten

Wenn ein Objekt in einem"Cloud-Speicherpool" , eine RestoreObject-Anforderung weist basierend auf dem Status des Objekts das folgende Verhalten auf. Sehen"HeadObject" für weitere Details.

Wenn ein Objekt in einem Cloud-Speicherpool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, ist es nicht erforderlich, das Objekt durch Ausgeben einer RestoreObject-Anforderung wiederherzustellen. Stattdessen kann die lokale Kopie direkt mithilfe einer GetObject-Anforderung abgerufen werden.

Zustand des Objekts	Verhalten von RestoreObject
Objekt in StorageGRID aufgenommen, aber noch nicht von ILM ausgewertet, oder Objekt befindet sich nicht in einem Cloud-Speicherpool	`403 Forbidden` , `InvalidObjectState`
Objekt im Cloud-Speicherpool, aber noch nicht in einen nicht abrufbaren Zustand übergegangen	`200 OK`Es werden keine Änderungen vorgenommen. **Hinweis**: Bevor ein Objekt in einen nicht abrufbaren Zustand überführt wurde, können Sie seine `expiry-date` .
Objekt in einen nicht abrufbaren Zustand überführt	`202 Accepted`Stellt eine abrufbare Kopie des Objekts für die im Anforderungstext angegebene Anzahl von Tagen im Cloud-Speicherpool wieder her. Am Ende dieses Zeitraums wird das Objekt in einen nicht abrufbaren Zustand zurückversetzt. Optional können Sie die `Tier` Anforderungselement, um zu bestimmen, wie lange es dauert, bis der Wiederherstellungsjob abgeschlossen ist(`Expedited` , `Standard` , oder `Bulk`). Wenn Sie nicht angeben `Tier` , Die `Standard` Ebene verwendet wird. **Wichtig**: Wenn ein Objekt in das S3 Glacier Deep Archive verschoben wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, können Sie es nicht mit dem `Expedited` Stufe. Der folgende Fehler wird zurückgegeben `403 Forbidden` , `InvalidTier` : `Retrieval option is not supported by this storage class.`
Objekt wird gerade aus einem nicht abrufbaren Zustand wiederhergestellt	`409 Conflict` , `RestoreAlreadyInProgress`
Objekt vollständig im Cloud-Speicherpool wiederhergestellt	`200 OK` **Hinweis:** Wenn ein Objekt in einen abrufbaren Zustand zurückversetzt wurde, können Sie seine `expiry-date` durch erneutes Ausgeben der RestoreObject-Anforderung mit einem neuen Wert für `Days` . Das Wiederherstellungsdatum wird relativ zum Zeitpunkt der Anfrage aktualisiert.

SelectObjectContent

Sie können die S3 SelectObjectContent-Anforderung verwenden, um den Inhalt eines S3-Objekts basierend auf einer einfachen SQL-Anweisung zu filtern.

Weitere Informationen finden Sie unter "Amazon Simple Storage Service API-Referenz: SelectObjectContent" .

Bevor Sie beginnen

- Das Mandantenkonto verfügt über die Berechtigung „S3 Select“.
- Du hast `s3:GetObject` Berechtigung für das Objekt, das Sie abfragen möchten.
- 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.
- Ihr SQL-Ausdruck hat eine maximale Länge von 256 KB.
- Jeder Datensatz in der Eingabe oder den Ergebnissen hat eine maximale Länge von 1 MiB.

Beispiel für die CSV-Anforderungssyntax

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Beispiel für die Parquet-Anforderungssyntax

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL-Abfragebeispiel

Diese Abfrage ermittelt den Namen des Bundesstaates, die Bevölkerungszahlen von 2010, die geschätzten Bevölkerungszahlen von 2015 und die prozentuale Veränderung gegenüber den US-Volkszählungsdaten. Datensätze in der Datei, die keine Zustände sind, werden ignoriert.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Die ersten Zeilen der abzufragenden Datei, `SUB-EST2020_ALL.csv` , sehen so aus:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS-CLI-Nutzungsbeispiel (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Die ersten paar Zeilen der Ausgabedatei, `changes.csv` , sehen so aus:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

AWS-CLI-Nutzungsbeispiel (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Die ersten Zeilen der Ausgabedatei changes.csv sehen folgendermaßen aus:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Vorgänge für mehrteilige Uploads

Vorgänge für mehrteilige Uploads

In diesem Abschnitt wird beschrieben, wie StorageGRID Vorgänge für mehrteilige Uploads unterstützt.

Für alle mehrteiligen Uploadvorgänge gelten die folgenden Bedingungen und Hinweise:

- Sie sollten nicht mehr als 1.000 gleichzeitige mehrteilige Uploads in einen einzelnen Bucket durchführen, da die Ergebnisse von ListMultipartUploads-Abfragen für diesen Bucket möglicherweise unvollständige Ergebnisse zurückgeben.
- StorageGRID erzwingt AWS-Größenbeschränkungen für mehrteilige Teile. S3-Clients müssen diese Richtlinien befolgen:
  - Jeder Teil eines mehrteiligen Uploads muss zwischen 5 MiB (5.242.880 Bytes) und 5 GiB (5.368.709.120 Bytes) groß sein.
  - Der letzte Teil kann kleiner als 5 MiB (5.242.880 Bytes) sein.
  - Generell sollten die Teilegrößen möglichst groß sein. Verwenden Sie beispielsweise Teilgrößen von 5 GiB für ein 100-GiB-Objekt. Da jedes Teil als einzigartiges Objekt betrachtet wird, reduziert die Verwendung großer Teilegrößen den StorageGRID Metadaten-Overhead.
  - Erwägen Sie für Objekte, die kleiner als 5 GiB sind, stattdessen die Verwendung eines nicht mehrteiligen Uploads.
- ILM wird für jeden Teil eines mehrteiligen Objekts ausgewertet, wenn es aufgenommen wird, und für das Objekt als Ganzes, wenn der mehrteilige Upload abgeschlossen ist, wenn die ILM-Regel die Balanced- oder Strict-Regel verwendet."Aufnahmeoption" . Sie sollten sich darüber im Klaren sein, welche Auswirkungen dies auf die Platzierung von Objekten und Teilen hat:

- Wenn sich ILM während eines laufenden S3-Multipart-Uploads ändert, erfüllen einige Teile des Objekts nach Abschluss des Multipart-Uploads möglicherweise nicht die aktuellen ILM-Anforderungen. Alle Teile, die nicht richtig platziert sind, werden zur erneuten ILM-Bewertung in die Warteschlange gestellt und später an die richtige Position verschoben.
- Bei der Auswertung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils, nicht nach der Größe des Objekts. Dies bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn beispielsweise eine Regel angibt, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert werden, wird jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei der Aufnahme bei DC2 gespeichert. Wenn ILM jedoch für das gesamte Objekt ausgewertet wird, werden alle Teile des Objekts nach DC1 verschoben.

- Alle mehrteiligen Upload-Vorgänge unterstützen StorageGRID"Konsistenzwerte" .
- Wenn ein Objekt per mehrteiligem Upload aufgenommen wird,"Schwellenwert für Objektsegmentierung (1 GiB)" wird nicht angewendet.
- Bei Bedarf können Sie"serverseitige Verschlüsselung" mit mehrteiligen Uploads. Um SSE (serverseitige Verschlüsselung mit StorageGRID-verwalteten Schlüsseln) zu verwenden, schließen Sie die `x-amz-server-side-encryption` Anforderungsheader nur in der CreateMultipartUpload-Anforderung. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der CreateMultipartUpload-Anforderung und in jeder nachfolgenden UploadPart-Anforderung dieselben drei Anforderungsheader für Verschlüsselungsschlüssel an.

Betrieb	Durchführung
AbortMultipartUpload	Implementiert mit dem gesamten Amazon S3 REST API-Verhalten. Änderungen vorbehalten.
CompleteMultipartUpload	Sehen"CompleteMultipartUpload"
CreateMultipartUpload (früher „Mehrteiligen Upload initiieren“ genannt)	Sehen"CreateMultipartUpload"
ListMultipartUploads	Sehen"ListMultipartUploads"
Teileliste	Implementiert mit dem gesamten Amazon S3 REST API-Verhalten. Änderungen vorbehalten.
UploadPart	Sehen"UploadPart"
UploadPartCopy	Sehen"UploadPartCopy"

CompleteMultipartUpload

Der Vorgang „CompleteMultipartUpload“ schließt einen mehrteiligen Upload eines Objekts ab, indem er die zuvor hochgeladenen Teile zusammenfügt.

StorageGRID unterstützt nicht aufeinanderfolgende Werte in aufsteigender Reihenfolge für die `partNumber` Anforderungsparameter mit CompleteMultipartUpload. Der Parameter kann mit einem beliebigen Wert beginnen.

Konflikte lösen

Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  Der `x-amz-storage-class` Der Header beeinflusst, wie viele Objektkopien StorageGRID erstellt, wenn die entsprechende ILM-Regel Folgendes angibt:"Option für doppeltes Commit oder ausgeglichene Aufnahme" .

- `STANDARD`

  (Standard) Gibt einen Dual-Commit-Aufnahmevorgang an, wenn die ILM-Regel die Option „Dual Commit“ verwendet oder wenn die Option „Balanced“ auf die Erstellung von Zwischenkopien zurückgreift.

- `REDUCED_REDUNDANCY`

  Gibt einen Single-Commit-Ingest-Vorgang an, wenn die ILM-Regel die Option „Dual Commit“ verwendet oder wenn die Option „Balanced“ auf die Erstellung von Zwischenkopien zurückgreift.

  Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperre aufnehmen, wird die `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-Compliant-Bucket aufnehmen, `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine Dual-Commit-Aufnahme durch, um sicherzustellen, dass die Compliance-Anforderungen erfüllt werden.

Wenn ein mehrteiliger Upload nicht innerhalb von 15 Tagen abgeschlossen wird, wird der Vorgang als inaktiv markiert und alle zugehörigen Daten werden aus dem System gelöscht.

Der `ETag` Der zurückgegebene Wert ist keine MD5-Summe der Daten, sondern folgt der Amazon S3 API-Implementierung des `ETag` Wert für mehrteilige Objekte.

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Versionierung

Dieser Vorgang schließt einen mehrteiligen Upload ab. Wenn die Versionierung für einen Bucket aktiviert ist, wird die Objektversion nach Abschluss des mehrteiligen Uploads erstellt.

Wenn die Versionierung für einen Bucket aktiviert ist, `versionId` wird automatisch für die Version des gespeicherten Objekts generiert. Das `versionId` wird auch in der Antwort zurückgegeben, indem der `x-amz-version-id` Antwortheader.

Wenn die Versionierung ausgesetzt ist, wird die Objektversion mit einem Nullwert gespeichert. `versionId` und wenn bereits eine Nullversion vorhanden ist, wird diese überschrieben.

> Wenn die Versionsverwaltung für einen Bucket aktiviert ist, wird beim Abschließen eines mehrteiligen Uploads immer eine neue Version erstellt, auch wenn gleichzeitig mehrteilige Uploads für denselben Objektschlüssel abgeschlossen wurden. Wenn die Versionsverwaltung für einen Bucket nicht aktiviert ist, ist es möglich, einen mehrteiligen Upload zu initiieren und dann zunächst einen weiteren mehrteiligen Upload mit demselben Objektschlüssel zu initiieren und abzuschließen. Bei Buckets ohne Versionsangabe hat der zuletzt abgeschlossene mehrteilige Upload Vorrang.

Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

Wenn der Bucket, in dem der mehrteilige Upload erfolgt, für einen Plattformdienst konfiguriert ist, ist der mehrteilige Upload auch dann erfolgreich, wenn die zugehörige Replikations- oder Benachrichtigungsaktion fehlschlägt.

Ein Mandant kann die fehlgeschlagene Replikation oder Benachrichtigung auslösen, indem er die Metadaten oder Tags des Objekts aktualisiert. Um unerwünschte Änderungen zu vermeiden, kann ein Mandant die vorhandenen Werte erneut übermitteln.

Weitere Informationen finden Sie unter "Fehlerbehebung bei Plattformdiensten" .

CreateMultipartUpload

Der Vorgang „CreateMultipartUpload“ (früher „Initiate Multipart Upload“) initiiert einen mehrteiligen Upload für ein Objekt und gibt eine Upload-ID zurück.

Der `x-amz-storage-class` Anforderungsheader wird unterstützt. Der übermittelte Wert für `x-amz-storage-class` beeinflusst, wie StorageGRID Objektdaten während der Aufnahme schützt, und nicht, wie viele persistente Kopien des Objekts im StorageGRID -System gespeichert werden (was durch ILM bestimmt wird).

Wenn die ILM-Regel, die einem aufgenommenen Objekt entspricht, die strikte"Aufnahmeoption" , Die `x-amz-storage-class` Header hat keine Wirkung.

Folgende Werte können verwendet werden für `x-amz-storage-class` :

- `STANDARD`(Standard)
  - **Dual Commit**: Wenn die ILM-Regel die Aufnahmeoption „Dual Commit“ angibt, wird, sobald ein Objekt aufgenommen wird, eine zweite Kopie dieses Objekts erstellt und an einen anderen Speicherknoten verteilt (Dual Commit). Bei der Auswertung des ILM ermittelt StorageGRID , ob diese ersten Zwischenkopien die Platzierungsanweisungen in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an anderen Orten erstellt und die ersten Zwischenkopien gelöscht

werden.

- **Ausgeglichen**: Wenn die ILM-Regel die Option „Ausgeglichen“ angibt und StorageGRID nicht sofort alle in der Regel angegebenen Kopien erstellen kann, erstellt StorageGRID zwei Zwischenkopien auf verschiedenen Speicherknoten.

  Wenn StorageGRID alle in der ILM-Regel angegebenen Objektkopien sofort erstellen kann (synchrone Platzierung), `x-amz-storage-class` Header hat keine Wirkung.

- `REDUCED_REDUNDANCY`

  - **Dual Commit**: Wenn die ILM-Regel die Option „Dual Commit“ angibt, erstellt StorageGRID beim Einlesen des Objekts eine einzelne Zwischenkopie (Single Commit).
  - **Ausgeglichen**: Wenn die ILM-Regel die Option „Ausgeglichen“ angibt, erstellt StorageGRID nur dann eine einzelne Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat dieser Header keine Wirkung. Der `REDUCED_REDUNDANCY` Die Option wird am besten verwendet, wenn die ILM-Regel, die dem Objekt entspricht, eine einzelne replizierte Kopie erstellt. In diesem Fall mit `REDUCED_REDUNDANCY` vermeidet das unnötige Erstellen und Löschen einer zusätzlichen Objektkopie für jeden Aufnahmevorgang.

  Verwenden des `REDUCED_REDUNDANCY` Unter anderen Umständen wird diese Option nicht empfohlen. `REDUCED_REDUNDANCY` erhöht das Risiko eines Objektdatenverlusts während der Aufnahme. Beispielsweise können Daten verloren gehen, wenn die einzelne Kopie zunächst auf einem Speicherknoten gespeichert wird, der ausfällt, bevor die ILM-Auswertung erfolgen kann.

> Wenn für einen bestimmten Zeitraum nur eine Kopie vorhanden ist, besteht die Gefahr eines dauerhaften Datenverlusts. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

Festlegen `REDUCED_REDUNDANCY` wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Es hat keinen Einfluss darauf, wie viele Kopien des Objekts erstellt werden, wenn das Objekt von den aktiven ILM-Richtlinien ausgewertet wird, und führt nicht dazu, dass Daten im StorageGRID System auf niedrigeren Redundanzebenen gespeichert werden.

> Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperre aufnehmen, wird die `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-Compliant-Bucket aufnehmen, `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine Dual-Commit-Aufnahme durch, um sicherzustellen, dass die Compliance-Anforderungen erfüllt werden.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

- `Content-Type`
- `x-amz-checksum-algorithm`

  Derzeit ist nur der SHA256-Wert für `x-amz-checksum-algorithm` wird unterstützt.

- `x-amz-meta-`, gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten

  Verwenden Sie beim Angeben des Name-Wert-Paares für benutzerdefinierte Metadaten dieses allgemeine Format:

  ```
  x-amz-meta-_name_: `value`
  ```

  Wenn Sie die Option **Benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie `creation-time` als Name der Metadaten, die aufzeichnen, wann das Objekt erstellt wurde. Beispiel:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  Der Wert für `creation-time` wird seit dem 1. Januar 1970 in Sekunden ausgewertet.

  > Hinzufügen `creation-time` da benutzerdefinierte Metadaten nicht zulässig sind, wenn Sie ein Objekt zu einem Bucket hinzufügen, für den die Legacy-Compliance aktiviert ist. Es wird ein Fehler zurückgegeben.

- S3 Object Lock-Anforderungsheader:

  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Wenn eine Anfrage ohne diese Header gestellt wird, werden die Bucket-Standardaufbewahrungseinstellungen verwendet, um das Aufbewahrungsdatum der Objektversion zu berechnen.

  "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

- SSE-Anforderungsheader:

  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Anforderungsheader für serverseitige Verschlüsselung

  > Informationen zur Verarbeitung von UTF-8-Zeichen durch StorageGRID finden Sie unter"PutObject" .

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein mehrteiliges Objekt mit serverseitiger

Verschlüsselung zu verschlüsseln. Die Optionen SSE und SSE-C schließen sich gegenseitig aus.

- **SSE**: Verwenden Sie den folgenden Header in der CreateMultipartUpload-Anforderung, wenn Sie das Objekt mit einem eindeutigen, von StorageGRID verwalteten Schlüssel verschlüsseln möchten. Geben Sie diesen Header in keiner der UploadPart-Anfragen an.
  - `x-amz-server-side-encryption`
- **SSE-C**: Verwenden Sie alle drei dieser Header in der CreateMultipartUpload-Anfrage (und in jeder nachfolgenden UploadPart-Anfrage), wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
  - `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.
  - `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Überlegungen für"Verwendung serverseitiger Verschlüsselung" .

Nicht unterstützte Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt:

- `x-amz-website-redirect-location`

  Der `x-amz-website-redirect-location` Header-Returns `XNotImplemented` .

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang CompleteMultipartUpload ausgeführt wird.

ListMultipartUploads

Der Vorgang „ListMultipartUploads“ listet laufende mehrteilige Uploads für einen Bucket auf.

Die folgenden Anforderungsparameter werden unterstützt:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`

- `Date`
- `Authorization`

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang CompleteMultipartUpload ausgeführt wird.

UploadPart

Der Vorgang „UploadPart“ lädt einen Teil in einem mehrteiligen Upload für ein Objekt hoch.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie für die CreateMultipartUpload-Anforderung die SSE-C-Verschlüsselung angegeben haben, müssen Sie in jede UploadPart-Anforderung auch die folgenden Anforderungsheader einfügen:

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der CreateMultipartUpload-Anforderung angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie denselben MD5-Digest an, den Sie in der CreateMultipartUpload-Anforderung angegeben haben.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in"Verwenden Sie serverseitige Verschlüsselung" .

Wenn Sie während der CreateMultipartUpload-Anforderung eine SHA-256-Prüfsumme angegeben haben, müssen Sie in jede UploadPart-Anforderung auch den folgenden Anforderungsheader einfügen:

- `x-amz-checksum-sha256`: Geben Sie die SHA-256-Prüfsumme für diesen Teil an.

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang CompleteMultipartUpload ausgeführt wird.

UploadPartCopy

Der Vorgang „UploadPartCopy“ lädt einen Teil eines Objekts hoch, indem Daten aus einem vorhandenen Objekt als Datenquelle kopiert werden.

Der Vorgang „UploadPartCopy“ wird mit dem gesamten Amazon S3 REST-API-Verhalten implementiert. Änderungen vorbehalten.

Diese Anfrage liest und schreibt die Objektdaten, die in `x-amz-copy-source-range` innerhalb des StorageGRID -Systems.

Die folgenden Anforderungsheader werden unterstützt:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie für die CreateMultipartUpload-Anforderung eine SSE-C-Verschlüsselung angegeben haben, müssen Sie in jede UploadPartCopy-Anforderung auch die folgenden Anforderungsheader einfügen:

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der CreateMultipartUpload-Anforderung angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie denselben MD5-Digest an, den Sie in der CreateMultipartUpload-Anforderung angegeben haben.

Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt ist, müssen Sie die folgenden drei Header in die UploadPartCopy-Anforderung aufnehmen, damit das Objekt entschlüsselt und dann kopiert werden kann:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-copy-source-server-side-encryption-customer-key`: Geben Sie den Verschlüsselungsschlüssel an, den Sie beim Erstellen des Quellobjekts angegeben haben.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest an, den Sie beim Erstellen des Quellobjekts angegeben haben.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in"Verwenden Sie serverseitige Verschlüsselung" .

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang CompleteMultipartUpload ausgeführt wird.

Fehlerantworten

Das StorageGRID -System unterstützt alle zutreffenden Standardfehlerantworten der S3 REST-API. Darüber hinaus fügt die StorageGRID -Implementierung mehrere benutzerdefinierte Antworten hinzu.

Unterstützte S3-API-Fehlercodes

Name	HTTP-Status
Zugriff verweigert	403 Verboten
BadDigest	400 Ungültige Anfrage
BucketExistsAlready	409 Konflikt
EimerNichtLeer	409 Konflikt
Unvollständiger Körper	400 Ungültige Anfrage
Interner Fehler	500 Interner Serverfehler
Ungültige Zugriffsschlüssel-ID	403 Verboten
Ungültiges Argument	400 Ungültige Anfrage
Ungültiger BucketName	400 Ungültige Anfrage
Ungültiger BucketState	409 Konflikt
InvalidDigest	400 Ungültige Anfrage
Fehler „Ungültiger Verschlüsselungsalgorithmus“	400 Ungültige Anfrage
UngültigesTeil	400 Ungültige Anfrage
UngültigeTeilebestellung	400 Ungültige Anfrage
Ungültiger Bereich	416 Angeforderter Bereich nicht erfüllbar
Ungültige Anfrage	400 Ungültige Anfrage

Name	HTTP-Status
Ungültige Speicherklasse	400 Ungültige Anfrage
Ungültiges Tag	400 Ungültige Anfrage
Ungültige URI	400 Ungültige Anfrage
Schlüssel zu lang	400 Ungültige Anfrage
MalformedXML	400 Ungültige Anfrage
Metadaten zu groß	400 Ungültige Anfrage
MethodeNichtZulässig	405 Methode nicht zulässig
MissingContentLength	411 Erforderliche Länge
MissingRequestBodyError	400 Ungültige Anfrage
MissingSecurityHeader	400 Ungültige Anfrage
KeinSuchBucket	404 Nicht gefunden
NoSuchKey	404 Nicht gefunden
NoSuchUpload	404 Nicht gefunden
Nicht implementiert	501 Nicht implementiert
NoSuchBucketPolicy	404 Nicht gefunden
ObjectLockConfigurationNotFoundError	404 Nicht gefunden
Vorbedingung fehlgeschlagen	412 Vorbedingung fehlgeschlagen
RequestTimeTooSkewed	403 Verboten
Dienst nicht verfügbar	503 Dienst nicht verfügbar
Signatur stimmt nicht überein	403 Verboten
Zu viele Eimer	400 Ungültige Anfrage
Benutzerschlüssel muss angegeben werden	400 Ungültige Anfrage

Benutzerdefinierte StorageGRID -Fehlercodes

Name	Beschreibung	HTTP-Status
XBucketLifecycleNotAllowed	Die Bucket-Lebenszykluskonfiguration ist in einem älteren konformen Bucket nicht zulässig	400 Ungültige Anfrage
XBucketPolicyParseException	Das Parsen der empfangenen Bucket-Richtlinien-JSON ist fehlgeschlagen.	400 Ungültige Anfrage
XComplianceConflict	Vorgang aufgrund veralteter Compliance-Einstellungen abgelehnt.	403 Verboten
XComplianceReduzierteRedundanzVerboten	Reduzierte Redundanz ist im Legacy-Compliant-Bucket nicht zulässig	400 Ungültige Anfrage
XMaxBucketPolicyLengthExceeded	Ihre Richtlinie überschreitet die maximal zulässige Bucket-Richtlinienlänge.	400 Ungültige Anfrage
XMissingInternalRequestHeader	Es fehlt ein Header einer internen Anfrage.	400 Ungültige Anfrage
XNoSuchBucketCompliance	Für den angegebenen Bucket ist die Legacy-Compliance nicht aktiviert.	404 Nicht gefunden
XNichtAkzeptabel	Die Anfrage enthält einen oder mehrere Accept-Header, die nicht erfüllt werden konnten.	406 Nicht akzeptabel
XNotImplemented	Die von Ihnen angegebene Anfrage impliziert eine Funktionalität, die nicht implementiert ist.	501 Nicht implementiert

Benutzerdefinierte StorageGRID -Vorgänge

Benutzerdefinierte StorageGRID -Vorgänge

Das StorageGRID -System unterstützt benutzerdefinierte Vorgänge, die der S3 REST-API hinzugefügt werden.

In der folgenden Tabelle sind die von StorageGRID unterstützten benutzerdefinierten Vorgänge aufgeführt.

Betrieb	Beschreibung
"GET Bucket-Konsistenz"	Gibt die Konsistenz zurück, die auf einen bestimmten Bucket angewendet wird.

Betrieb	Beschreibung
"PUT Bucket-Konsistenz"	Legt die Konsistenz fest, die auf einen bestimmten Bucket angewendet wird.
"GET Bucket – Letzte Zugriffszeit"	Gibt zurück, ob Aktualisierungen der letzten Zugriffszeit für einen bestimmten Bucket aktiviert oder deaktiviert sind.
"PUT Bucket: Letzte Zugriffszeit"	Ermöglicht Ihnen, Aktualisierungen der letzten Zugriffszeit für einen bestimmten Bucket zu aktivieren oder zu deaktivieren.
"Konfiguration der Benachrichtigung über DELETE-Bucket-Metadaten"	Löscht die XML-Metadatenbenachrichtigungskonfiguration, die einem bestimmten Bucket zugeordnet ist.
"GET Bucket-Metadaten-Benachrichtigungskonfiguration"	Gibt die XML-Konfigurationsdatei für Metadatenbenachrichtigungen zurück, die einem bestimmten Bucket zugeordnet ist.
"Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten"	Konfiguriert den Metadaten-Benachrichtigungsdienst für einen Bucket.
"GET-Speichernutzung"	Gibt die Gesamtspeichermenge an, die von einem Konto und jedem mit dem Konto verknüpften Bucket verwendet wird.
"Veraltet: CreateBucket mit Compliance-Einstellungen"	Veraltet und nicht unterstützt: Sie können keine neuen Buckets mehr erstellen, wenn Compliance aktiviert ist.
"Veraltet: GET Bucket-Konformität"	Veraltet, aber unterstützt: Gibt die aktuell gültigen Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zurück.
"Veraltet: PUT-Bucket-Konformität"	Veraltet, aber unterstützt: Ermöglicht Ihnen, die Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ändern.

GET Bucket-Konsistenz

Mit der Anforderung „GET Bucket Consistency“ können Sie die Konsistenz ermitteln, die auf einen bestimmten Bucket angewendet wird.

Die Standardkonsistenz ist so eingestellt, dass für neu erstellte Objekte das Lesen nach dem Schreiben gewährleistet ist.

Sie müssen über die Berechtigung s3:GetBucketConsistency verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwort

In der Antwort-XML `<Consistency>` gibt einen der folgenden Werte zurück:

Konsistenz	Beschreibung
alle	Alle Knoten empfangen die Daten sofort, andernfalls schlägt die Anforderung fehl.
stark-global	Garantiert Lese- und Schreibkonsistenz für alle Clientanforderungen auf allen Sites.
starke Site	Garantiert die Lese- und Schreibkonsistenz für alle Clientanforderungen innerhalb einer Site.
Lesen nach neuem Schreiben	(Standard) Bietet Read-After-Write-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
verfügbar	Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

Antwortbeispiel

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Ähnliche Informationen

"Konsistenzwerte"

PUT Bucket-Konsistenz

Mit der PUT-Bucket-Konsistenzanforderung können Sie die Konsistenz angeben, die auf Vorgänge angewendet werden soll, die an einem Bucket ausgeführt werden.

Die Standardkonsistenz ist so eingestellt, dass für neu erstellte Objekte das Lesen nach dem Schreiben gewährleistet ist.

Bevor Sie beginnen

Sie müssen über die Berechtigung „s3:PutBucketConsistency“ verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anfrage

Der `x-ntap-sg-consistency` Der Parameter muss einen der folgenden Werte enthalten:

Konsistenz	Beschreibung
alle	Alle Knoten empfangen die Daten sofort, andernfalls schlägt die Anforderung fehl.
stark-global	Garantiert Lese- und Schreibkonsistenz für alle Clientanforderungen auf allen Sites.
starke Site	Garantiert die Lese- und Schreibkonsistenz für alle Clientanforderungen innerhalb einer Site.
Lesen nach neuem Schreiben	(Standard) Bietet Read-After-Write-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
verfügbar	Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

Hinweis: Im Allgemeinen sollten Sie die Konsistenz „Lesen nach neuem Schreiben“ verwenden. Wenn Anfragen nicht richtig funktionieren, ändern Sie nach Möglichkeit das Verhalten des Anwendungsclients. Oder konfigurieren Sie den Client so, dass die Konsistenz für jede API-Anforderung angegeben wird. Stellen Sie die Konsistenz auf Eimerebene nur als letztes Mittel ein.

Anforderungsbeispiel

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ähnliche Informationen

"Konsistenzwerte"

GET Bucket – Letzte Zugriffszeit

Mit der Anforderung „GET Bucket last access time“ können Sie feststellen, ob Aktualisierungen der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind.

Sie müssen über die Berechtigung s3:GetBucketLastAccessTime verfügen oder Root-Kontobenutzer sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

Dieses Beispiel zeigt, dass Aktualisierungen der letzten Zugriffszeit für den Bucket aktiviert sind.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket: Letzte Zugriffszeit

Mit der Anforderung „PUT Bucket Last Access Time“ können Sie Aktualisierungen der letzten Zugriffszeit für einzelne Buckets aktivieren oder deaktivieren. Das Deaktivieren der Aktualisierung der letzten Zugriffszeit verbessert die Leistung und ist die

Standardeinstellung für alle Buckets, die mit Version 10.3.0 oder höher erstellt wurden.

Sie müssen über die Berechtigung s3:PutBucketLastAccessTime für einen Bucket verfügen oder Konto-Root sein, um diesen Vorgang abzuschließen.

> Ab StorageGRID Version 10.3 sind Aktualisierungen der letzten Zugriffszeit für alle neuen Buckets standardmäßig deaktiviert. Wenn Sie Buckets haben, die mit einer früheren Version von StorageGRID erstellt wurden, und Sie das neue Standardverhalten übernehmen möchten, müssen Sie die Aktualisierung der letzten Zugriffszeit für jeden dieser früheren Buckets explizit deaktivieren. Sie können Aktualisierungen der letzten Zugriffszeit mithilfe der Anforderung „PUT Bucket-Letztzugriffszeit“ oder auf der Detailseite für einen Bucket im Mandanten-Manager aktivieren oder deaktivieren. Sehen "Aktivieren oder Deaktivieren der Aktualisierung der letzten Zugriffszeit" .

Wenn die Aktualisierung der letzten Zugriffszeit für einen Bucket deaktiviert ist, wird das folgende Verhalten auf Vorgänge im Bucket angewendet:

- GetObject-, GetObjectAcl-, GetObjectTagging- und HeadObject-Anfragen aktualisieren die letzte Zugriffszeit nicht. Das Objekt wird nicht zu Warteschlangen für die Auswertung des Information Lifecycle Management (ILM) hinzugefügt.
- CopyObject- und PutObjectTagging-Anfragen, die nur die Metadaten aktualisieren, aktualisieren auch die letzte Zugriffszeit. Das Objekt wird zur ILM-Auswertung zu Warteschlangen hinzugefügt.
- Wenn Aktualisierungen der letzten Zugriffszeit für den Quell-Bucket deaktiviert sind, aktualisieren CopyObject-Anfragen die letzte Zugriffszeit für den Quell-Bucket nicht. Das kopierte Objekt wird nicht zu den Warteschlangen für die ILM-Auswertung für den Quell-Bucket hinzugefügt. Für das Ziel aktualisieren CopyObject-Anfragen jedoch immer die letzte Zugriffszeit. Die Kopie des Objekts wird zur ILM-Auswertung zu Warteschlangen hinzugefügt.
- CompleteMultipartUpload-Anfragen aktualisieren die letzte Zugriffszeit. Das fertige Objekt wird zur ILM-Auswertung in die Warteschlangen aufgenommen.

Anforderungsbeispiele

Dieses Beispiel aktiviert die letzte Zugriffszeit für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Dieses Beispiel deaktiviert die letzte Zugriffszeit für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Konfiguration der Benachrichtigung über DELETE-Bucket-Metadaten

Mit der Konfigurationsanforderung „DELETE Bucket-Metadaten-Benachrichtigung“ können Sie den Suchintegrationsdienst für einzelne Buckets deaktivieren, indem Sie die Konfigurations-XML löschen.

Sie müssen über die Berechtigung s3:DeleteBucketMetadataNotification für einen Bucket verfügen oder Konto-Root sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Dieses Beispiel zeigt das Deaktivieren des Suchintegrationsdienstes für einen Bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

GET Bucket-Metadaten-Benachrichtigungskonfiguration

Mit der Konfigurationsanforderung „GET Bucket-Metadatenbenachrichtigung“ können Sie die Konfigurations-XML abrufen, die zum Konfigurieren der Suchintegration für einzelne Buckets verwendet wird.

Sie müssen über die Berechtigung s3:GetBucketMetadataNotification verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Diese Anfrage ruft die Metadaten-Benachrichtigungskonfiguration für den Bucket mit dem Namen ab. `bucket` .

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwort

Der Antworttext enthält die Metadatenbenachrichtigungskonfiguration für den Bucket. Mit der Konfiguration der Metadatenbenachrichtigung können Sie festlegen, wie der Bucket für die Suchintegration konfiguriert wird. Das heißt, Sie können feststellen, welche Objekte indiziert werden und an welche Endpunkte ihre Objektmetadaten gesendet werden.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Jede Metadatenbenachrichtigungskonfiguration umfasst eine oder mehrere Regeln. Jede Regel gibt die Objekte an, auf die sie angewendet wird, und das Ziel, an das StorageGRID Objektmetadaten senden soll. Ziele müssen mithilfe der URN eines StorageGRID Endpunkts angegeben werden.

Name	Beschreibung	Erforderlich
Metadatenbenachrichtigungskonfiguration	Container-Tag für Regeln, die zum Angeben der Objekte und des Ziels für Metadatenbenachrichtigungen verwendet werden. Enthält ein oder mehrere Regelelemente.	Ja
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten einem angegebenen Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration-Element enthalten.	Ja
AUSWEIS	Eindeutige Kennung für die Regel. Im Regelelement enthalten.	Nein
Status	Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen. Im Regelelement enthalten.	Ja

Name	Beschreibung	Erforderlich
Präfix	Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet. Um alle Objekte abzugleichen, geben Sie ein leeres Präfix an. Im Regelelement enthalten.	Ja
Ziel	Container-Tag für das Ziel einer Regel. Im Regelelement enthalten.	Ja
Urne	URN des Ziels, an das die Objektmetadaten gesendet werden. Muss die URN eines StorageGRID -Endpunkts mit den folgenden Eigenschaften sein: • `es`muss das dritte Element sein. • Die URN muss mit dem Index und Typ enden, in dem die Metadaten gespeichert sind, in der Form `domain-name/myindex/mytype` . Endpunkte werden mithilfe des Tenant Managers oder der Tenant Management API konfiguriert. Sie haben folgende Form: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML übermittelt wird, andernfalls schlägt die Konfiguration mit einem 404-Fehler fehl. Die Urne ist im Zielelement enthalten.	Ja

Antwortbeispiel

Das XML, das zwischen den `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Tags zeigen, wie die Integration mit einem Suchintegrationsendpunkt für den Bucket konfiguriert ist. In diesem Beispiel werden Objektmetadaten an einen Elasticsearch-Index namens gesendet. `current` und geben Sie den Namen ein `2017` das in einer AWS-Domäne namens gehostet wird `records` .

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Ähnliche Informationen

"Verwenden eines Mandantenkontos"

Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten

Mit der Konfigurationsanforderung für die Benachrichtigung über PUT-Bucket-Metadaten können Sie den Suchintegrationsdienst für einzelne Buckets aktivieren. Die XML-Konfigurations-XML für die Metadatenbenachrichtigung, die Sie im Anforderungstext angeben, gibt die Objekte an, deren Metadaten an den Zielsuchindex gesendet werden.

Sie müssen über die Berechtigung s3:PutBucketMetadataNotification für einen Bucket verfügen oder Konto-Root sein, um diesen Vorgang abzuschließen.

Anfrage

Die Anfrage muss die Metadatenbenachrichtigungskonfiguration im Anfragetext enthalten. Jede Metadatenbenachrichtigungskonfiguration umfasst eine oder mehrere Regeln. Jede Regel gibt die Objekte an, auf die sie angewendet wird, und das Ziel, an das StorageGRID Objektmetadaten senden soll.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise könnten Sie Metadaten für Objekte mit dem Präfix `/images` zu einem Ziel und Objekte mit dem Präfix `/videos` zu einem anderen.

Konfigurationen mit überlappenden Präfixen sind ungültig und werden bei der Übermittlung abgelehnt. Beispielsweise eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` und eine zweite Regel für Objekte mit dem Präfix `test2` wäre nicht erlaubt.

Ziele müssen mithilfe der URN eines StorageGRID Endpunkts angegeben werden. Der Endpunkt muss vorhanden sein, wenn die Konfiguration der Metadatenbenachrichtigung übermittelt wird, sonst schlägt die

Anfrage fehl, da `400 Bad Request` Die Fehlermeldung lautet: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Die Tabelle beschreibt die Elemente in der XML-Konfiguration der Metadatenbenachrichtigung.

Name	Beschreibung	Erforderlich
Metadatenbenachrichtigungskonfiguration	Container-Tag für Regeln, die zum Angeben der Objekte und des Ziels für Metadatenbenachrichtigungen verwendet werden. Enthält ein oder mehrere Regelelemente.	Ja
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten einem angegebenen Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration-Element enthalten.	Ja
AUSWEIS	Eindeutige Kennung für die Regel. Im Regelelement enthalten.	Nein

Name	Beschreibung	Erforderlich
Status	Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen. Im Regelelement enthalten.	Ja
Präfix	Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet. Um alle Objekte abzugleichen, geben Sie ein leeres Präfix an. Im Regelelement enthalten.	Ja
Ziel	Container-Tag für das Ziel einer Regel. Im Regelelement enthalten.	Ja
Urne	URN des Ziels, an das die Objektmetadaten gesendet werden. Muss die URN eines StorageGRID -Endpunkts mit den folgenden Eigenschaften sein: • `es`muss das dritte Element sein. • Die URN muss mit dem Index und Typ enden, in dem die Metadaten gespeichert sind, in der Form `domain-name/myindex/mytype` . Endpunkte werden mithilfe des Tenant Managers oder der Tenant Management API konfiguriert. Sie haben folgende Form: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML übermittelt wird, andernfalls schlägt die Konfiguration mit einem 404-Fehler fehl. Die Urne ist im Zielelement enthalten.	Ja

Anforderungsbeispiele

Dieses Beispiel zeigt die Aktivierung der Suchintegration für einen Bucket. In diesem Beispiel werden die Objektmetadaten für alle Objekte an dasselbe Ziel gesendet.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

In diesem Beispiel werden Objektmetadaten für Objekte verwendet, die mit dem Präfix `/images` wird an ein Ziel gesendet, während Objektmetadaten für Objekte, die dem Präfix entsprechen `/videos` wird an ein zweites Ziel gesendet.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Vom Suchintegrationsdienst generiertes JSON

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, wird jedes Mal, wenn Objektmetadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden, ein JSON-Dokument generiert und an den Zielendpunkt gesendet.

Dieses Beispiel zeigt ein Beispiel des JSON, das generiert werden könnte, wenn ein Objekt mit dem Schlüssel `SGWS/Tagging.txt` wird in einem Bucket namens erstellt `test` . Der `test` Bucket ist nicht versioniert, also die `versionId` -Tag ist leer.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

In Metadatenbenachrichtigungen enthaltene Objektmetadaten

In der Tabelle sind alle Felder aufgeführt, die im JSON-Dokument enthalten sind, das an den Zielendpunkt gesendet wird, wenn die Suchintegration aktiviert ist.

Der Dokumentname umfasst den Bucket-Namen, den Objektnamen und die Versions-ID, falls vorhanden.

Typ	Artikelname	Beschreibung
Bucket- und Objektinformationen	Eimer	Name des Buckets
Bucket- und Objektinformationen	Schlüssel	Objektschlüsselname
Bucket- und Objektinformationen	Versions-ID	Objektversion für Objekte in versionierten Buckets
Bucket- und Objektinformationen	Region	Bucket-Region, zum Beispiel `us-east-1`
Systemmetadaten	Größe	Objektgröße (in Bytes), wie sie für einen HTTP-Client sichtbar ist
Systemmetadaten	md5	Objekt-Hash
Benutzermetadaten	Metadaten *`key:value`*	Alle Benutzermetadaten für das Objekt als Schlüssel-Wert-Paare
Schlagwörter	Schlagworte *`key:value`*	Alle für das Objekt definierten Objekt-Tags als Schlüssel-Wert-Paare

Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur Zuordnung von Datumsformaten. Sie müssen die dynamischen Feldzuordnungen im Index aktivieren, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Ähnliche Informationen

"Verwenden eines Mandantenkontos"

GET-Speichernutzungsanforderung

Die Anforderung „GET Storage Usage“ gibt Auskunft über die Gesamtmenge des von einem Konto und jedem mit dem Konto verknüpften Bucket verwendeten Speichers.

Die Menge des von einem Konto und seinen Buckets verwendeten Speichers kann durch eine modifizierte ListBuckets-Anfrage mit dem `x-ntap-sg-usage` Abfrageparameter. Die Bucket-Speichernutzung wird getrennt von den vom System verarbeiteten PUT- und DELETE-Anfragen verfolgt. Es kann zu einer gewissen Verzögerung kommen, bevor die Nutzungswerte den erwarteten Werten auf Grundlage der Verarbeitung von Anfragen entsprechen, insbesondere wenn das System stark ausgelastet ist.

Standardmäßig versucht StorageGRID , Nutzungsinformationen mithilfe einer starken globalen Konsistenz abzurufen. Wenn keine starke globale Konsistenz erreicht werden kann, versucht StorageGRID , die Nutzungsinformationen mit einer starken Site-Konsistenz abzurufen.

Sie müssen über die Berechtigung s3:ListAllMyBuckets verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

Dieses Beispiel zeigt ein Konto mit vier Objekten und 12 Byte Daten in zwei Buckets. Jeder Bucket enthält zwei Objekte und sechs Bytes Daten.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Versionierung

Jede gespeicherte Objektversion trägt dazu bei, `ObjectCount` Und `DataBytes` Werte in der Antwort. Löschmarkierungen werden nicht hinzugefügt zum `ObjectCount` gesamt.

Ähnliche Informationen

"Konsistenzwerte"

Veraltete Bucket-Anfragen für Legacy-Compliance

Veraltete Bucket-Anfragen für Legacy-Compliance

Möglicherweise müssen Sie die StorageGRID S3 REST-API verwenden, um Buckets zu verwalten, die mit der alten Compliance-Funktion erstellt wurden.

Compliance-Funktion veraltet

Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt.

Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, ist die globale S3-Objektsperreinstellung in StorageGRID 11.6 aktiviert. Sie können keine neuen Buckets mehr erstellen, wenn Compliance aktiviert ist. Bei Bedarf können Sie jedoch die StorageGRID S3 REST API verwenden, um vorhandene ältere konforme Buckets zu verwalten.

- "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
- "Objekte mit ILM verwalten"
- "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"

Veraltete Compliance-Anfragen:

- "Veraltet – PUT-Bucket-Anforderungsänderungen zur Einhaltung der Vorschriften"

  Das XML-Element SGCompliance ist veraltet. Bisher konnten Sie dieses benutzerdefinierte StorageGRID Element in den optionalen XML-Anforderungstext von PUT-Bucket-Anforderungen aufnehmen, um einen konformen Bucket zu erstellen.

- "Veraltet – GET Bucket-Konformität"

  Die GET Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die aktuell geltenden Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ermitteln.

- "Veraltet – PUT-Bucket-Konformität"

  Die PUT-Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ändern. Sie können beispielsweise einen vorhandenen Bucket auf Legal Hold setzen oder seine Aufbewahrungsdauer verlängern.

Veraltet: CreateBucket-Anforderungsänderungen zur Einhaltung der Vorschriften

Das XML-Element SGCompliance ist veraltet. Bisher konnten Sie dieses benutzerdefinierte StorageGRID Element in den optionalen XML-Anforderungstext von CreateBucket-Anforderungen aufnehmen, um einen konformen Bucket zu erstellen.

> Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt. Weitere Einzelheiten finden Sie im Folgenden:
>
> - "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
> - "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"

Sie können keine neuen Buckets mehr erstellen, wenn Compliance aktiviert ist. Die folgende Fehlermeldung wird zurückgegeben, wenn Sie versuchen, mithilfe der CreateBucket-Anforderungsänderungen für die Konformität einen neuen konformen Bucket zu erstellen:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Veraltet: GET Bucket-Compliance-Anforderung

Die GET Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die aktuell geltenden Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ermitteln.

> Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt. Weitere Einzelheiten finden Sie im Folgenden:
>
> - "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
> - "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"

Sie müssen über die Berechtigung s3:GetBucketCompliance verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Mit dieser Beispielanfrage können Sie die Compliance-Einstellungen für den Bucket mit dem Namen ermitteln. `mybucket` .

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

In der Antwort-XML `<SGCompliance>` listet die für den Bucket geltenden Compliance-Einstellungen auf. Diese Beispielantwort zeigt die Compliance-Einstellungen für einen Bucket, in dem jedes Objekt ab dem Zeitpunkt der Aufnahme des Objekts in das Grid ein Jahr lang (525.600 Minuten) aufbewahrt wird. Für diesen Bucket besteht derzeit keine rechtliche Sperre. Jedes Objekt wird nach einem Jahr automatisch gelöscht.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Name	Beschreibung
Aufbewahrungsdauer in Minuten	Die Länge der Aufbewahrungsfrist für diesem Bucket hinzugefügte Objekte in Minuten. Die Aufbewahrungsfrist beginnt, wenn das Objekt in das Raster aufgenommen wird.
LegalHold	• True: Dieser Bucket unterliegt derzeit einer rechtlichen Sperre. Objekte in diesem Bucket können erst gelöscht werden, wenn die rechtliche Sperre aufgehoben wird, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Bucket unterliegt derzeit keiner rechtlichen Sperre. Objekte in diesem Bucket können gelöscht werden, wenn ihre Aufbewahrungsfrist abgelaufen ist.
AutoDelete	• True: Die Objekte in diesem Bucket werden automatisch gelöscht, wenn ihre Aufbewahrungsfrist abläuft, es sei denn, der Bucket unterliegt einer rechtlichen Sperre. • Falsch: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abläuft. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Fehlerantworten

Wenn der Bucket nicht konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort `404 Not Found`, mit einem S3-Fehlercode von `XNoSuchBucketCompliance`.

Veraltet: PUT Bucket-Compliance-Anforderung

Die PUT-Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ändern. Sie können beispielsweise einen vorhandenen Bucket auf Legal Hold setzen oder seine Aufbewahrungsdauer verlängern.

> Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt. Weitere Einzelheiten finden Sie im Folgenden:
>
> - "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
> - "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"

Sie müssen über die Berechtigung s3:PutBucketCompliance verfügen oder Root-Kontobenutzer sein, um diesen Vorgang abzuschließen.

Sie müssen für jedes Feld der Compliance-Einstellungen einen Wert angeben, wenn Sie eine PUT-Bucket-Compliance-Anforderung stellen.

Anforderungsbeispiel

Diese Beispielanforderung ändert die Compliance-Einstellungen für den Bucket mit dem Namen `mybucket`. In diesem Beispiel werden Objekte in `mybucket` werden nun zwei Jahre (1.051.200 Minuten) statt einem Jahr

aufbewahrt, beginnend mit der Aufnahme des Objekts in das Grid. Für diesen Bucket besteht keine rechtliche Sperre. Jedes Objekt wird nach zwei Jahren automatisch gelöscht.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Name	Beschreibung
Aufbewahrungsdauer in Minuten	Die Länge der Aufbewahrungsfrist für diesem Bucket hinzugefügte Objekte in Minuten. Die Aufbewahrungsfrist beginnt, wenn das Objekt in das Raster aufgenommen wird. **Wichtig** Wenn Sie einen neuen Wert für RetentionPeriodMinutes angeben, müssen Sie einen Wert angeben, der gleich oder größer als die aktuelle Aufbewahrungsdauer des Buckets ist. Nachdem die Aufbewahrungsdauer des Buckets festgelegt wurde, können Sie diesen Wert nicht mehr verringern, sondern nur erhöhen.
LegalHold	• True: Dieser Bucket unterliegt derzeit einer rechtlichen Sperre. Objekte in diesem Bucket können erst gelöscht werden, wenn die rechtliche Sperre aufgehoben wird, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Bucket unterliegt derzeit keiner rechtlichen Sperre. Objekte in diesem Bucket können gelöscht werden, wenn ihre Aufbewahrungsfrist abgelaufen ist.
AutoDelete	• True: Die Objekte in diesem Bucket werden automatisch gelöscht, wenn ihre Aufbewahrungsfrist abläuft, es sei denn, der Bucket unterliegt einer rechtlichen Sperre. • Falsch: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abläuft. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Konsistenz für Compliance-Einstellungen

Wenn Sie die Compliance-Einstellungen für einen S3-Bucket mit einer PUT-Bucket-Compliance-Anforderung aktualisieren, versucht StorageGRID , die Metadaten des Buckets im gesamten Grid zu aktualisieren. Standardmäßig verwendet StorageGRID die **starke globale** Konsistenz, um zu gewährleisten, dass alle Rechenzentrumsstandorte und alle Speicherknoten, die Bucket-Metadaten enthalten, für die geänderten

Compliance-Einstellungen eine Lese-nach-Schreib-Konsistenz aufweisen.

Wenn StorageGRID die **Starke globale** Konsistenz nicht erreichen kann, weil ein Rechenzentrumsstandort oder mehrere Speicherknoten an einem Standort nicht verfügbar sind, lautet der HTTP-Statuscode für die Antwort `503 Service Unavailable.`

Wenn Sie diese Antwort erhalten, müssen Sie sich an den Grid-Administrator wenden, um sicherzustellen, dass die erforderlichen Speicherdienste so schnell wie möglich bereitgestellt werden. Wenn der Grid-Administrator nicht in der Lage ist, genügend Speicherknoten an jedem Standort verfügbar zu machen, weist Sie der technische Support möglicherweise an, die fehlgeschlagene Anfrage zu wiederholen, indem er die **Strong-Site**-Konsistenz erzwingt.

> Erzwingen Sie niemals die **Strong-Site**-Konsistenz für die PUT-Bucket-Konformität, es sei denn, Sie wurden vom technischen Support dazu aufgefordert und sind sich der möglichen Konsequenzen der Verwendung dieser Ebene bewusst.

Wenn die Konsistenz auf **Strong-Site** reduziert wird, garantiert StorageGRID , dass aktualisierte Compliance-Einstellungen nur für Clientanforderungen innerhalb einer Site eine Read-After-Write-Konsistenz aufweisen. Dies bedeutet, dass das StorageGRID -System vorübergehend mehrere inkonsistente Einstellungen für diesen Bucket haben könnte, bis alle Sites und Storage Nodes verfügbar sind. Die inkonsistenten Einstellungen können zu unerwartetem und unerwünschtem Verhalten führen. Wenn Sie beispielsweise einen Bucket einer rechtlichen Sperre unterziehen und eine geringere Konsistenz erzwingen, bleiben die vorherigen Compliance-Einstellungen des Buckets (d. h. die rechtliche Sperre) an einigen Rechenzentrumsstandorten möglicherweise weiterhin wirksam. Dies hat zur Folge, dass Objekte, die Ihrer Meinung nach rechtlich gesperrt sind, nach Ablauf ihrer Aufbewahrungsfrist möglicherweise gelöscht werden, entweder durch den Benutzer oder durch AutoDelete (sofern aktiviert).

Um die Verwendung der **Strong-site**-Konsistenz zu erzwingen, stellen Sie die PUT Bucket-Compliance-Anforderung erneut aus und schließen Sie die `Consistency-Control` HTTP-Anforderungsheader, wie folgt:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Fehlerantworten

- Wenn der Bucket nicht konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort `404 Not Found` .
- Wenn `RetentionPeriodMinutes` in der Anfrage kleiner ist als die aktuelle Aufbewahrungsdauer des Buckets, lautet der HTTP-Statuscode `400 Bad Request` .

Ähnliche Informationen

"Veraltet: PUT-Bucket-Anforderungsänderungen zur Einhaltung der Vorschriften"

Bucket- und Gruppenzugriffsrichtlinien

Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien

StorageGRID verwendet die Richtliniensprache von Amazon Web Services (AWS), um S3-Mietern die Kontrolle über den Zugriff auf Buckets und Objekte in diesen Buckets zu ermöglichen. Das StorageGRID -System implementiert eine Teilmenge der S3 REST API-

Richtliniensprache. Zugriffsrichtlinien für die S3-API sind in JSON geschrieben.

Übersicht über die Zugriffsrichtlinie

StorageGRID unterstützt zwei Arten von Zugriffsrichtlinien.

- **Bucket-Richtlinien**, die mithilfe der S3-API-Operationen GetBucketPolicy, PutBucketPolicy und DeleteBucketPolicy oder der Tenant Manager- oder Tenant Management-API verwaltet werden. Bucket-Richtlinien sind an Buckets angehängt und daher so konfiguriert, dass sie den Zugriff von Benutzern im Bucket-Eigentümerkonto oder anderen Konten auf den Bucket und die darin enthaltenen Objekte steuern. Eine Bucket-Richtlinie gilt nur für einen Bucket und möglicherweise für mehrere Gruppen.
- **Gruppenrichtlinien**, die mithilfe des Tenant Managers oder der Tenant Management API konfiguriert werden. Gruppenrichtlinien sind einer Gruppe im Konto zugeordnet und daher so konfiguriert, dass diese Gruppe auf bestimmte Ressourcen zugreifen kann, die diesem Konto gehören. Eine Gruppenrichtlinie gilt nur für eine Gruppe und möglicherweise mehrere Buckets.

Es gibt keinen Unterschied in der Priorität zwischen Gruppen- und Bucket-Richtlinien.

StorageGRID Bucket- und Gruppenrichtlinien folgen einer bestimmten, von Amazon definierten Grammatik. Innerhalb jeder Richtlinie befindet sich ein Array von Richtlinienanweisungen und jede Anweisung enthält die folgenden Elemente:

- Anweisungs-ID (Sid) (optional)
- Wirkung
- Auftraggeber/NichtAuftraggeber
- Ressource/NichtRessource
- Aktion/NichtAktion
- Bedingung (optional)

Richtlinienanweisungen werden mithilfe dieser Struktur erstellt, um Berechtigungen anzugeben: Gewähren Sie <Effekt>, um <Principal> die Ausführung von <Aktion> auf <Ressource> zu erlauben/verweigern, wenn <Bedingung> zutrifft.

Jedes Richtlinienelement wird für eine bestimmte Funktion verwendet:

Element	Beschreibung
Sid	Das Sid-Element ist optional. Die Sid dient lediglich als Beschreibung für den Benutzer. Es wird gespeichert, aber nicht vom StorageGRID -System interpretiert.
Wirkung	Verwenden Sie das Effect-Element, um festzulegen, ob die angegebenen Vorgänge zulässig oder verweigert werden. Sie müssen Vorgänge, die Sie für Buckets oder Objekte zulassen (oder verweigern), mithilfe der unterstützten Schlüsselwörter des Aktionselements identifizieren.

Element	Beschreibung
Auftraggeber/NichtAuftraggeber	Sie können Benutzern, Gruppen und Konten den Zugriff auf bestimmte Ressourcen und die Ausführung bestimmter Aktionen gestatten. Wenn in der Anfrage keine S3-Signatur enthalten ist, wird der anonyme Zugriff durch Angabe des Platzhalterzeichens (*) als Prinzipal zugelassen. Standardmäßig hat nur der Konto-Root Zugriff auf die Ressourcen, die dem Konto gehören. Sie müssen nur das Principal-Element in einer Bucket-Richtlinie angeben. Bei Gruppenrichtlinien ist die Gruppe, an die die Richtlinie angehängt ist, das implizite Principal-Element.
Ressource/NichtRessource	Das Ressourcenelement identifiziert Buckets und Objekte. Sie können Berechtigungen für Buckets und Objekte erteilen oder verweigern, indem Sie den Amazon Resource Name (ARN) zur Identifizierung der Ressource verwenden.
Aktion/NichtAktion	Die Elemente „Aktion“ und „Effekt“ sind die beiden Komponenten von Berechtigungen. Wenn eine Gruppe eine Ressource anfordert, wird ihr der Zugriff auf die Ressource entweder gewährt oder verweigert. Der Zugriff wird verweigert, sofern Sie keine ausdrücklichen Berechtigungen erteilen. Sie können jedoch eine durch eine andere Richtlinie erteilte Berechtigung durch eine explizite Verweigerung außer Kraft setzen.
Zustand	Das Bedingungselement ist optional. Mithilfe von Bedingungen können Sie Ausdrücke erstellen, um zu bestimmen, wann eine Richtlinie angewendet werden soll.

Im Aktionselement können Sie das Platzhalterzeichen (*) verwenden, um alle Vorgänge oder eine Teilmenge von Vorgängen anzugeben. Diese Aktion entspricht beispielsweise Berechtigungen wie s3:GetObject, s3:PutObject und s3:DeleteObject.

```
s3:*Object
```

Im Ressourcenelement können Sie die Platzhalterzeichen (*) und (?) verwenden. Während das Sternchen (*) 0 oder mehr Zeichen entspricht, entspricht das Fragezeichen (?) einem beliebigen einzelnen Zeichen.

Im Principal-Element werden Platzhalterzeichen nur zum Festlegen des anonymen Zugriffs unterstützt, der jedem die Berechtigung erteilt. Beispielsweise legen Sie das Platzhalterzeichen (*) als Hauptwert fest.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

Im folgenden Beispiel verwendet die Anweisung die Elemente „Effect“, „Principal“, „Action“ und „Resource“. Dieses Beispiel zeigt eine vollständige Bucket-Richtlinienanweisung, die den Effekt "Zulassen" verwendet, um

den Principals, der Admin-Gruppe `federated-group/admin` und die Finanzgruppe `federated-group/finance` , Berechtigungen zum Ausführen der Aktion `s3:ListBucket` auf dem Eimer namens `mybucket` und die Aktion `s3:GetObject` auf allen Objekten in diesem Bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

Die Bucket-Richtlinie hat eine Größenbeschränkung von 20.480 Bytes und die Gruppenrichtlinie eine Größenbeschränkung von 5.120 Bytes.

Konsistenz für Richtlinien

Standardmäßig sind alle Aktualisierungen, die Sie an Gruppenrichtlinien vornehmen, letztendlich konsistent. Wenn eine Gruppenrichtlinie konsistent wird, kann es aufgrund der Richtlinienzwischenspeicherung weitere 15 Minuten dauern, bis die Änderungen wirksam werden. Standardmäßig sind alle Aktualisierungen, die Sie an Bucket-Richtlinien vornehmen, streng konsistent.

Bei Bedarf können Sie die Konsistenzgarantien für Bucket-Richtlinienaktualisierungen ändern. Beispielsweise möchten Sie möglicherweise, dass eine Änderung an einer Bucket-Richtlinie während eines Site-Ausfalls verfügbar ist.

In diesem Fall können Sie entweder die `Consistency-Control` Header in der PutBucketPolicy-Anforderung, oder Sie können die PUT Bucket-Konsistenzanforderung verwenden. Wenn eine Bucket-Richtlinie konsistent wird, kann es aufgrund der Richtlinienzwischenspeicherung weitere 8 Sekunden dauern, bis die Änderungen wirksam werden.

> Wenn Sie die Konsistenz auf einen anderen Wert einstellen, um eine vorübergehende Situation zu umgehen, denken Sie daran, die Einstellung auf Bucket-Ebene wieder auf den ursprünglichen Wert zurückzusetzen, wenn Sie fertig sind. Andernfalls verwenden alle zukünftigen Bucket-Anfragen die geänderte Einstellung.

Verwenden Sie ARN in Richtlinienanweisungen

In Richtlinienanweisungen wird die ARN in den Elementen „Principal“ und „Resource“ verwendet.

- Verwenden Sie diese Syntax, um die S3-Ressourcen-ARN anzugeben:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Verwenden Sie diese Syntax, um die ARN der Identitätsressource (Benutzer und Gruppen) anzugeben:

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Weitere Überlegungen:

- Sie können das Sternchen (*) als Platzhalter verwenden, um null oder mehr Zeichen im Objektschlüssel abzugleichen.
- Internationale Zeichen, die im Objektschlüssel angegeben werden können, sollten mit JSON UTF-8 oder mit JSON \u-Escapesequenzen codiert werden. Prozentkodierung wird nicht unterstützt.

  "RFC 2141 URN-Syntax"

  Der HTTP-Anforderungstext für den PutBucketPolicy-Vorgang muss mit charset=UTF-8 codiert sein.

Angeben von Ressourcen in einer Richtlinie

In Richtlinienanweisungen können Sie das Ressourcenelement verwenden, um den Bucket oder das Objekt anzugeben, für das Berechtigungen erteilt oder verweigert werden.

- Jede Richtlinienanweisung erfordert ein Ressourcenelement. In einer Richtlinie werden Ressourcen durch das Element gekennzeichnet `Resource` oder alternativ `NotResource` zum Ausschluss.
- Sie geben Ressourcen mit einer S3-Ressourcen-ARN an. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Sie können auch Richtlinienvariablen innerhalb des Objektschlüssels verwenden. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Der Ressourcenwert kann einen Bucket angeben, der beim Erstellen einer Gruppenrichtlinie noch nicht vorhanden ist.

Angeben von Prinzipalen in einer Richtlinie

Verwenden Sie das Principal-Element, um den Benutzer, die Gruppe oder das Mandantenkonto zu identifizieren, dem durch die Richtlinienanweisung der Zugriff auf die Ressource gestattet bzw. verweigert wird.

- Jede Richtlinienanweisung in einer Bucket-Richtlinie muss ein Principal-Element enthalten. Richtlinienanweisungen in einer Gruppenrichtlinie benötigen das Principal-Element nicht, da die Gruppe als Auftraggeber verstanden wird.
- In einer Richtlinie werden Auftraggeber durch das Element „Principal“ oder alternativ „NotPrincipal“ zum Ausschluss gekennzeichnet.
- Kontobasierte Identitäten müssen mithilfe einer ID oder einer ARN angegeben werden:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- In diesem Beispiel wird die Mandantenkonto-ID 27233906934684427525 verwendet, die das Stammkonto und alle Benutzer im Konto umfasst:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Sie können nur das Stammkonto angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Sie können einen bestimmten Verbundbenutzer („Alex“) angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Sie können eine bestimmte föderierte Gruppe („Manager“) angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Sie können einen anonymen Auftraggeber angeben:

```
"Principal": "*"
```

- Um Mehrdeutigkeiten zu vermeiden, können Sie anstelle des Benutzernamens die Benutzer-UUID verwenden:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

Nehmen wir beispielsweise an, Alex verlässt die Organisation und der Benutzername `Alex` wird gelöscht. Wenn ein neuer Alex in die Organisation eintritt und ihm die gleiche `Alex` Benutzernamen, könnte der neue Benutzer unbeabsichtigt die dem ursprünglichen Benutzer erteilten Berechtigungen erben.

- Der Prinzipalwert kann einen Gruppen-/Benutzernamen angeben, der beim Erstellen einer Bucket-Richtlinie noch nicht vorhanden ist.

Festlegen von Berechtigungen in einer Richtlinie

In einer Richtlinie wird das Aktionselement verwendet, um Berechtigungen für eine Ressource zuzulassen/zu verweigern. Es gibt eine Reihe von Berechtigungen, die Sie in einer Richtlinie angeben können. Diese werden durch das Element „Action“ oder alternativ „NotAction“ zum Ausschluss gekennzeichnet. Jedes dieser Elemente ist bestimmten S3 REST-API-Operationen zugeordnet.

In den Tabellen sind die Berechtigungen aufgeführt, die für Buckets gelten, und die Berechtigungen, die für Objekte gelten.

> Amazon S3 verwendet jetzt die Berechtigung s3:PutReplicationConfiguration sowohl für die Aktionen PutBucketReplication als auch DeleteBucketReplication. StorageGRID verwendet für jede Aktion separate Berechtigungen, was der ursprünglichen Amazon S3-Spezifikation entspricht.

> Ein Löschen wird ausgeführt, wenn ein Put zum Überschreiben eines vorhandenen Werts verwendet wird.

Berechtigungen, die für Buckets gelten

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:Bucket erstellen	Bucket erstellen	Ja. **Hinweis**: Nur in Gruppenrichtlinien verwenden.
s3:Bucket löschen	Bucket löschen	
s3:DeleteBucketMetadataNotification	Konfiguration der Benachrichtigung über DELETE-Bucket-Metadaten	Ja
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:Replikationskonfiguration löschen	DeleteBucketReplication	Ja, separate Berechtigungen für PUT und DELETE

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET Bucket-Konformität (veraltet)	Ja
s3:GetBucketConsistency	GET Bucket-Konsistenz	Ja
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	GET Bucket – Letzte Zugriffszeit	Ja
s3:GetBucketLocation	BucketLocation abrufen	
s3:GetBucketMetadataNotification	GET Bucket-Metadaten-Benachrichtigungskonfiguration	Ja
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListeAlleMeineBuckets	• Buckets auflisten • GET-Speichernutzung	Ja, für die GET-Speichernutzung. **Hinweis**: Nur in Gruppenrichtlinien verwenden.
s3:ListBucket	• ListObjects • Kopfeimer • RestoreObject	

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:ListBucketMultipartUploads	• ListMultipartUploads • RestoreObject	
s3:ListBucketVersions	GET Bucket-Versionen	
s3:PutBucketCompliance	PUT-Bucket-Konformität (veraltet)	Ja
s3:PutBucketConsistency	PUT Bucket-Konsistenz	Ja
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT Bucket: Letzte Zugriffszeit	Ja
s3:PutBucketMetadataNotification	Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten	Ja
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	• CreateBucket mit dem `x-amz-bucket-object-lock-enabled: true` Anforderungsheader (erfordert auch die Berechtigung s3:CreateBucket) • PutObjectLockConfiguration	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	• BucketTagging löschen† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Ja, separate Berechtigungen für PUT und DELETE

Berechtigungen, die für Objekte gelten

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
s3:BypassGovernanceRetention	• Objekt löschen • Objekte löschen • PutObjectRetention	
s3:Objekt löschen	• Objekt löschen • Objekte löschen • RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (eine bestimmte Version des Objekts)	
s3:DeleteObjectVersion	DeleteObject (eine bestimmte Version des Objekts)	
s3:GetObject	• GetObject • HeadObject • RestoreObject • SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (eine bestimmte Version des Objekts)	
s3:GetObjectVersion	GetObject (eine bestimmte Version des Objekts)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:PutObject	• PutObject • Objekt kopieren • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (eine bestimmte Version des Objekts)	
s3:PutOverwriteObject	• PutObject • Objekt kopieren • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload	Ja
s3:RestoreObject	RestoreObject	

PutOverwriteObject-Berechtigung verwenden

Die Berechtigung s3:PutOverwriteObject ist eine benutzerdefinierte StorageGRID Berechtigung, die für Vorgänge gilt, die Objekte erstellen oder aktualisieren. Die Einstellung dieser Berechtigung bestimmt, ob der Client die Daten, benutzerdefinierten Metadaten oder S3-Objektmarkierungen eines Objekts überschreiben kann.

Mögliche Einstellungen für diese Berechtigung sind:

- **Zulassen**: Der Client kann ein Objekt überschreiben. Dies ist die Standardeinstellung.
- **Ablehnen**: Der Client kann ein Objekt nicht überschreiben. Wenn die Berechtigung „PutOverwriteObject“ auf „Verweigern“ gesetzt ist, funktioniert sie wie folgt:
  - Wenn ein vorhandenes Objekt am gleichen Pfad gefunden wird:
    - Die Daten, benutzerdefinierten Metadaten oder S3-Objektmarkierungen des Objekts können nicht überschrieben werden.
    - Alle laufenden Aufnahmevorgänge werden abgebrochen und ein Fehler zurückgegeben.

        - Wenn die S3-Versionierung aktiviert ist, verhindert die Einstellung „Verweigern“, dass PutObjectTagging- oder DeleteObjectTagging-Vorgänge das TagSet für ein Objekt und seine nicht aktuellen Versionen ändern.
    - Wenn ein vorhandenes Objekt nicht gefunden wird, hat diese Berechtigung keine Wirkung.
- Wenn diese Berechtigung nicht vorhanden ist, ist die Wirkung dieselbe, als ob „Zulassen“ gesetzt wäre.

> Wenn die aktuelle S3-Richtlinie das Überschreiben zulässt und die Berechtigung „PutOverwriteObject“ auf „Verweigern“ gesetzt ist, kann der Client die Daten, benutzerdefinierten Metadaten oder Objektmarkierungen eines Objekts nicht überschreiben. Wenn außerdem das Kontrollkästchen **Client-Änderung verhindern** aktiviert ist (**KONFIGURATION** > **Sicherheitseinstellungen** > **Netzwerk und Objekte**), überschreibt diese Einstellung die Einstellung der Berechtigung „PutOverwriteObject“.

Bedingungen in einer Richtlinie angeben

Bedingungen definieren, wann eine Richtlinie in Kraft tritt. Bedingungen bestehen aus Operatoren und Schlüssel-Wert-Paaren.

Bedingungen verwenden Schlüssel-Wert-Paare zur Auswertung. Ein Bedingungselement kann mehrere Bedingungen enthalten und jede Bedingung kann mehrere Schlüssel-Wert-Paare enthalten. Der Bedingungsblock verwendet das folgende Format:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Im folgenden Beispiel verwendet die Bedingung „IpAddress“ den Bedingungsschlüssel „SourceIp“.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Unterstützte Bedingungsoperatoren

Bedingungsoperatoren werden wie folgt kategorisiert:

- Zeichenfolge
- Numerisch
- Boolescher Wert
- IP-Adresse
- Nullprüfung

Bedingungsoperatoren	Beschreibung
StringEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert auf Basis einer genauen Übereinstimmung (Groß-/Kleinschreibung beachten).
StringNotEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf negierter Übereinstimmung (Groß-/Kleinschreibung beachten).
StringEqualsIgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf einer genauen Übereinstimmung (Groß-/Kleinschreibung wird ignoriert).
StringNotEqualsIgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf negierter Übereinstimmung (Groß-/Kleinschreibung wird ignoriert).
StringLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert auf Basis einer genauen Übereinstimmung (Groß-/Kleinschreibung beachten). Kann die Platzhalterzeichen * und ? enthalten.
StringNotLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf negierter Übereinstimmung (Groß-/Kleinschreibung beachten). Kann die Platzhalterzeichen * und ? enthalten.
NumericEquals	Vergleicht einen Schlüssel mit einem numerischen Wert auf Basis einer exakten Übereinstimmung.
NumericNotEquals	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf negierter Übereinstimmung.
NumerischGrößerAls	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf einer „Größer-als“-Übereinstimmung.
NumerischGrößerAlsGleich	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf der Übereinstimmung „größer als oder gleich“.
NumericLessThan	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf einer „kleiner als“-Übereinstimmung.
NumerischKleinerAlsGleich	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf der Übereinstimmung „kleiner als oder gleich“.
Bool	Vergleicht einen Schlüssel mit einem Booleschen Wert basierend auf der Übereinstimmung „wahr oder falsch“.
IP-Adresse	Vergleicht einen Schlüssel mit einer IP-Adresse oder einem IP-Adressbereich.
NotIpAddress	Vergleicht einen Schlüssel mit einer IP-Adresse oder einem IP-Adressbereich basierend auf negierter Übereinstimmung.

Bedingungsoperatoren	Beschreibung
Null	Überprüft, ob im aktuellen Anforderungskontext ein Bedingungsschlüssel vorhanden ist.

Unterstützte Bedingungsschlüssel

Bedingungsschlüssel	Aktionen	Beschreibung
aws:SourceIp	IP-Betreiber	Wird mit der IP-Adresse verglichen, von der die Anfrage gesendet wurde. Kann für Bucket- oder Objektoperationen verwendet werden. **Hinweis:** Wenn die S3-Anforderung über den Load Balancer-Dienst auf Admin-Knoten und Gateway-Knoten gesendet wurde, wird dies mit der IP-Adresse vor dem Load Balancer-Dienst verglichen. **Hinweis**: Wenn ein nicht transparenter Load Balancer eines Drittanbieters verwendet wird, wird dies mit der IP-Adresse dieses Load Balancers verglichen. Beliebig `X-Forwarded-For` Header wird ignoriert, da seine Gültigkeit nicht festgestellt werden kann.
aws:Benutzername	Ressource/Identität	Wird mit dem Benutzernamen des Absenders verglichen, von dem die Anfrage gesendet wurde. Kann für Bucket- oder Objektoperationen verwendet werden.
s3:Trennzeichen	s3:ListBucket und s3:ListBucketVersions-Berechtigungen	Wird mit dem in einer ListObjects- oder ListObjectVersions-Anforderung angegebenen Trennzeichenparameter verglichen.

Bedingungsschlüssel	Aktionen	Beschreibung
s3:ExistingObjectTag/<Tag-Schlüssel>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Erfordert, dass das vorhandene Objekt über den spezifischen Tag-Schlüssel und -Wert verfügt.
s3:max-Schlüssel	s3:ListBucket und s3:ListBucketVersions-Berechtigungen	Wird mit dem in einer ListObjects- oder ListObjectVersions-Anforderung angegebenen Max-Keys-Parameter verglichen.
s3:Objektsperre-verbleibende-Aufbewahrungstage	s3:PutObject	Vergleicht mit dem Aufbewahrungsdatum, das in der `x-amz-object-lock-retain-until-date` Anforderungsheader oder berechnet aus der Standardaufbewahrungsdauer des Buckets, um sicherzustellen, dass diese Werte innerhalb des zulässigen Bereichs für die folgenden Anforderungen liegen: • PutObject • Objekt kopieren • CreateMultipartUpload
s3:Objektsperre-verbleibende-Aufbewahrungstage	s3:PutObjectRetention	Vergleicht mit dem in der PutObjectRetention-Anforderung angegebenen Aufbewahrungsdatum, um sicherzustellen, dass es innerhalb des zulässigen Bereichs liegt.

Bedingungsschlüssel	Aktionen	Beschreibung
s3:Präfix	s3:ListBucket und s3:ListBucketVersions-Berechtigungen	Wird mit dem in einer ListObjects- oder ListObjectVersions-Anforderung angegebenen Präfixparameter verglichen.
s3:RequestObjectTag/<Tag-Schlüssel>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Erfordert einen bestimmten Tag-Schlüssel und -Wert, wenn die Objektanforderung Tagging enthält.

Angeben von Variablen in einer Richtlinie

Sie können Variablen in Richtlinien verwenden, um Richtlinieninformationen einzufügen, wenn diese verfügbar sind. Sie können Richtlinienvariablen in der `Resource` Element und in Stringvergleichen im `Condition` Element.

In diesem Beispiel ist die Variable `${aws:username}` ist Teil des Ressourcenelements:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In diesem Beispiel ist die Variable `${aws:username}` ist Teil des Bedingungswerts im Bedingungsblock:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Beschreibung
`${aws:SourceIp}`	Verwendet den SourceIp-Schlüssel als bereitgestellte Variable.
`${aws:username}`	Verwendet den Benutzernamenschlüssel als bereitgestellte Variable.
`${s3:prefix}`	Verwendet den dienstspezifischen Präfixschlüssel als bereitgestellte Variable.
`${s3:max-keys}`	Verwendet den dienstspezifischen Max-Keys-Schlüssel als bereitgestellte Variable.
`${*}`	Sonderzeichen. Verwendet das Zeichen als wörtliches *-Zeichen.

Variable	Beschreibung
`${?}`	Sonderzeichen. Verwendet das Zeichen als wörtliches ?-Zeichen.
`${$}`	Sonderzeichen. Verwendet das Zeichen als wörtliches $-Zeichen.

Erstellen Sie Richtlinien, die eine besondere Behandlung erfordern

Manchmal kann eine Richtlinie Berechtigungen erteilen, die eine Gefahr für die Sicherheit oder den laufenden Betrieb darstellen, wie etwa das Sperren des Root-Benutzers des Kontos. Die StorageGRID S3 REST-API-Implementierung ist bei der Richtlinienvalidierung weniger restriktiv als Amazon, bei der Richtlinienauswertung jedoch ebenso streng.

Richtlinienbeschreibung	Richtlinientyp	Amazon-Verhalten	StorageGRID -Verhalten
Verweigern Sie sich selbst alle Berechtigungen für das Root-Konto	Eimer	Gültig und erzwungen, aber das Root-Benutzerkonto behält die Berechtigung für alle S3-Bucket-Richtlinienvorgänge	Dasselbe
Sich selbst alle Berechtigungen für Benutzer/Gruppe verweigern	Gruppe	Gültig und durchgesetzt	Dasselbe
Erteilen Sie einer fremden Kontogruppe alle Berechtigungen	Eimer	Ungültiger Auftraggeber	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405-Methodenfehler zurück, wenn sie durch eine Richtlinie erlaubt sind
Erteilen Sie einem fremden Root- oder Benutzerkonto alle Berechtigungen	Eimer	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405-Methodenfehler zurück, wenn sie durch eine Richtlinie erlaubt sind	Dasselbe
Jedem die Berechtigung für alle Aktionen erteilen	Eimer	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405-Methode nicht zulässig-Fehler für das Stammkonto und die Benutzer des Fremdkontos zurück	Dasselbe

Richtlinienbeschreibung	Richtlinientyp	Amazon-Verhalten	StorageGRID -Verhalten
Allen die Berechtigung für alle Aktionen verweigern	Eimer	Gültig und erzwungen, aber das Root-Benutzerkonto behält die Berechtigung für alle S3-Bucket-Richtlinienvorgänge	Dasselbe
Der Auftraggeber ist ein nicht vorhandener Benutzer oder eine nicht vorhandene Gruppe.	Eimer	Ungültiger Auftraggeber	Gültig
Ressource ist ein nicht vorhandener S3-Bucket	Gruppe	Gültig	Dasselbe
Principal ist eine lokale Gruppe	Eimer	Ungültiger Auftraggeber	Gültig
Die Richtlinie erteilt Nichtbesitzerkonten (einschließlich anonymer Konten) die Berechtigung, Objekte abzulegen.	Eimer	Gültig. Objekte sind Eigentum des Erstellerkontos und die Bucket-Richtlinie gilt nicht. Das Erstellerkonto muss mithilfe von Objekt-ACLs Zugriffsberechtigungen für das Objekt erteilen.	Gültig. Objekte sind Eigentum des Bucket-Eigentümerkontos. Es gilt die Bucket-Richtlinie.

WORM-Schutz (Write-Once-Read-Many)

Sie können WORM-Buckets (Write-Once-Read-Many) erstellen, um Daten, benutzerdefinierte Objektmetadaten und S3-Objekt-Tagging zu schützen. Sie konfigurieren die WORM-Buckets, um die Erstellung neuer Objekte zu ermöglichen und das Überschreiben oder Löschen vorhandener Inhalte zu verhindern. Verwenden Sie einen der hier beschriebenen Ansätze.

Um sicherzustellen, dass Überschreibungen immer verweigert werden, können Sie:

- Gehen Sie im Grid Manager zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** > **Netzwerk und Objekte** und aktivieren Sie das Kontrollkästchen **Client-Änderung verhindern**.
- Wenden Sie die folgenden Regeln und S3-Richtlinien an:
  - Fügen Sie der S3-Richtlinie eine PutOverwriteObject DENY-Operation hinzu.
  - Fügen Sie der S3-Richtlinie eine DeleteObject DENY-Operation hinzu.
  - Fügen Sie der S3-Richtlinie eine PutObject ALLOW-Operation hinzu.

> Das Festlegen von „DeleteObject“ auf „DENY“ in einer S3-Richtlinie verhindert nicht, dass ILM Objekte löscht, wenn eine Regel wie „Null Kopien nach 30 Tagen“ vorhanden ist.

Selbst wenn alle diese Regeln und Richtlinien angewendet werden, schützen sie nicht vor gleichzeitigen Schreibvorgängen (siehe Situation A). Sie schützen vor sequenziellen Überschreibungen (siehe Situation B).

Situation A: Gleichzeitige Schreibvorgänge (nicht geschützt)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situation B: Sequentielles Überschreiben abgeschlossen (vorbeugend)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Ähnliche Informationen

- "So verwalten StorageGRID ILM-Regeln Objekte"
- "Beispiele für Bucket-Richtlinien"
- "Beispiele für Gruppenrichtlinien"
- "Objekte mit ILM verwalten"
- "Verwenden eines Mandantenkontos"

Beispiele für Bucket-Richtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID Zugriffsrichtlinien für Buckets zu erstellen.

Bucket-Richtlinien geben die Zugriffsberechtigungen für den Bucket an, an den die Richtlinie angehängt ist. Sie konfigurieren eine Bucket-Richtlinie mithilfe der S3 PutBucketPolicy-API über eines dieser Tools:

- "Mietermanager" .
- AWS CLI mit diesem Befehl (siehe"Operationen an Buckets"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Beispiel: Allen Lesezugriff auf einen Bucket gewähren

In diesem Beispiel darf jeder, auch anonyme Benutzer, Objekte im Bucket auflisten und GetObject-Operationen für alle Objekte im Bucket ausführen. Alle anderen Vorgänge werden abgelehnt. Beachten Sie, dass diese Richtlinie möglicherweise nicht besonders nützlich ist, da niemand außer dem Konto-Root über die Berechtigung zum Schreiben in den Bucket verfügt.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Beispiel: Erlauben Sie allen Benutzern eines Kontos den Vollzugriff und allen Benutzern eines anderen Kontos den Lesezugriff auf einen Bucket.

In diesem Beispiel erhält jeder in einem angegebenen Konto vollen Zugriff auf einen Bucket, während jeder in einem anderen angegebenen Konto nur den Bucket auflisten und GetObject-Operationen für Objekte im Bucket ausführen darf, beginnend mit dem `shared/` Objektschlüsselpräfix.

> In StorageGRID sind Objekte, die von einem Nicht-Eigentümerkonto (einschließlich anonymer Konten) erstellt wurden, Eigentum des Bucket-Eigentümerkontos. Für diese Objekte gilt die Bucket-Richtlinie.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Beispiel: Erlauben Sie allen nur Lesezugriff auf einen Bucket und Vollzugriff für eine bestimmte Gruppe

In diesem Beispiel darf jeder, auch anonym, den Bucket auflisten und GetObject-Operationen für alle Objekte im Bucket durchführen, während nur Benutzer der Gruppe `Marketing` im angegebenen Konto wird der volle Zugriff gewährt.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Beispiel: Erlauben Sie jedem Lese- und Schreibzugriff auf einen Bucket, wenn sich der Client im IP-Bereich befindet

In diesem Beispiel darf jeder, auch anonyme Benutzer, den Bucket auflisten und beliebige Objektoperationen für alle Objekte im Bucket ausführen, vorausgesetzt, die Anforderungen stammen aus einem angegebenen IP-Bereich (54.240.143.0 bis 54.240.143.255, außer 54.240.143.188). Alle anderen Vorgänge werden abgelehnt und alle Anfragen außerhalb des IP-Bereichs werden abgelehnt.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Beispiel: Vollzugriff auf einen Bucket ausschließlich durch einen angegebenen Verbundbenutzer zulassen

In diesem Beispiel erhält der Verbundbenutzer Alex vollen Zugriff auf die `examplebucket` Bucket und seine Objekte. Allen anderen Benutzern, einschließlich „root“, werden sämtliche Vorgänge ausdrücklich verweigert. Beachten Sie jedoch, dass „root“ niemals die Berechtigung zum Put/Get/DeleteBucketPolicy verweigert wird.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Beispiel: PutOverwriteObject-Berechtigung

In diesem Beispiel `Deny` Die Wirkung von PutOverwriteObject und DeleteObject stellt sicher, dass niemand die Daten, benutzerdefinierten Metadaten und S3-Objektmarkierungen des Objekts überschreiben oder löschen kann.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Beispiele für Gruppenrichtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID Zugriffsrichtlinien für Gruppen zu erstellen.

Gruppenrichtlinien geben die Zugriffsberechtigungen für die Gruppe an, der die Richtlinie zugeordnet ist. Es gibt keine `Principal` Element in der Richtlinie, da es implizit ist. Gruppenrichtlinien werden mithilfe des Tenant Managers oder der API konfiguriert.

Beispiel: Festlegen der Gruppenrichtlinie mit dem Mandanten-Manager

Wenn Sie im Mandanten-Manager eine Gruppe hinzufügen oder bearbeiten, können Sie eine Gruppenrichtlinie auswählen, um festzulegen, welche S3-Zugriffsberechtigungen die Mitglieder dieser Gruppe haben. Sehen "Erstellen von Gruppen für einen S3-Mandanten" .

- **Kein S3-Zugriff**: Standardoption. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat standardmäßig nur der Root-Benutzer Zugriff auf S3-Ressourcen.
- **Nur-Lesezugriff**: Benutzer in dieser Gruppe haben nur Lesezugriff auf S3-Ressourcen. Beispielsweise können Benutzer dieser Gruppe Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine schreibgeschützte Gruppenrichtlinie im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.
- **Vollzugriff**: Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine Gruppenrichtlinie mit vollem Zugriff im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.
- **Ransomware-Minderung**: Diese Beispielrichtlinie gilt für alle Buckets dieses Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber keine Objekte dauerhaft aus Buckets löschen, für die die Objektversionierung aktiviert ist.

  Tenant Manager-Benutzer mit der Berechtigung „Alle Buckets verwalten“ können diese Gruppenrichtlinie außer Kraft setzen. Beschränken Sie die Berechtigung „Alle Buckets verwalten“ auf vertrauenswürdige Benutzer und verwenden Sie, sofern verfügbar, die Multi-Faktor-Authentifizierung (MFA).

- **Benutzerdefiniert**: Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.

Beispiel: Gruppe vollen Zugriff auf alle Buckets gewähren

In diesem Beispiel wird allen Mitgliedern der Gruppe der vollständige Zugriff auf alle Buckets gewährt, die dem Mandantenkonto gehören, sofern die Bucket-Richtlinie diesen Zugriff nicht ausdrücklich verweigert.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Beispiel: Gruppe schreibgeschützten Zugriff auf alle Buckets gewähren

In diesem Beispiel haben alle Mitglieder der Gruppe schreibgeschützten Zugriff auf S3-Ressourcen, sofern dies nicht ausdrücklich durch die Bucket-Richtlinie verweigert wird. Beispielsweise können Benutzer dieser Gruppe Objekte auflisten und Objektdaten, Metadaten und Tags lesen.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Beispiel: Gruppenmitgliedern vollen Zugriff nur auf ihren „Ordner“ in einem Bucket gewähren

In diesem Beispiel dürfen Mitglieder der Gruppe nur ihren spezifischen Ordner (Schlüsselpräfix) im angegebenen Bucket auflisten und darauf zugreifen. Beachten Sie, dass bei der Festlegung des Datenschutzes dieser Ordner Zugriffsberechtigungen aus anderen Gruppenrichtlinien und der Bucket-Richtlinie berücksichtigt werden sollten.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

In den Prüfprotokollen verfolgte S3-Operationen

Audit-Nachrichten werden von StorageGRID -Diensten generiert und in Textprotokolldateien gespeichert. Sie können die S3-spezifischen Prüfmeldungen im Prüfprotokoll überprüfen, um Details zu Bucket- und Objektvorgängen zu erhalten.

In den Audit-Protokollen verfolgte Bucket-Operationen

- Bucket erstellen
- Bucket löschen
- BucketTagging löschen
- Objekte löschen
- GetBucketTagging
- Kopfeimer
- ListObjects
- ListObjectVersions
- PUT Bucket-Konformität
- PutBucketTagging
- PutBucketVersioning

In den Überwachungsprotokollen verfolgte Objektvorgänge

- CompleteMultipartUpload
- Objekt kopieren
- Objekt löschen
- GetObject
- HeadObject
- PutObject
- RestoreObject
- Objekt auswählen
- UploadPart (wenn eine ILM-Regel eine ausgeglichene oder strikte Aufnahme verwendet)
- UploadPartCopy (wenn eine ILM-Regel eine ausgeglichene oder strikte Aufnahme verwendet)

Ähnliche Informationen

- "Zugriff auf die Überwachungsprotokolldatei"
- "Client schreibt Prüfmeldungen"
- "Client liest Audit-Nachrichten"

Swift REST API verwenden (Ende der Lebensdauer)

Verwenden Sie die Swift REST-API

Der Support für die Swift-API hat das Ende seiner Lebensdauer erreicht und wird in einer zukünftigen Version entfernt.

Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "StorageGRID 11.8: Swift REST API verwenden" .

Überwachen und beheben Sie Fehler eines StorageGRID -Systems

Überwachen Sie das StorageGRID -System

Überwachen Sie ein StorageGRID -System

Überwachen Sie Ihr StorageGRID System regelmäßig, um sicherzustellen, dass es die erwartete Leistung erbringt.

Bevor Sie beginnen

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

> Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Grid Manager und dann **Benutzereinstellungen**.

Informationen zu diesem Vorgang

Diese Anweisungen beschreiben Folgendes:

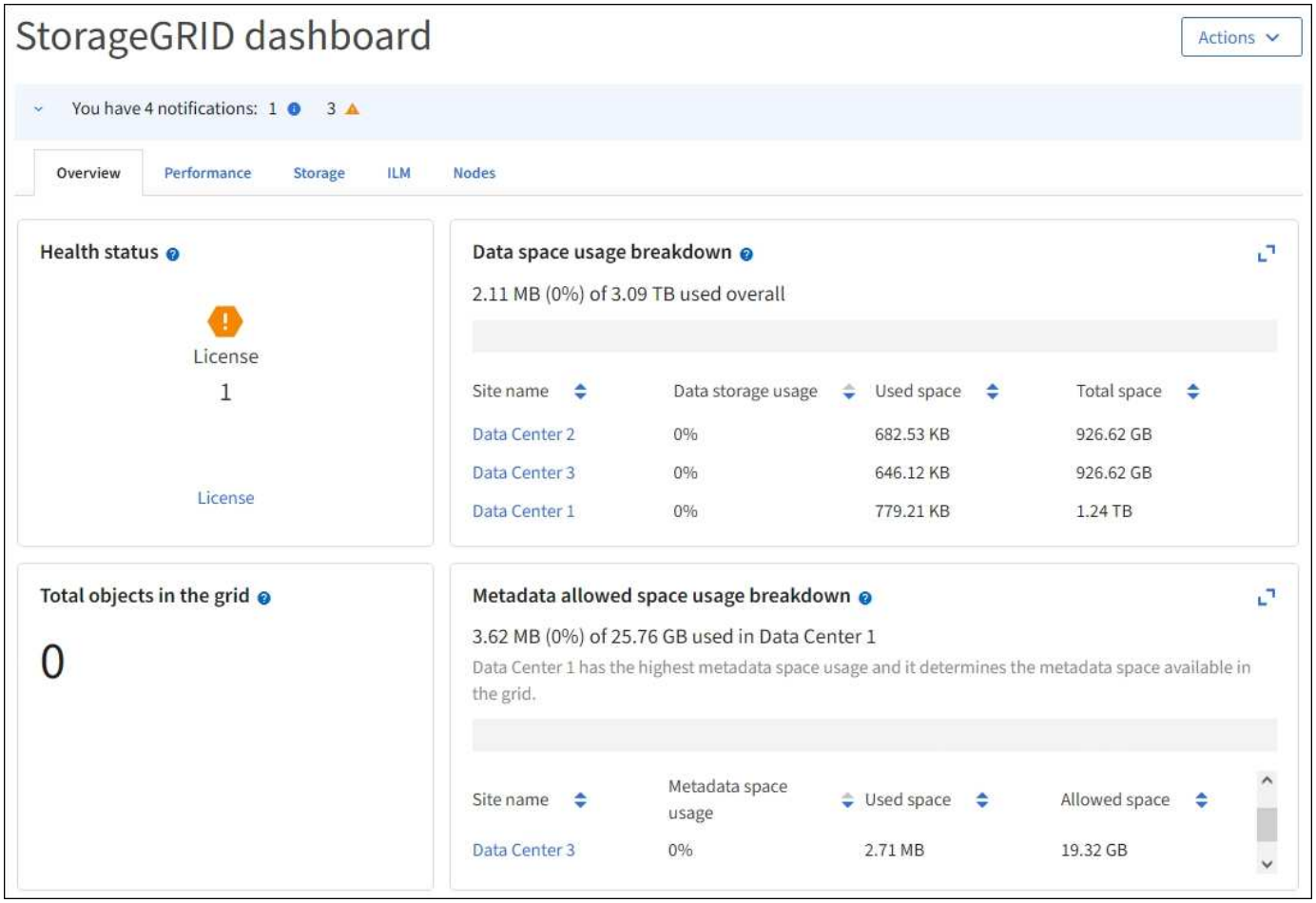
- "Anzeigen und Verwalten des Dashboards"
- "Anzeigen der Seite „Knoten“"
- "Überwachen Sie diese Aspekte des Systems regelmäßig:"
  - "Systemzustand"
  - "Speicherkapazität"
  - "Informationslebenszyklusmanagement"
  - "Netzwerk- und Systemressourcen"
  - "Mieteraktivität"
  - "Lastausgleichsvorgänge"
  - "Grid-Föderation-Verbindungen"
- "Verwalten von Warnungen"
- "Protokolldateien anzeigen"
- "Konfigurieren von Überwachungsmeldungen und Protokollzielen"
- "Verwenden Sie einen externen Syslog-Server"um Auditinformationen zu sammeln
- "Verwenden Sie SNMP zur Überwachung"
- "Erhalten Sie zusätzliche StorageGRID Daten", einschließlich Metriken und Diagnose

Anzeigen und Verwalten des Dashboards

Über das Dashboard können Sie die Systemaktivitäten auf einen Blick überwachen. Sie können benutzerdefinierte Dashboards erstellen, um Ihre StorageGRID-Implementierung zu überwachen.

Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Grid Manager und dann **Benutzereinstellungen**.

Ihr Dashboard kann je nach Systemkonfiguration unterschiedlich sein.



Dashboard anzeigen

Das Dashboard besteht aus Registerkarten, die spezifische Informationen zum StorageGRID -System enthalten. Jede Registerkarte enthält Kategorien von Informationen, die auf Karten angezeigt werden.

Sie können das vom System bereitgestellte Dashboard unverändert verwenden. Darüber hinaus können Sie benutzerdefinierte Dashboards erstellen, die nur die Registerkarten und Karten enthalten, die für die Überwachung Ihrer StorageGRID-Implementierung relevant sind.

Die vom System bereitgestellten Dashboard-Registerkarten enthalten Karten mit den folgenden Arten von Informationen:

Registerkarte auf dem vom System bereitgestellten Dashboard	Enthält
Überblick	Allgemeine Informationen zum Raster, z. B. aktive Warnungen, Speicherplatznutzung und Gesamtzahl der Objekte im Raster.

Registerkarte auf dem vom System bereitgestellten Dashboard	Enthält
Performance	Speicherplatznutzung, im Laufe der Zeit verwendeter Speicher, S3-Vorgänge, Anforderungsdauer, Fehlerrate.
Storage	Nutzung des Mandantenkontingents und Nutzung des logischen Speicherplatzes. Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten.
ILM	Warteschlange und Auswertungsrate für das Informationslebenszyklusmanagement.
Nodes	CPU-, Daten- und Speichernutzung nach Knoten. S3-Operationen nach Knoten. Knoten-zu-Site-Verteilung.

Einige der Karten können zur besseren Anzeige maximiert werden. Wählen Sie das Maximierungssymbol in der oberen rechten Ecke der Karte. Um eine maximierte Karte zu schließen, wählen Sie das Symbol „Minimieren“ oder wählen Sie **Schließen**.

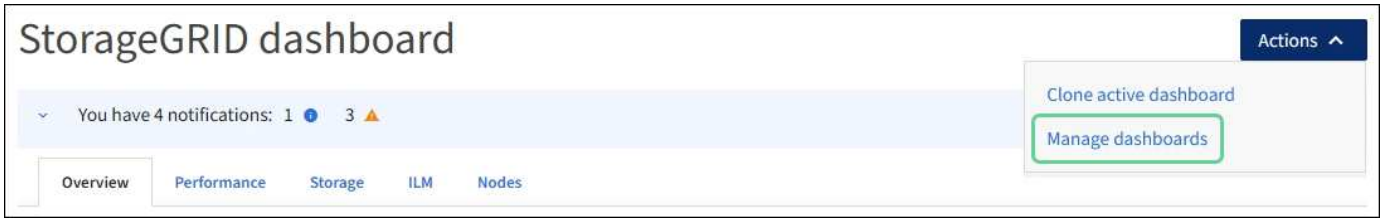
Dashboards verwalten

Wenn Sie Root-Zugriff haben (siehe"Berechtigungen der Administratorgruppe") können Sie die folgenden Verwaltungsaufgaben für Dashboards ausführen:

- Erstellen Sie ein benutzerdefiniertes Dashboard von Grund auf. Sie können benutzerdefinierte Dashboards verwenden, um zu steuern, welche StorageGRID -Informationen angezeigt werden und wie diese Informationen organisiert sind.
- Klonen Sie ein Dashboard, um benutzerdefinierte Dashboards zu erstellen.
- Legen Sie ein aktives Dashboard für einen Benutzer fest. Das aktive Dashboard kann das vom System bereitgestellte Dashboard oder ein benutzerdefiniertes Dashboard sein.
- Legen Sie ein Standard-Dashboard fest, das allen Benutzern angezeigt wird, sofern sie nicht ihr eigenes Dashboard aktivieren.
- Bearbeiten Sie einen Dashboard-Namen.
- Bearbeiten Sie ein Dashboard, um Registerkarten und Karten hinzuzufügen oder zu entfernen. Sie können mindestens 1 und höchstens 20 Registerkarten haben.
- Entfernen Sie ein Dashboard.

> Wenn Sie neben dem Root-Zugriff über eine andere Berechtigung verfügen, können Sie nur ein aktives Dashboard festlegen.

Um Dashboards zu verwalten, wählen Sie **Aktionen** > **Dashboards verwalten**.



Dashboards konfigurieren

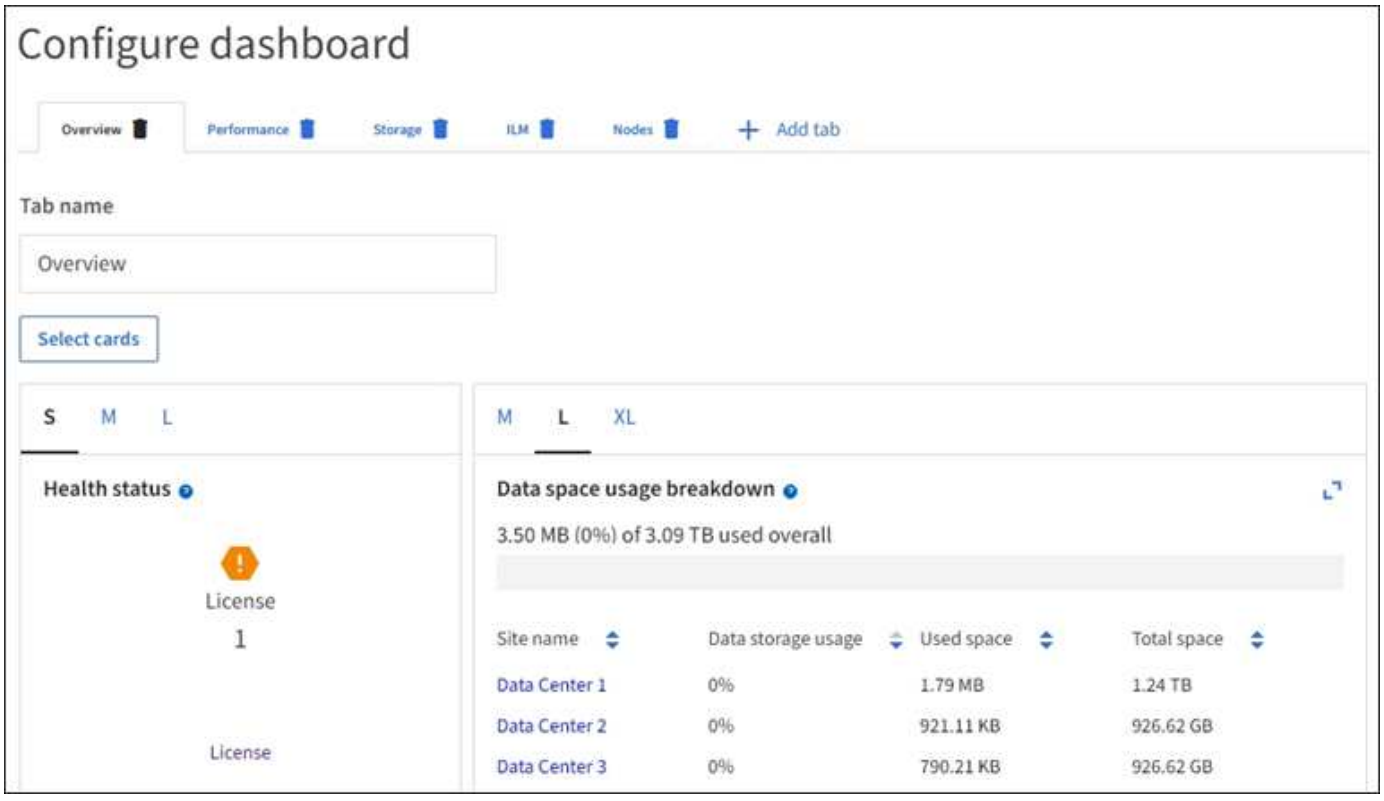
Um durch Klonen des aktiven Dashboards ein neues Dashboard zu erstellen, wählen Sie **Aktionen** > **Aktives Dashboard klonen**.

Um ein vorhandenes Dashboard zu bearbeiten oder zu klonen, wählen Sie **Aktionen** > **Dashboards verwalten**.

Das vom System bereitgestellte Dashboard kann nicht bearbeitet oder entfernt werden.

Beim Konfigurieren eines Dashboards können Sie:

- Registerkarten hinzufügen oder entfernen
- Benennen Sie Registerkarten um und geben Sie neuen Registerkarten eindeutige Namen
- Karten für jede Registerkarte hinzufügen, entfernen oder neu anordnen (ziehen)
- Wählen Sie die Größe für einzelne Karten, indem Sie oben auf der Karte **S**, **M**, **L** oder **XL** auswählen



Anzeigen der Seite „Knoten“

Anzeigen der Seite „Knoten“

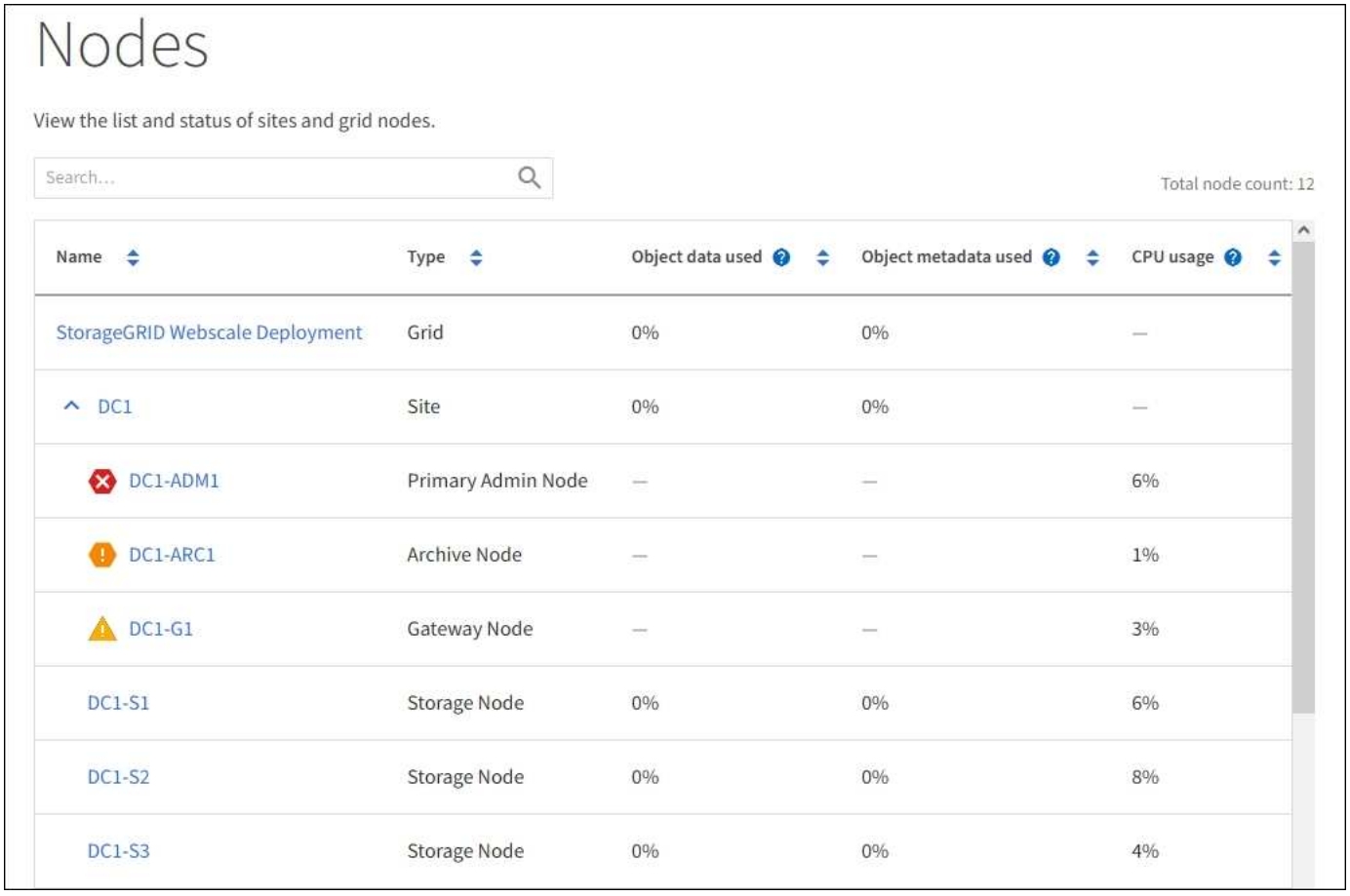
Wenn Sie detailliertere Informationen zu Ihrem StorageGRID -System benötigen, als das Dashboard bietet, können Sie auf der Seite „Knoten“ Metriken für das gesamte Grid, jeden Standort im Grid und jeden Knoten an einem Standort anzeigen.

In der Knotentabelle sind zusammenfassende Informationen für das gesamte Raster, jeden Standort und jeden Knoten aufgeführt. Wenn die Verbindung zu einem Knoten getrennt ist oder eine aktive Warnung vorliegt, wird neben dem Knotennamen ein Symbol angezeigt. Wenn der Knoten verbunden ist und keine aktiven Warnungen aufweist, wird kein Symbol angezeigt.

Wenn ein Knoten nicht mit dem Grid verbunden ist, beispielsweise während eines Upgrades oder in einem getrennten Zustand, sind bestimmte Metriken möglicherweise nicht verfügbar oder aus den Site- und Grid-Gesamtwerten ausgeschlossen. Nachdem ein Knoten die Verbindung zum Netz wiederhergestellt hat, warten Sie einige Minuten, bis sich die Werte stabilisiert haben.

Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Grid Manager und dann **Benutzereinstellungen**.

Bei den gezeigten Screenshots handelt es sich um Beispiele. Ihre Ergebnisse können je nach Ihrer StorageGRID -Version variieren.



Verbindungsstatussymbole

Wenn ein Knoten vom Netz getrennt wird, wird neben dem Knotennamen eines der folgenden Symbole angezeigt.

Symbol	Beschreibung	Handlungsbedarf
	**Nicht verbunden – Unbekannt** Aus einem unbekannten Grund wird die Verbindung zu einem Knoten getrennt oder die Dienste auf dem Knoten fallen unerwartet aus. Beispielsweise könnte ein Dienst auf dem Knoten gestoppt worden sein oder der Knoten könnte aufgrund eines Stromausfalls oder einer unerwarteten Störung seine Netzwerkverbindung verloren haben. Möglicherweise wird auch die Warnung **Kommunikation mit Knoten nicht möglich** ausgelöst. Möglicherweise sind auch andere Warnungen aktiv.	Erfordert sofortige Aufmerksamkeit. "Wählen Sie jede Warnung aus" und befolgen Sie die empfohlenen Maßnahmen. Beispielsweise müssen Sie möglicherweise einen angehaltenen Dienst neu starten oder den Host für den Knoten neu starten. **Hinweis**: Während verwalteter Herunterfahrvorgänge kann ein Knoten als „Unbekannt“ angezeigt werden. In diesen Fällen können Sie den Status „Unbekannt“ ignorieren.
	**Nicht verbunden – Administrator-Ausfall** Aus einem erwarteten Grund ist der Knoten nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Möglicherweise sind auch eine oder mehrere Warnungen aktiv. Je nach zugrunde liegendem Problem gehen diese Knoten häufig ohne Eingriff wieder online.	Stellen Sie fest, ob dieser Knoten von Warnungen betroffen ist. Wenn eine oder mehrere Warnungen aktiv sind,"Wählen Sie jede Warnung aus" und befolgen Sie die empfohlenen Maßnahmen.

Wenn ein Knoten vom Netz getrennt wird, liegt möglicherweise eine Warnung vor, es wird jedoch nur das Symbol „Nicht verbunden“ angezeigt. Um die aktiven Warnungen für einen Knoten anzuzeigen, wählen Sie den Knoten aus.

Warnsymbole

Wenn für einen Knoten eine aktive Warnung vorliegt, wird neben dem Knotennamen eines der folgenden Symbole angezeigt:

Kritisch: Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort angehen. Wenn das Problem nicht behoben wird, kann es zu Dienstunterbrechungen und Datenverlust kommen.

Schwerwiegend: Es liegt ein anormaler Zustand vor, der entweder den aktuellen Betrieb beeinträchtigt

oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten wichtige Warnungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder -Dienstes nicht stoppt.

⚠ **Geringfügig**: Das System funktioniert normal, es liegt jedoch ein anormaler Zustand vor, der die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn er anhält. Sie sollten kleinere Warnungen, die nicht von selbst verschwinden, überwachen und beheben, um sicherzustellen, dass sie nicht zu einem ernsteren Problem führen.

Details zu einem System, einer Site oder einem Knoten anzeigen

Um die in der Knotentabelle angezeigten Informationen zu filtern, geben Sie eine Suchzeichenfolge in das Feld **Suchen** ein. Sie können nach Systemnamen, Anzeigenamen oder Typ suchen (geben Sie beispielsweise **gat** ein, um schnell alle Gateway-Knoten zu finden).

So zeigen Sie die Informationen für das Raster, die Site oder den Knoten an:

- Wählen Sie den Rasternamen aus, um eine aggregierte Zusammenfassung der Statistiken für Ihr gesamtes StorageGRID System anzuzeigen.
- Wählen Sie einen bestimmten Rechenzentrumsstandort aus, um eine aggregierte Zusammenfassung der Statistiken für alle Knoten an diesem Standort anzuzeigen.
- Wählen Sie einen bestimmten Knoten aus, um detaillierte Informationen zu diesem Knoten anzuzeigen.

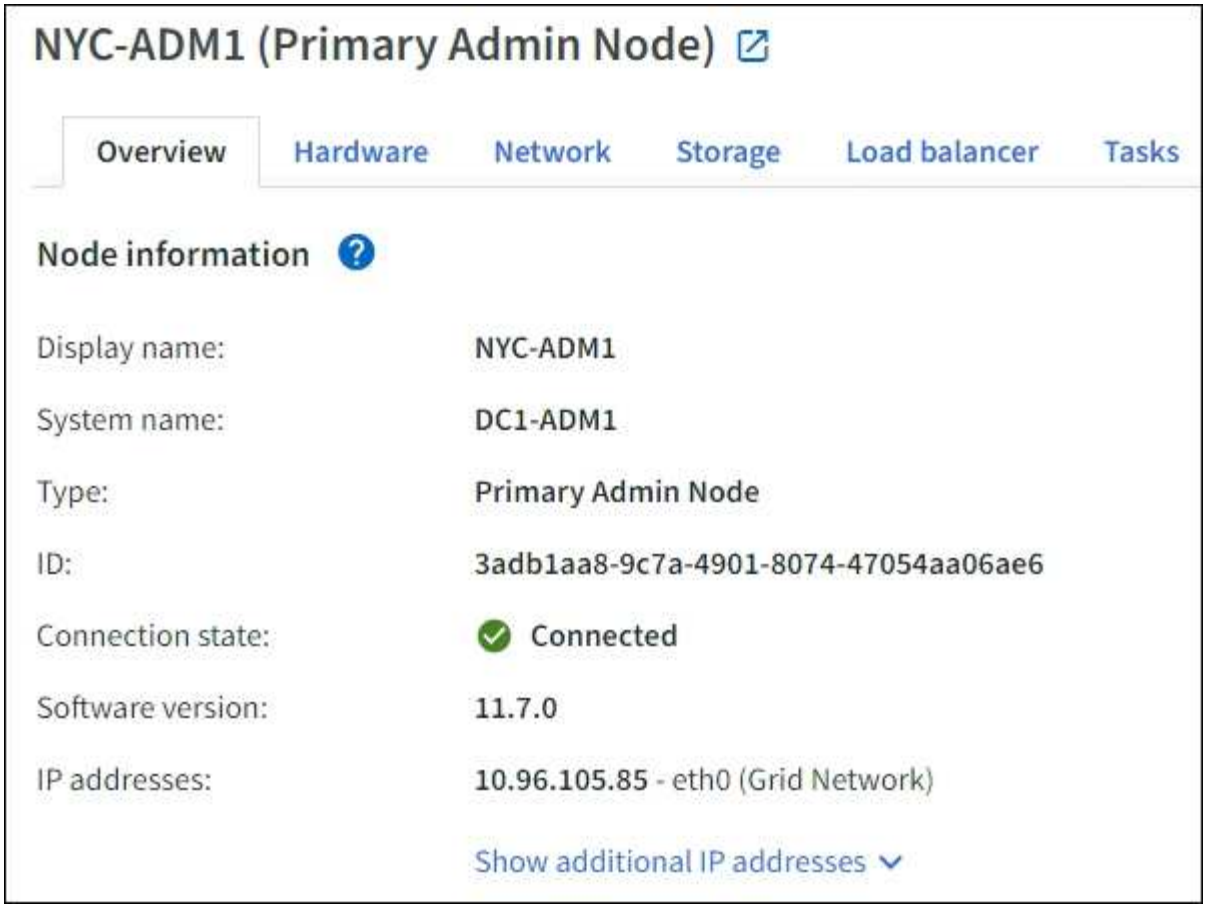
Anzeigen der Registerkarte „Übersicht“

Die Registerkarte „Übersicht“ bietet grundlegende Informationen zu jedem Knoten. Es werden auch alle Warnungen angezeigt, die derzeit den Knoten betreffen.

Die Registerkarte „Übersicht“ wird für alle Knoten angezeigt.

Knoteninformationen

Im Abschnitt „Knoteninformationen“ der Registerkarte „Übersicht“ werden grundlegende Informationen zum Knoten aufgeführt.



Die Übersichtsinformationen für einen Knoten umfassen Folgendes:

- **Anzeigename** (wird nur angezeigt, wenn der Knoten umbenannt wurde): Der aktuelle Anzeigename für den Knoten. Verwenden Sie die"Raster, Sites und Knoten umbenennen" Verfahren zum Aktualisieren dieses Werts.
- **Systemname**: Der Name, den Sie während der Installation für den Knoten eingegeben haben. Systemnamen werden für interne StorageGRID -Vorgänge verwendet und können nicht geändert werden.
- **Typ**: Der Knotentyp – Admin-Knoten, primärer Admin-Knoten, Speicherknoten oder Gateway-Knoten.
- **ID**: Die eindeutige Kennung für den Knoten, die auch als UUID bezeichnet wird.
- **Verbindungsstatus**: Einer von drei Zuständen. Das Symbol für den schwerwiegendsten Zustand wird angezeigt.
  - **Unbekannt* : Aus einem unbekannten Grund ist der Knoten nicht mit dem Netz verbunden oder ein oder mehrere Dienste sind unerwartet ausgefallen. Beispielsweise ist die Netzwerkverbindung zwischen Knoten verloren gegangen, der Strom ist ausgefallen oder ein Dienst ist ausgefallen. Möglicherweise wird auch die Warnung *Kommunikation mit Knoten nicht möglich** ausgelöst. Möglicherweise sind auch andere Warnungen aktiv. Diese Situation erfordert sofortige Aufmerksamkeit.

    Bei verwalteten Herunterfahrvorgängen kann ein Knoten als „Unbekannt“ angezeigt werden. In diesen Fällen können Sie den Status „Unbekannt“ ignorieren.

  - *Administrativ ausgefallen* : Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß

heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Möglicherweise sind auch eine oder mehrere Warnungen aktiv.

  - *Verbunden* : Der Knoten ist mit dem Netz verbunden.

- **Verwendeter Speicher**: Nur für Speicherknoten.
  - **Objektdaten**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der auf dem Speicherknoten verwendet wurde.
  - **Objektmetadaten**: Der Prozentsatz des insgesamt zulässigen Speicherplatzes für Objektmetadaten, der auf dem Speicherknoten verwendet wurde.
- **Softwareversion**: Die Version von StorageGRID , die auf dem Knoten installiert ist.
- **HA-Gruppen**: Nur für Admin-Knoten und Gateway-Knoten. Wird angezeigt, wenn eine Netzwerkschnittstelle auf dem Knoten in einer Hochverfügbarkeitsgruppe enthalten ist und ob diese Schnittstelle die primäre Schnittstelle ist.
- **IP-Adressen**: Die IP-Adressen des Knotens. Klicken Sie auf **Zusätzliche IP-Adressen anzeigen**, um die IPv4- und IPv6-Adressen und Schnittstellenzuordnungen des Knotens anzuzeigen.

Warnungen

Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle"Warnungen, die diesen Knoten derzeit betreffen und nicht stummgeschaltet wurden" . Wählen Sie den Warnungsnamen aus, um weitere Details und empfohlene Maßnahmen anzuzeigen.

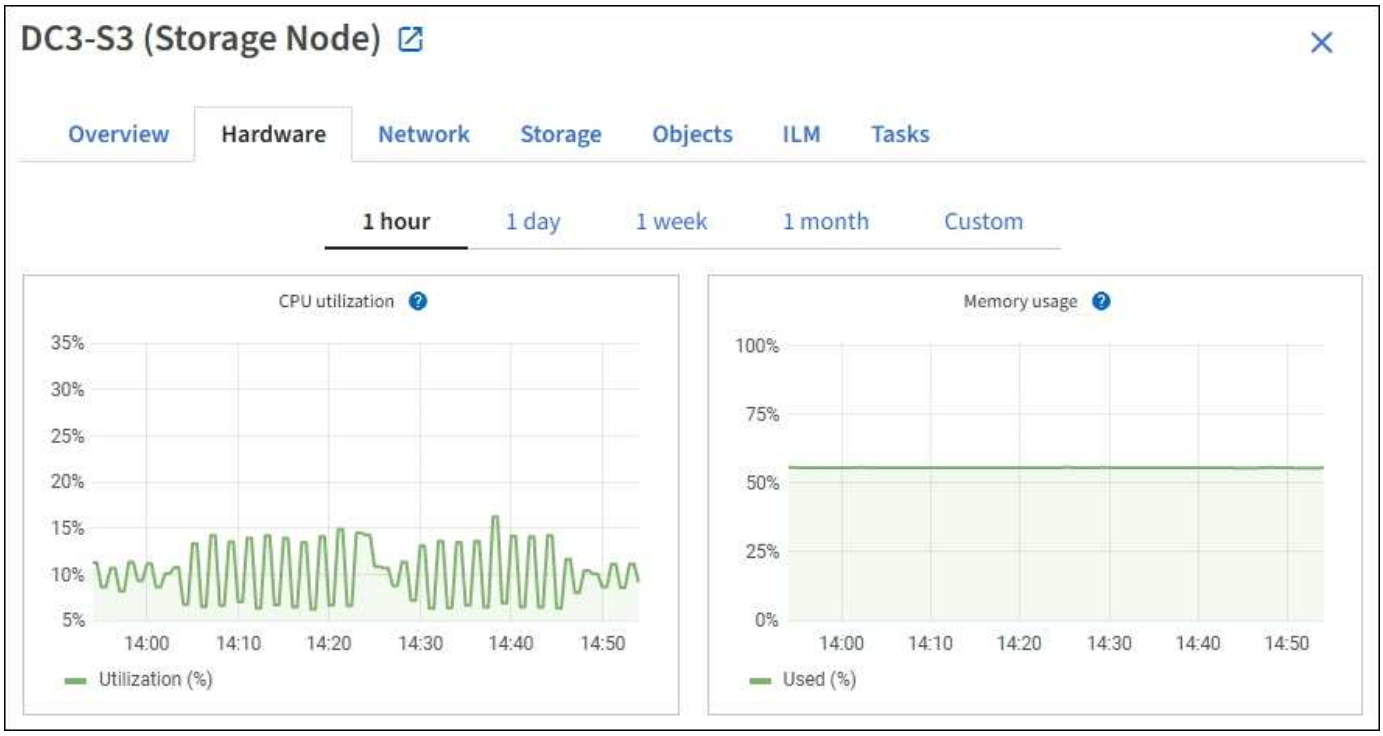
Benachrichtigungen sind auch enthalten für"Knotenverbindungszustände" .

Registerkarte „Hardware“ anzeigen

Auf der Registerkarte „Hardware“ werden die CPU-Auslastung und die Speichernutzung für jeden Knoten sowie zusätzliche Hardwareinformationen zu den Geräten angezeigt.

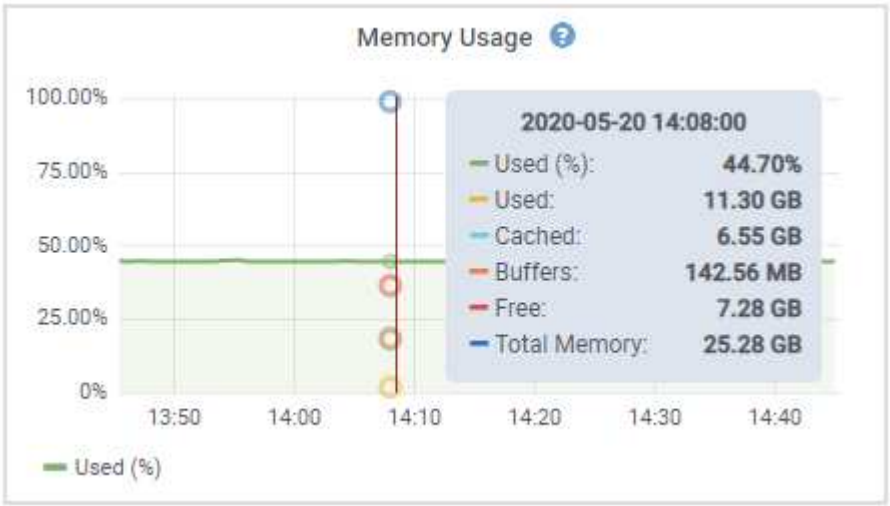
> Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispiel-Screenshots auf dieser Seite überein.

Die Registerkarte „Hardware“ wird für alle Knoten angezeigt.



Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.

Um Details zur CPU-Auslastung und Speichernutzung anzuzeigen, positionieren Sie den Cursor über jedem Diagramm.



Wenn es sich bei dem Knoten um einen Appliance-Knoten handelt, enthält diese Registerkarte auch einen Abschnitt mit weiteren Informationen zur Appliance-Hardware.

Informationen zu Appliance-Speicherknoten anzeigen

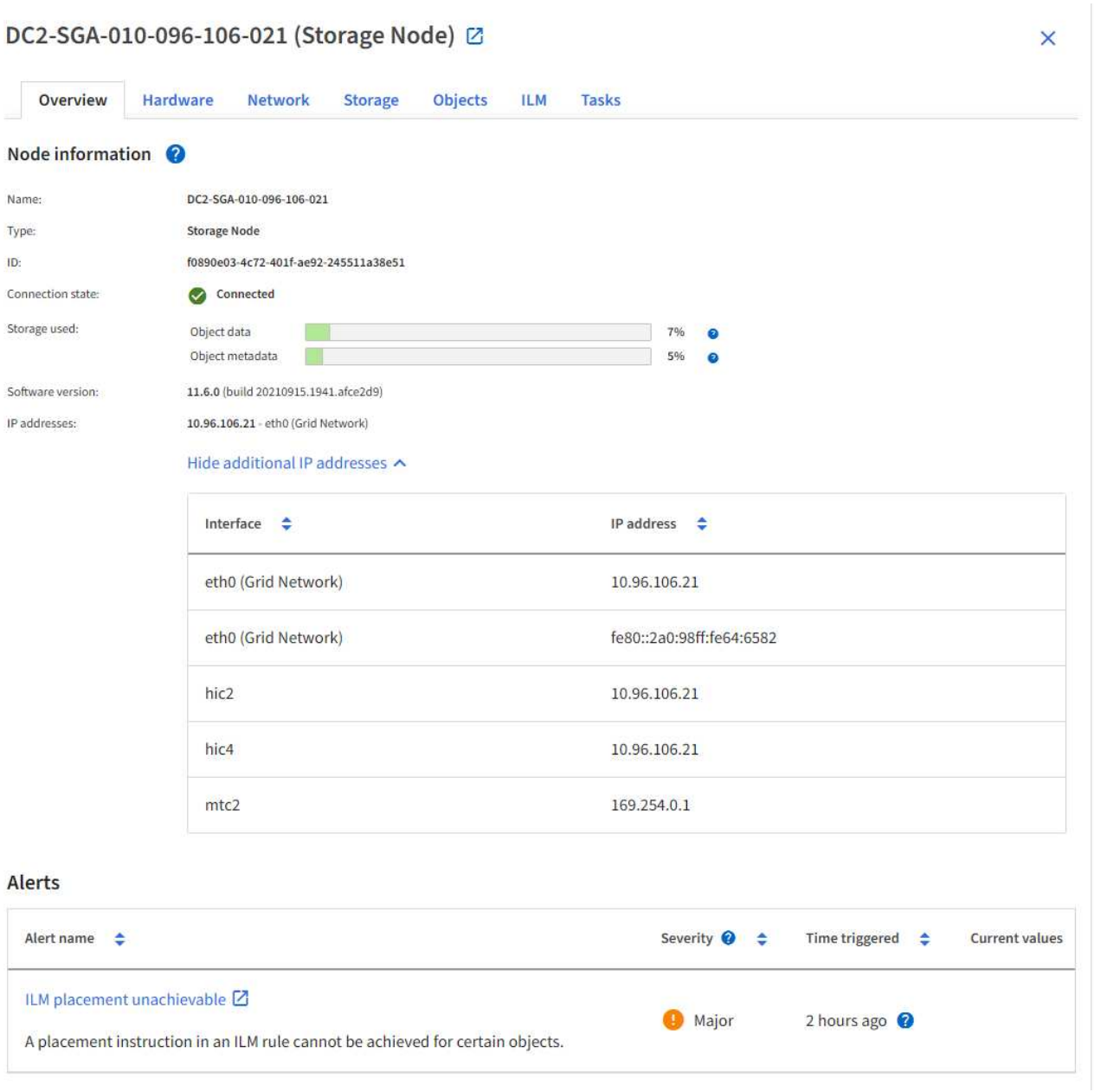
Auf der Seite „Knoten“ werden Informationen zum Dienstzustand und zu allen Rechen-, Festplatten- und Netzwerkressourcen für jeden Appliance-Speicherknoten aufgelistet. Sie können auch Speicher, Speicherhardware, Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen sowie Empfangs- und Sendedaten sehen.

Schritte

1. Wählen Sie auf der Seite „Knoten“ einen Appliance-Speicherknoten aus.
2. Wählen Sie **Übersicht**.

   Im Abschnitt „Knoteninformationen“ der Registerkarte „Übersicht“ werden zusammenfassende Informationen zum Knoten angezeigt, z. B. Name, Typ, ID und Verbindungsstatus des Knotens. Die Liste der IP-Adressen enthält den Namen der Schnittstelle für jede Adresse wie folgt:

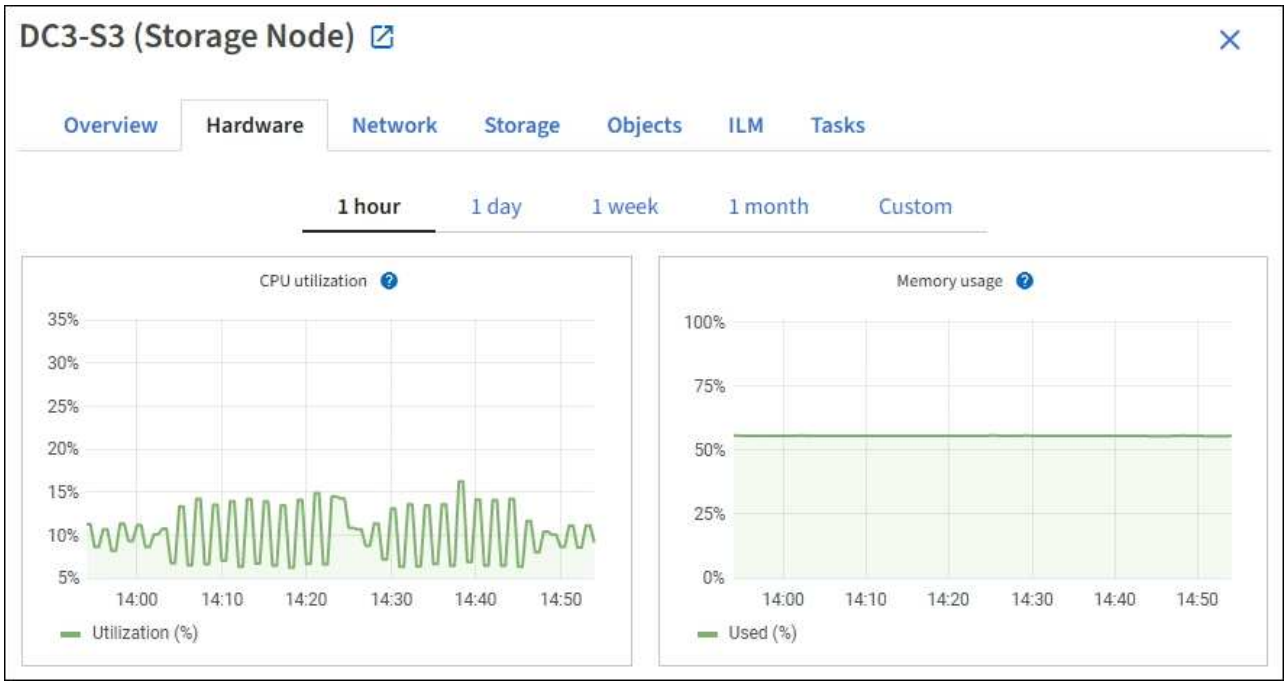
   - **eth**: Das Grid-Netzwerk, Admin-Netzwerk oder Client-Netzwerk.
   - **hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID Grid Network (eth0) und Client Network (eth2) verbunden werden.
   - **mtc**: Einer der physischen 1-GbE-Ports auf dem Gerät. Eine oder mehrere MTC-Schnittstellen werden verbunden, um die StorageGRID Admin Network-Schnittstelle (eth1) zu bilden. Sie können andere MTC-Schnittstellen für die temporäre lokale Konnektivität für einen Techniker im Rechenzentrum verfügbar lassen.



Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle aktiven Warnungen für den Knoten angezeigt.

3. Wählen Sie **Hardware** aus, um weitere Informationen zum Gerät anzuzeigen.

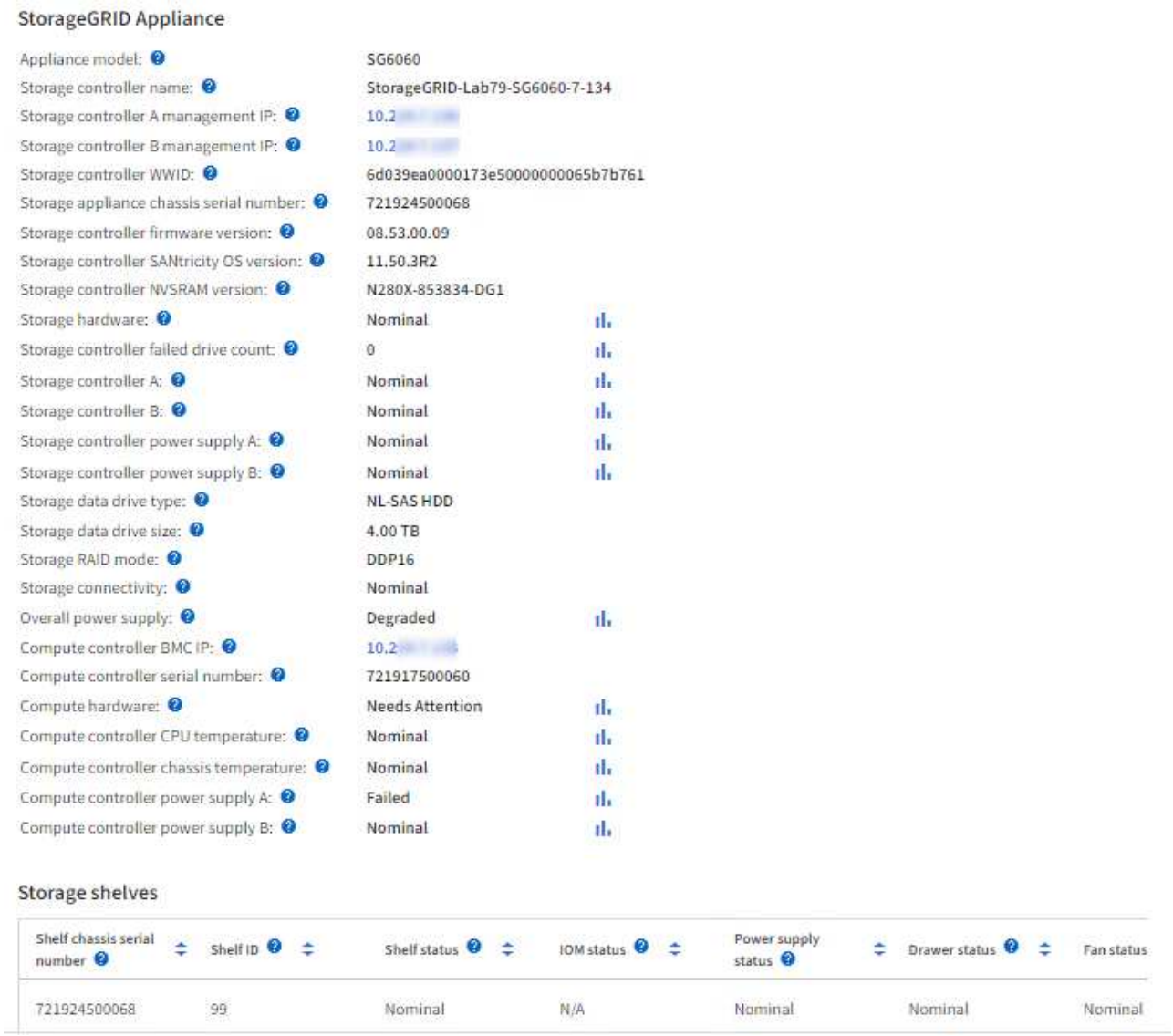
   a. Zeigen Sie die Diagramme zur CPU-Auslastung und zum Speicher an, um die Prozentsätze der CPU- und Speicherauslastung im Zeitverlauf zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.



b. Scrollen Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen wie den Modellnamen des Geräts, Controllernamen, Seriennummern und IP-Adressen sowie den Status jeder Komponente.

> Einige Felder, wie z. B. „Compute Controller BMC IP“ und „Compute Hardware“, werden nur für Geräte mit dieser Funktion angezeigt.

Komponenten für die Lagerregale und Erweiterungsregale, sofern diese Teil der Installation sind, werden in einer separaten Tabelle unterhalb der Gerätetabelle angezeigt.



Feld in der Appliance-Tabelle	Beschreibung
Gerätemodell	Die Modellnummer für dieses StorageGRID Gerät wird im SANtricity -Betriebssystem angezeigt.
Name des Speichercontrollers	Der Name für dieses StorageGRID Gerät wird im SANtricity -Betriebssystem angezeigt.
Speichercontroller A Verwaltungs-IP	IP-Adresse für Verwaltungsport 1 auf Speichercontroller A. Sie verwenden diese IP, um auf SANtricity OS zuzugreifen und Speicherprobleme zu beheben.
Verwaltungs-IP des Speichercontrollers B	IP-Adresse für Verwaltungsport 1 auf Speichercontroller B. Sie verwenden diese IP, um auf SANtricity OS zuzugreifen und Speicherprobleme zu beheben. Einige Gerätemodelle verfügen nicht über einen Speichercontroller B.

Feld in der Appliance-Tabelle	Beschreibung
WWID des Speichercontrollers	Die weltweite Kennung des Speichercontrollers, die im SANtricity -Betriebssystem angezeigt wird.
Seriennummer des Speichergerätgehäuses	Die Gehäuseseriennummer des Geräts.
Firmware-Version des Speichercontrollers	Die Version der Firmware auf dem Speichercontroller für dieses Gerät.
Speichercontroller SANtricity OS-Version	Die SANtricity OS-Version des Speichercontrollers A.
NVSRAM-Version des Speichercontrollers	NVSRAM-Version des Speichercontrollers, wie vom SANtricity System Manager gemeldet. Wenn beim SG6060 und SG6160 eine Nichtübereinstimmung der NVSRAM-Versionen zwischen den beiden Controllern vorliegt, wird die Version von Controller A angezeigt. Wenn Controller A nicht installiert oder betriebsbereit ist, wird die Version von Controller B angezeigt.
Speicherhardware	Der Gesamtstatus der Speichercontroller-Hardware. Wenn SANtricity System Manager den Status „Benötigt Aufmerksamkeit“ für die Speicherhardware meldet, meldet das StorageGRID -System ebenfalls diesen Wert. Wenn der Status „Benötigt Aufmerksamkeit“ lautet, überprüfen Sie zuerst den Speichercontroller mit SANtricity OS. Stellen Sie dann sicher, dass keine anderen Warnungen vorhanden sind, die für den Compute Controller gelten.
Anzahl der Laufwerksfehler des Speichercontrollers	Die Anzahl der Laufwerke, die nicht optimal sind.
Speichercontroller A	Der Status des Speichercontrollers A.
Speichercontroller B	Der Status des Speichercontrollers B. Einige Appliance-Modelle verfügen nicht über einen Speichercontroller B.
Speichercontroller-Netzteil A	Der Status des Netzteils A für den Speichercontroller.
Speichercontroller-Netzteil B	Der Status der Stromversorgung B für den Speichercontroller.
Speicherdatenlaufwerkstyp	Der Laufwerkstyp im Gerät, z. B. HDD (Festplatte) oder SSD (Solid-State-Laufwerk).

Feld in der Appliance-Tabelle	Beschreibung
Größe des Speicherdatenlaufwerks	Die effektive Größe eines Datenlaufwerks. Beim SG6160 wird auch die Größe des Cache-Laufwerks angezeigt. **Hinweis**: Für Knoten mit Erweiterungs-Shelfs verwenden Sie dieDatenlaufwerksgröße für jedes Regal stattdessen. Die effektive Laufwerksgröße kann je nach Regal unterschiedlich sein.
Speicher-RAID-Modus	Der für das Gerät konfigurierte RAID-Modus.
Speicherkonnektivität	Der Speicherkonnektivitätsstatus.
Gesamtstromversorgung	Der Status aller Stromversorgungen für das Gerät.
BMC -IP des Rechencontrollers	Die IP-Adresse des Baseboard Management Controller (BMC)-Ports im Compute Controller. Sie verwenden diese IP, um eine Verbindung zur BMC Schnittstelle herzustellen und die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird für Appliance-Modelle ohne BMC nicht angezeigt.
Seriennummer des Compute-Controllers	Die Seriennummer des Compute-Controllers.
Computerhardware	Der Status der Compute-Controller-Hardware. Dieses Feld wird für Appliance-Modelle ohne separate Rechen- und Speicherhardware nicht angezeigt.
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute Controllers.
Gehäusetemperatur des Compute-Controllers	Der Temperaturstatus des Compute-Controllers.

+

Spalte in der Tabelle „Lagerregale“	Beschreibung
Seriennummer des Regalgehäuses	Die Seriennummer für das Lagerregalgehäuse.

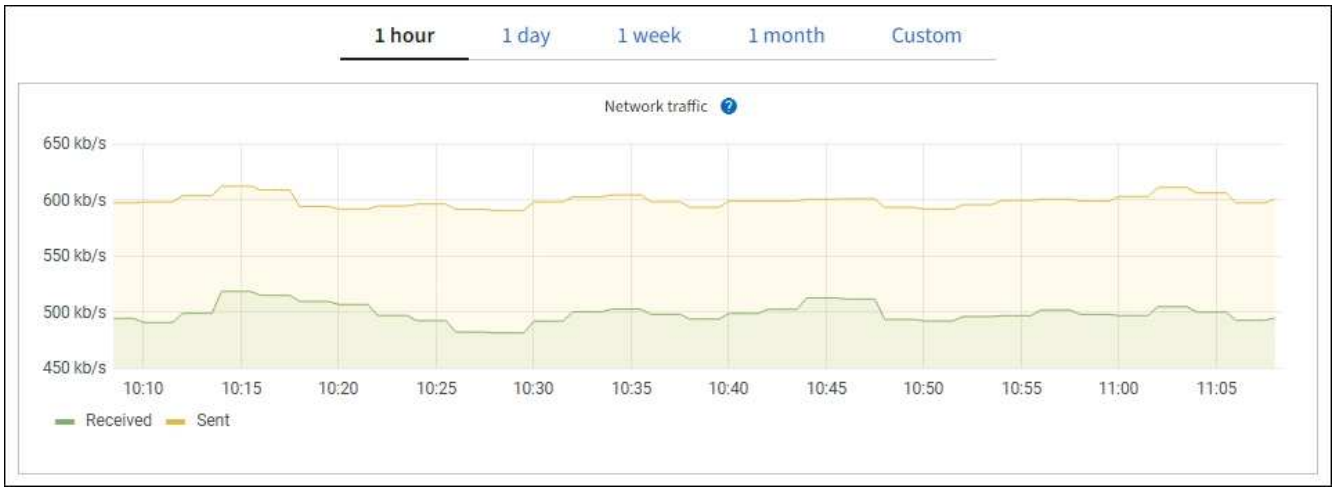
Spalte in der Tabelle „Lagerregale“	Beschreibung
Regal-ID	Die numerische Kennung für das Lagerregal. • 99: Speichercontroller-Regal • 0: Erstes Erweiterungsregal • 1: Zweites Erweiterungsregal **Hinweis:** Erweiterungsregale gelten nur für SG6060 und SG6160.
Regalstatus	Der Gesamtstatus des Lagerregals.
IOM-Status	Der Status der Eingabe-/Ausgabemodule (IOMs) in allen Erweiterungsregalen. N/A, wenn es sich nicht um ein Erweiterungsregal handelt.
Stromversorgungsstatus	Der Gesamtstatus der Stromversorgungen für das Speicherregal.
Schubladenstatus	Der Status der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Kühllüfter im Lagerregal.
Laufwerkssteckplätze	Die Gesamtzahl der Laufwerkssteckplätze im Speicherregal.
Datenlaufwerke	Die Anzahl der Laufwerke im Speicherregal, die zur Datenspeicherung verwendet werden.
Größe des Datenlaufwerks	Die effektive Größe eines Datenlaufwerks im Speicherregal.
Cache-Laufwerke	Die Anzahl der Laufwerke im Speicherregal, die als Cache verwendet werden.
Cache-Laufwerksgröße	Die Größe des kleinsten Cache-Laufwerks im Speicherregal. Normalerweise haben alle Cache-Laufwerke die gleiche Größe.
Konfigurationsstatus	Der Konfigurationsstatus des Speicherregals.

a. Bestätigen Sie, dass alle Status „Nominal“ sind.

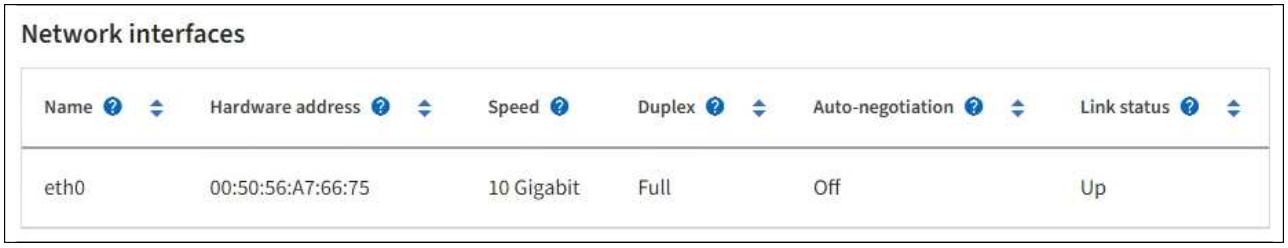
   Wenn ein Status nicht „Nominal“ ist, überprüfen Sie alle aktuellen Warnungen. Sie können auch SANtricity System Manager verwenden, um mehr über einige dieser Hardwarewerte zu erfahren. Lesen Sie die Anweisungen zur Installation und Wartung Ihres Geräts.

4. Wählen Sie **Netzwerk**, um Informationen zu jedem Netzwerk anzuzeigen.

   Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs.



a. Lesen Sie den Abschnitt „Netzwerkschnittstellen“.



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle „Netzwerkschnittstellen“, um zu bestimmen, ob die 10/25-GbE-Netzwerkports auf der Appliance für die Verwendung des Aktiv-/Sicherungsmodus oder des LACP-Modus konfiguriert wurden.

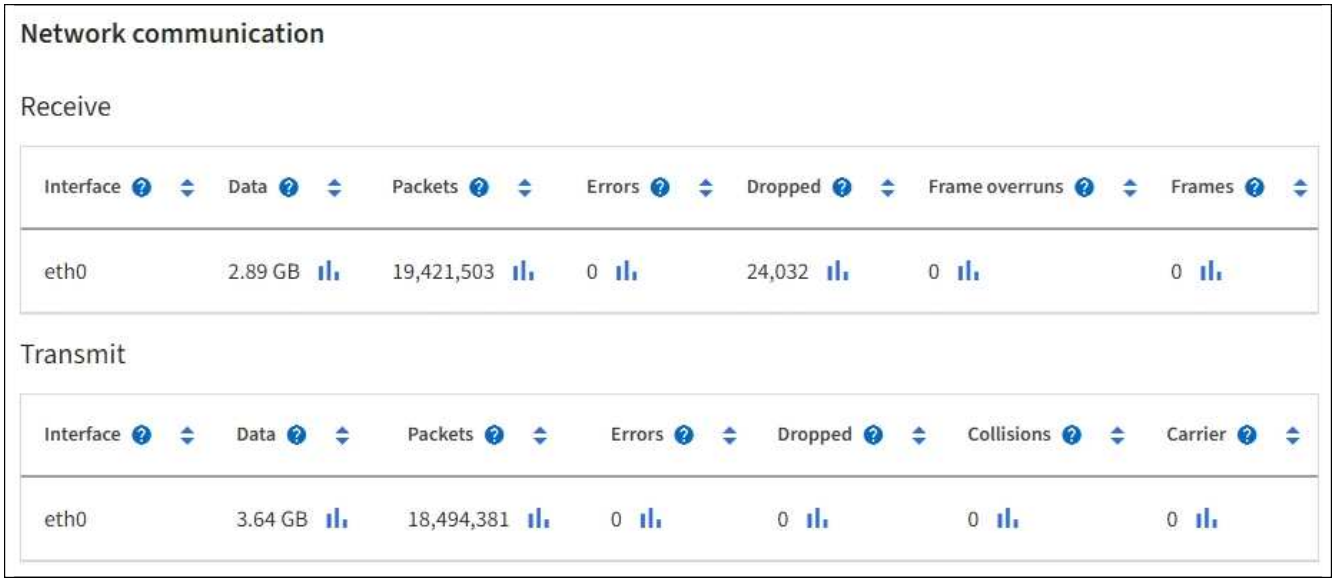
Bei den in der Tabelle angezeigten Werten wird davon ausgegangen, dass alle vier Links verwendet werden.

Link-Modus	Bond-Modus	Individuelle HIC-Verbindungsgeschwindigkeit (hic1, hic2, hic3, hic4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0,eth2)
Aggregat	LACP	25	100
Behoben	LACP	25	50
Behoben	Aktiv/Backup	25	25
Aggregat	LACP	10	40
Behoben	LACP	10	20
Behoben	Aktiv/Backup	10	10

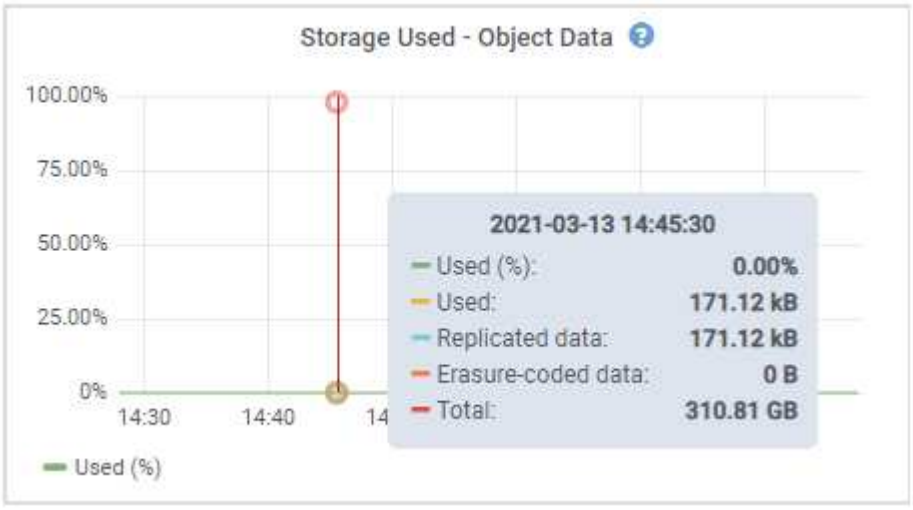
Sehen "Konfigurieren von Netzwerkverbindungen" Weitere Informationen zum Konfigurieren der 10/25-GbE-Ports.

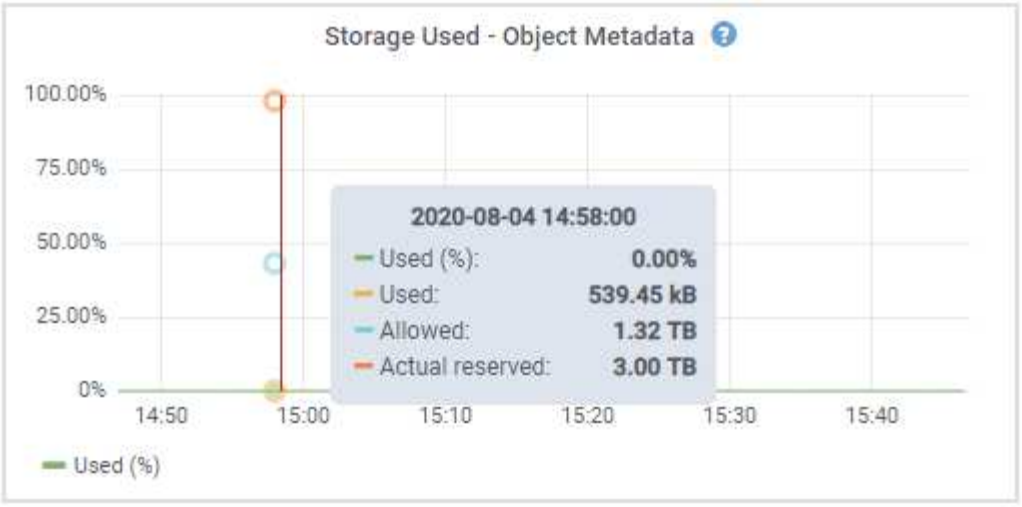
b. Lesen Sie den Abschnitt „Netzwerkkommunikation“.

   Die Empfangs- und Sendetabellen zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie weitere Empfangs- und Sendemetriken.



5. Wählen Sie **Speicher** aus, um Diagramme anzuzeigen, die den Prozentsatz des im Zeitverlauf für Objektdaten und Objektmetadaten verwendeten Speichers sowie Informationen zu Festplattengeräten, Volumes und Objektspeichern zeigen.

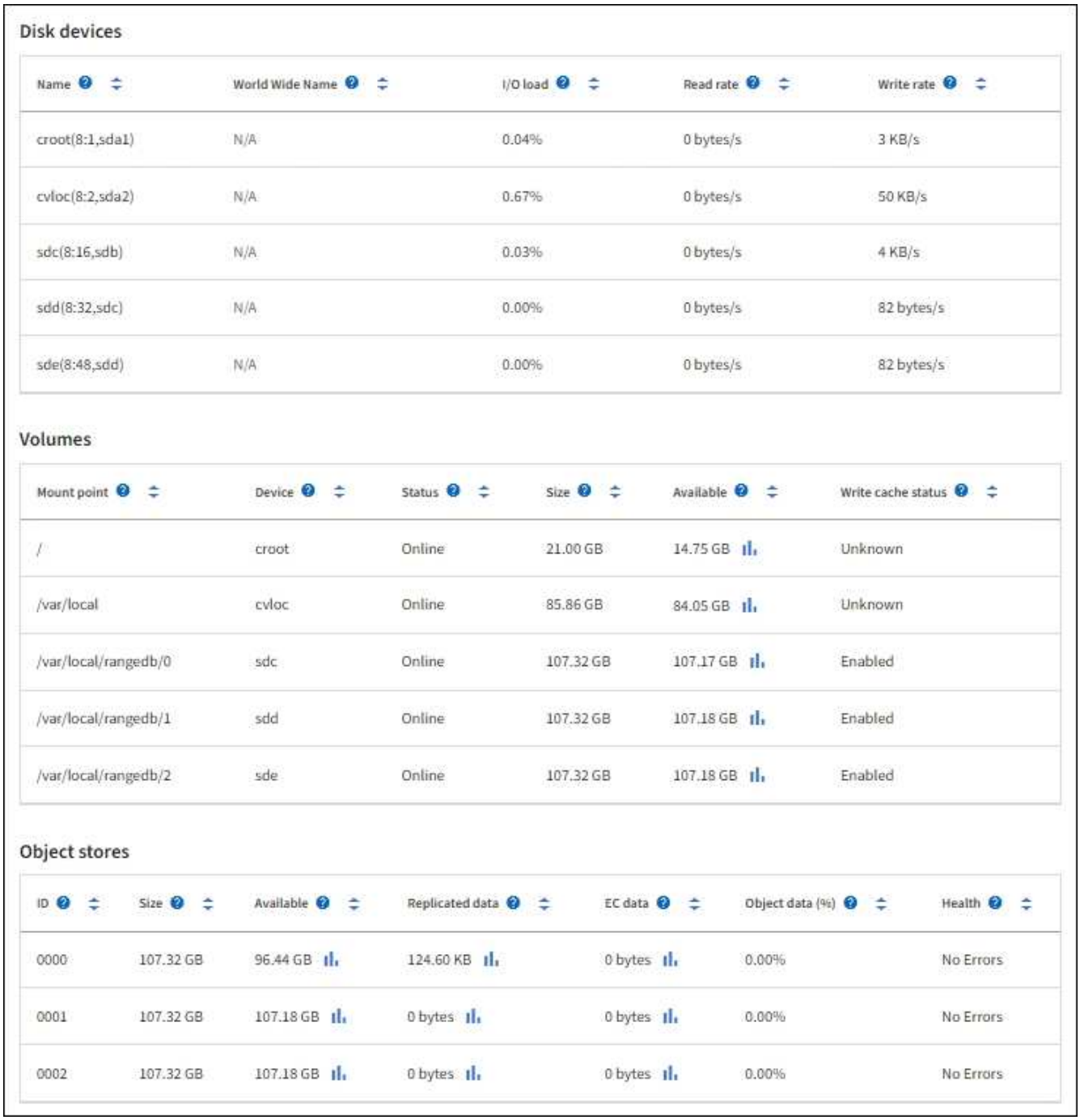




a. Scrollen Sie nach unten, um die Menge des verfügbaren Speichers für jedes Volume und jeden Objektspeicher anzuzeigen.

   Der weltweite Name für jede Festplatte entspricht der weltweiten Volume-Kennung (WWID), die angezeigt wird, wenn Sie die Standard-Volume-Eigenschaften in SANtricity OS anzeigen (der Verwaltungssoftware, die mit dem Speichercontroller des Geräts verbunden ist).

   Um Ihnen die Interpretation der Lese- und Schreibstatistiken für die Datenträger in Bezug auf Volume-Mount-Punkte zu erleichtern, entspricht der erste Teil des in der Spalte **Name** der Tabelle „Datenträgergeräte“ angezeigten Namens (also *sdc*, *sdd*, *sde* usw.) dem in der Spalte **Gerät** der Tabelle „Volumes“ angezeigten Wert.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Informationen zu Appliance-Admin-Knoten und Gateway-Knoten anzeigen

Auf der Seite „Knoten“ werden Informationen zum Dienstzustand und zu allen Rechen-, Festplatten- und Netzwerkressourcen für jede Dienst-Appliance aufgelistet, die als Admin-Knoten oder Gateway-Knoten verwendet wird. Sie können auch Speicher, Speicherhardware, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen sowie Empfangs- und Sendedaten sehen.

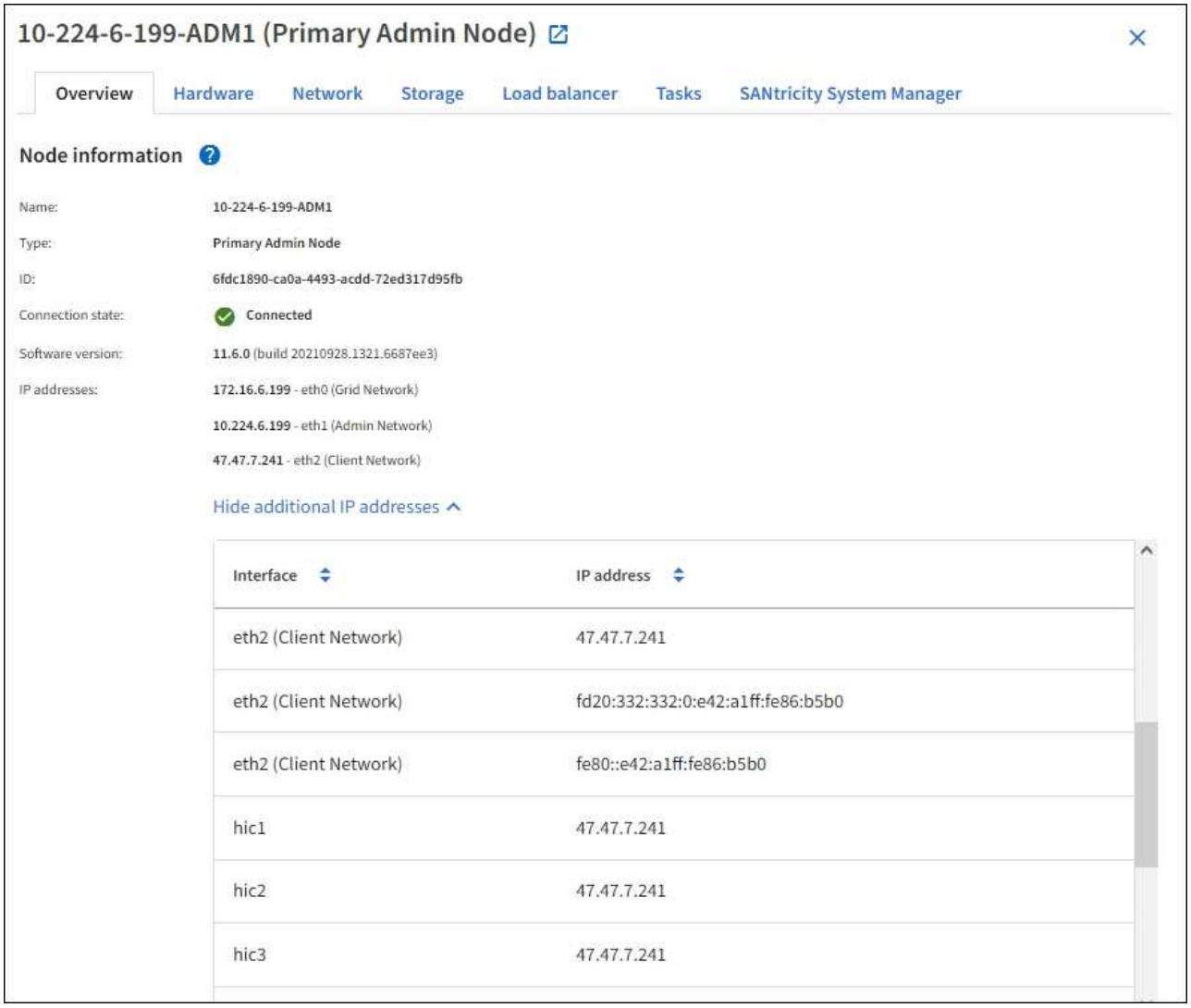
Schritte

1. Wählen Sie auf der Seite „Knoten“ einen Appliance-Admin-Knoten oder einen Appliance-Gateway-Knoten aus.
2. Wählen Sie **Übersicht**.

   Im Abschnitt „Knoteninformationen“ der Registerkarte „Übersicht“ werden zusammenfassende

Informationen zum Knoten angezeigt, z. B. Name, Typ, ID und Verbindungsstatus des Knotens. Die Liste der IP-Adressen enthält den Namen der Schnittstelle für jede Adresse wie folgt:

- **adllb** und **adlli**: Wird angezeigt, wenn Active/Backup-Bonding für die Admin-Netzwerkschnittstelle verwendet wird
- **eth**: Das Grid-Netzwerk, Admin-Netzwerk oder Client-Netzwerk.
- **hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID Grid Network (eth0) und Client Network (eth2) verbunden werden.
- **mtc**: Einer der physischen 1-GbE-Ports auf dem Gerät. Eine oder mehrere MTC-Schnittstellen werden zur Admin-Netzwerkschnittstelle (eth1) verbunden. Sie können andere MTC-Schnittstellen für die temporäre lokale Konnektivität für einen Techniker im Rechenzentrum verfügbar lassen.

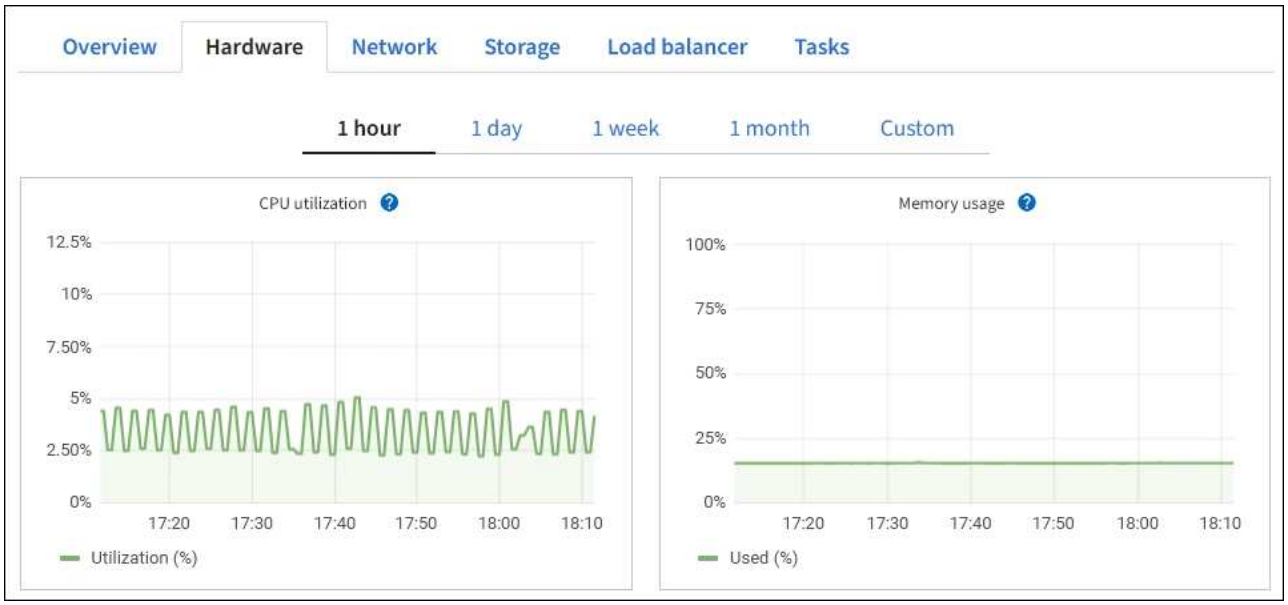


Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle aktiven Warnungen für den Knoten angezeigt.

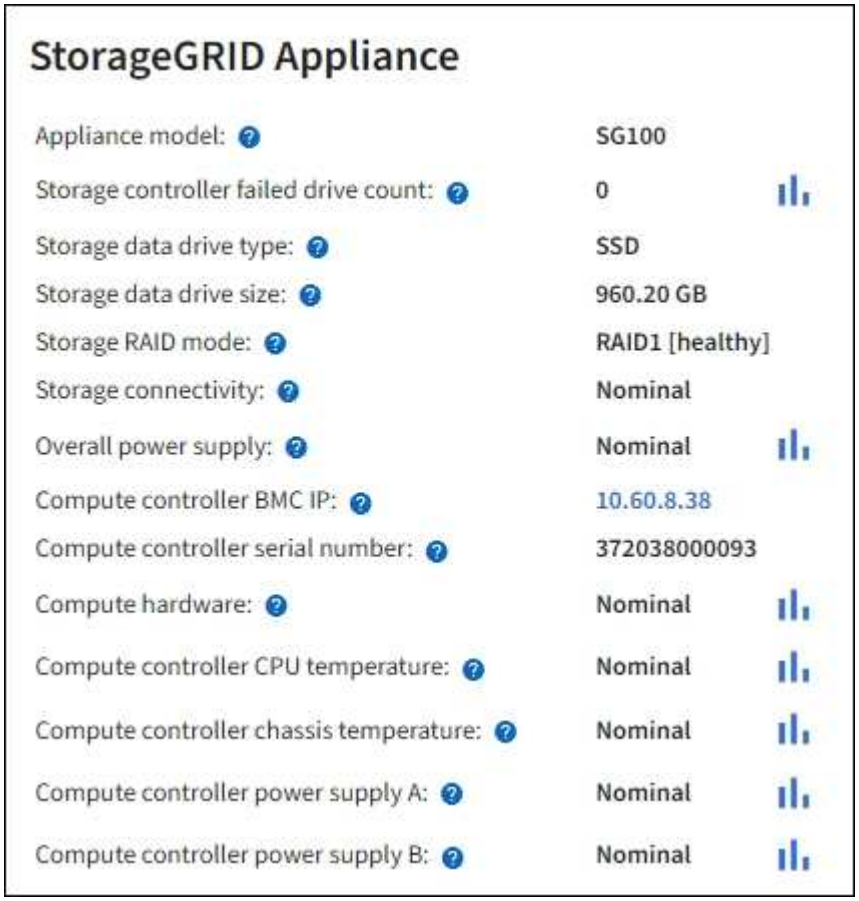
3. Wählen Sie **Hardware** aus, um weitere Informationen zum Gerät anzuzeigen.

   a. Zeigen Sie die Diagramme zur CPU-Auslastung und zum Speicher an, um die Prozentsätze der CPU- und Speicherauslastung im Zeitverlauf zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren

Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.



b. Scrollen Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen wie den Modellnamen, die Seriennummer, die Firmware-Version des Controllers und den Status jeder Komponente.



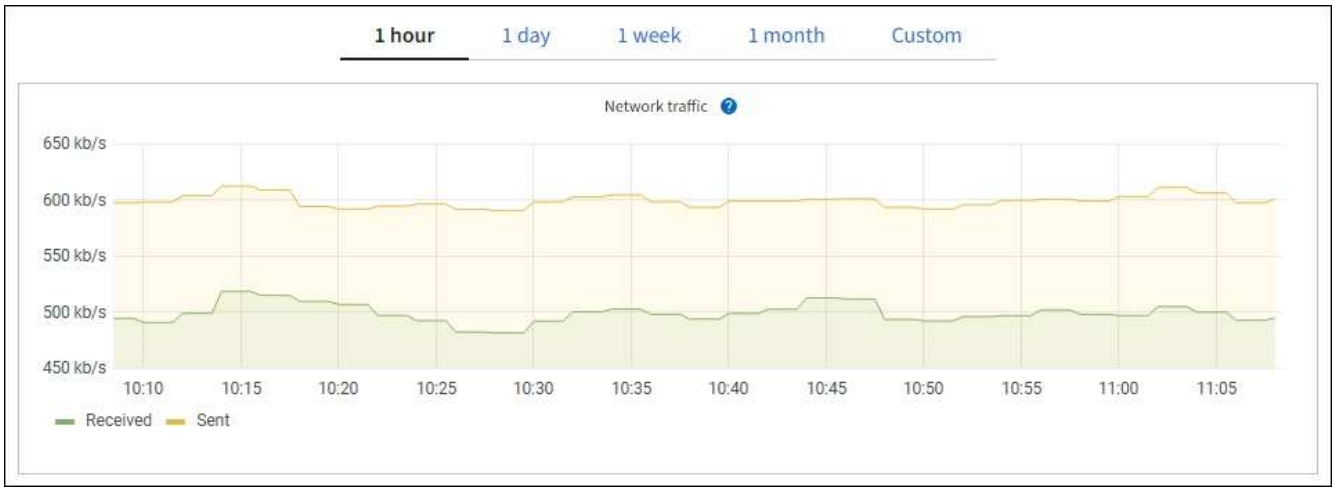
Feld in der Appliance-Tabelle	Beschreibung
Gerätemodell	Die Modellnummer für dieses StorageGRID Gerät.
Anzahl der Laufwerksfehler des Speichercontrollers	Die Anzahl der Laufwerke, die nicht optimal sind.
Speicherdatenlaufwerkstyp	Der Laufwerkstyp im Gerät, z. B. HDD (Festplatte) oder SSD (Solid-State-Laufwerk).
Größe des Speicherdatenlaufwerks	Die effektive Größe eines Datenlaufwerks.
Speicher-RAID-Modus	Der RAID-Modus für das Gerät.
Gesamtstromversorgung	Der Status aller Netzteile im Gerät.
BMC -IP des Rechencontrollers	Die IP-Adresse des Baseboard Management Controller (BMC)-Ports im Compute Controller. Sie können diese IP verwenden, um eine Verbindung zur BMC Schnittstelle herzustellen und die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird für Appliance-Modelle ohne BMC nicht angezeigt.
Seriennummer des Compute-Controllers	Die Seriennummer des Compute-Controllers.
Computerhardware	Der Status der Compute-Controller-Hardware.
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute Controllers.
Gehäusetemperatur des Compute-Controllers	Der Temperaturstatus des Compute-Controllers.

a. Bestätigen Sie, dass alle Status „Nominal“ sind.

   Wenn ein Status nicht „Nominal“ ist, überprüfen Sie alle aktuellen Warnungen.

4. Wählen Sie **Netzwerk**, um Informationen zu jedem Netzwerk anzuzeigen.

   Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs.



a. Lesen Sie den Abschnitt „Netzwerkschnittstellen“.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

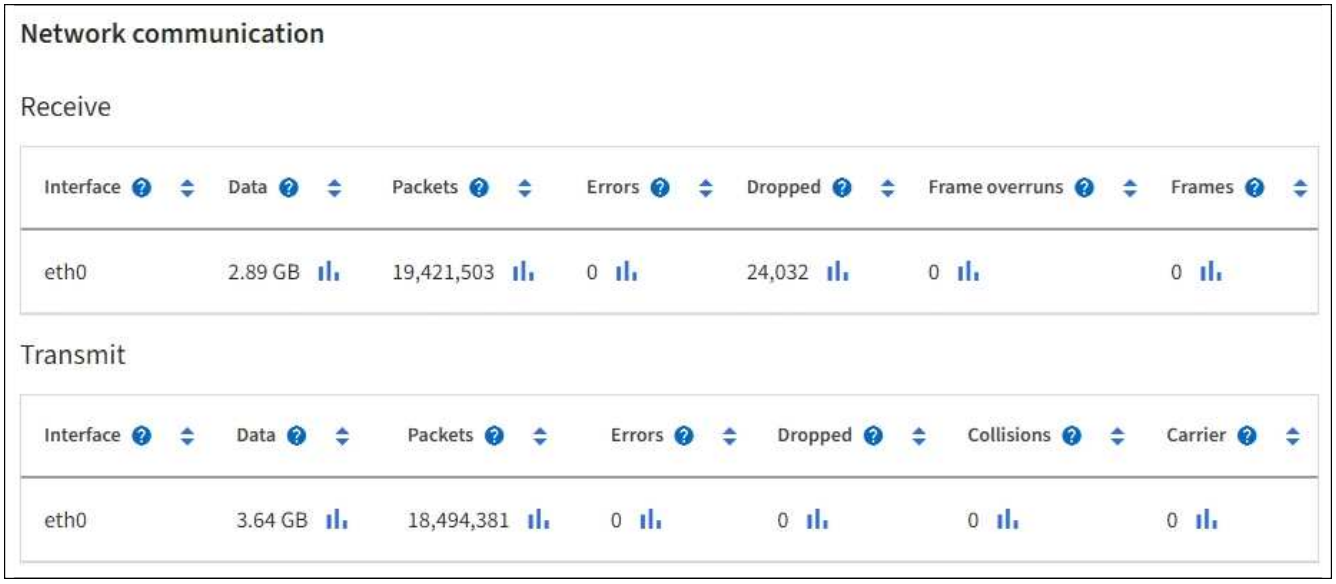
Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle „Netzwerkschnittstellen“, um zu bestimmen, ob die vier 40/100-GbE-Netzwerkports auf der Appliance für die Verwendung des Aktiv-/Sicherungsmodus oder des LACP-Modus konfiguriert wurden.

Bei den in der Tabelle angezeigten Werten wird davon ausgegangen, dass alle vier Links verwendet werden.

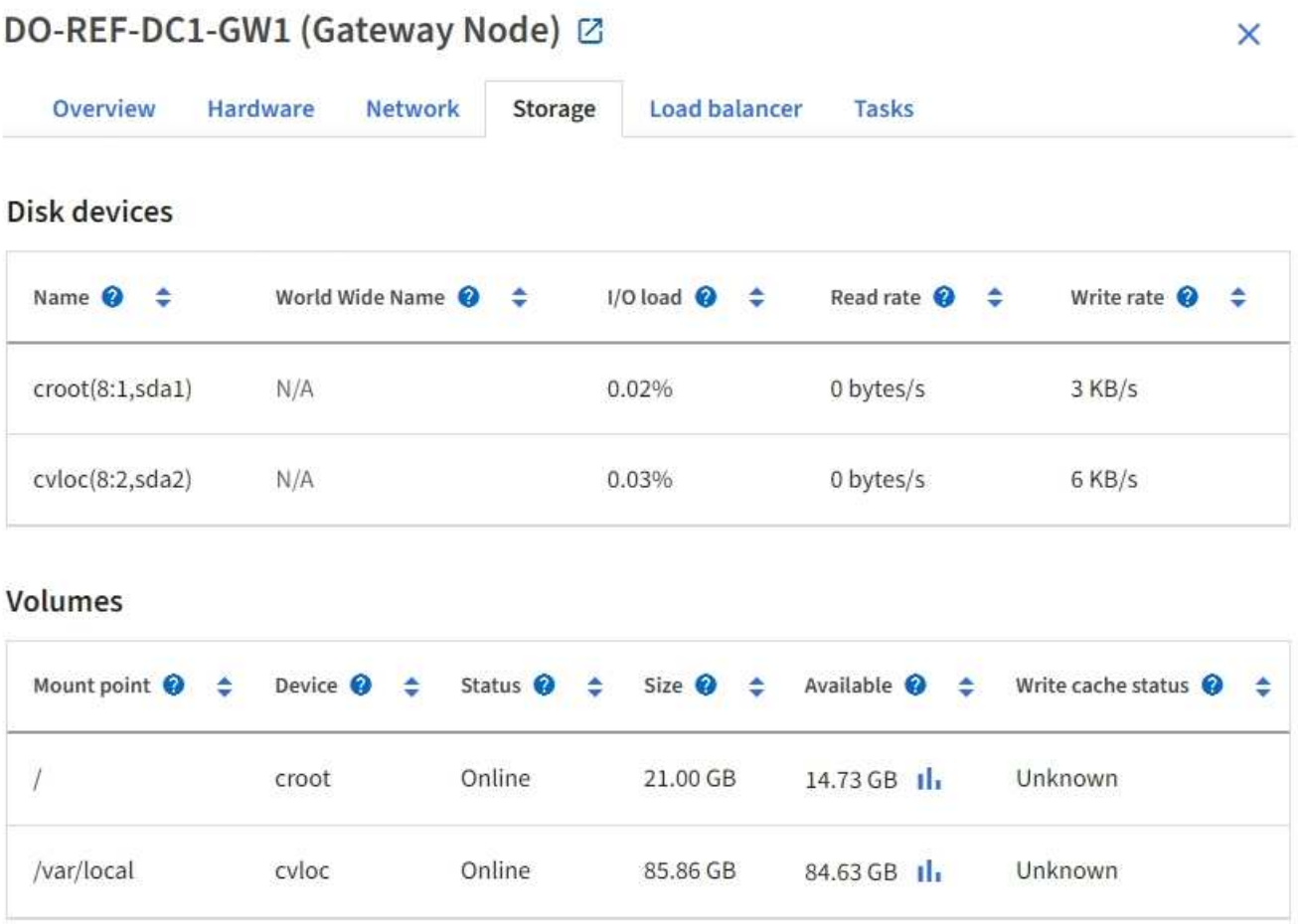
Link-Modus	Bond-Modus	Individuelle HIC-Verbindungsgeschwindigkeit (hic1, hic2, hic3, hic4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0, eth2)
Aggregat	LACP	100	400
Behoben	LACP	100	200
Behoben	Aktiv/Backup	100	100
Aggregat	LACP	40	160
Behoben	LACP	40	80
Behoben	Aktiv/Backup	40	40

b. Lesen Sie den Abschnitt „Netzwerkkommunikation“.

Die Empfangs- und Sendetabellen zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Sendemetriken.



5. Wählen Sie **Speicher** aus, um Informationen zu den Festplattengeräten und Volumes auf der Service-Appliance anzuzeigen.



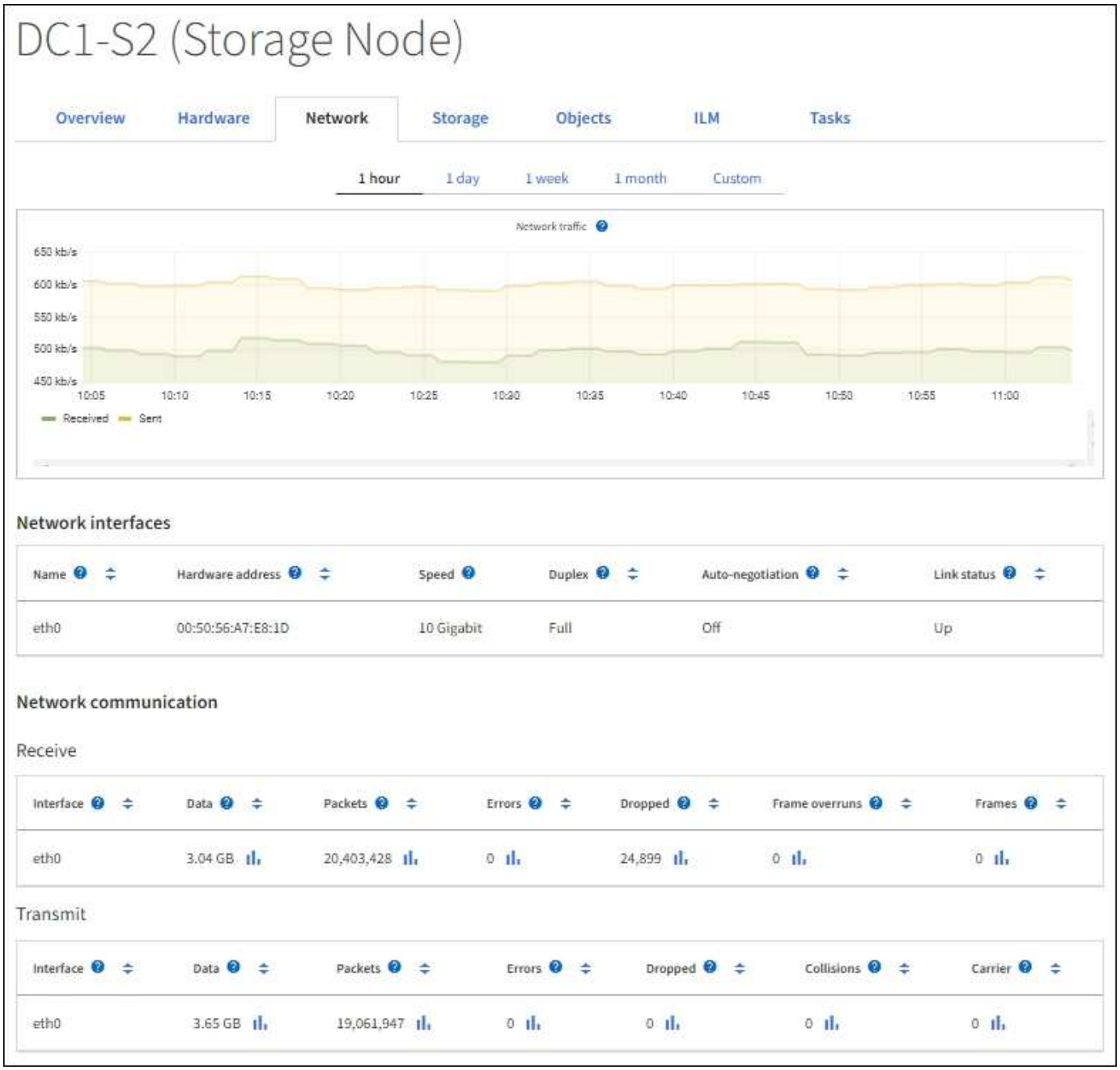
Anzeigen der Registerkarte „Netzwerk“

Auf der Registerkarte „Netzwerk“ wird ein Diagramm angezeigt, das den über alle Netzwerkschnittstellen auf dem Knoten, der Site oder dem Grid empfangenen und gesendeten Netzwerkverkehr darstellt.

Die Registerkarte „Netzwerk“ wird für alle Knoten, jeden Standort und das gesamte Raster angezeigt.

Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.

Für Knoten enthält die Tabelle „Netzwerkschnittstellen“ Informationen zu den physischen Netzwerkports jedes Knotens. Die Netzwerkkommunikationstabelle enthält Einzelheiten zu den Empfangs- und Sendevorgängen jedes Knotens und zu allen vom Treiber gemeldeten Fehlerzählern.



Ähnliche Informationen

"Überwachen Sie Netzwerkverbindungen und Leistung"

Registerkarte „Speicher“ anzeigen

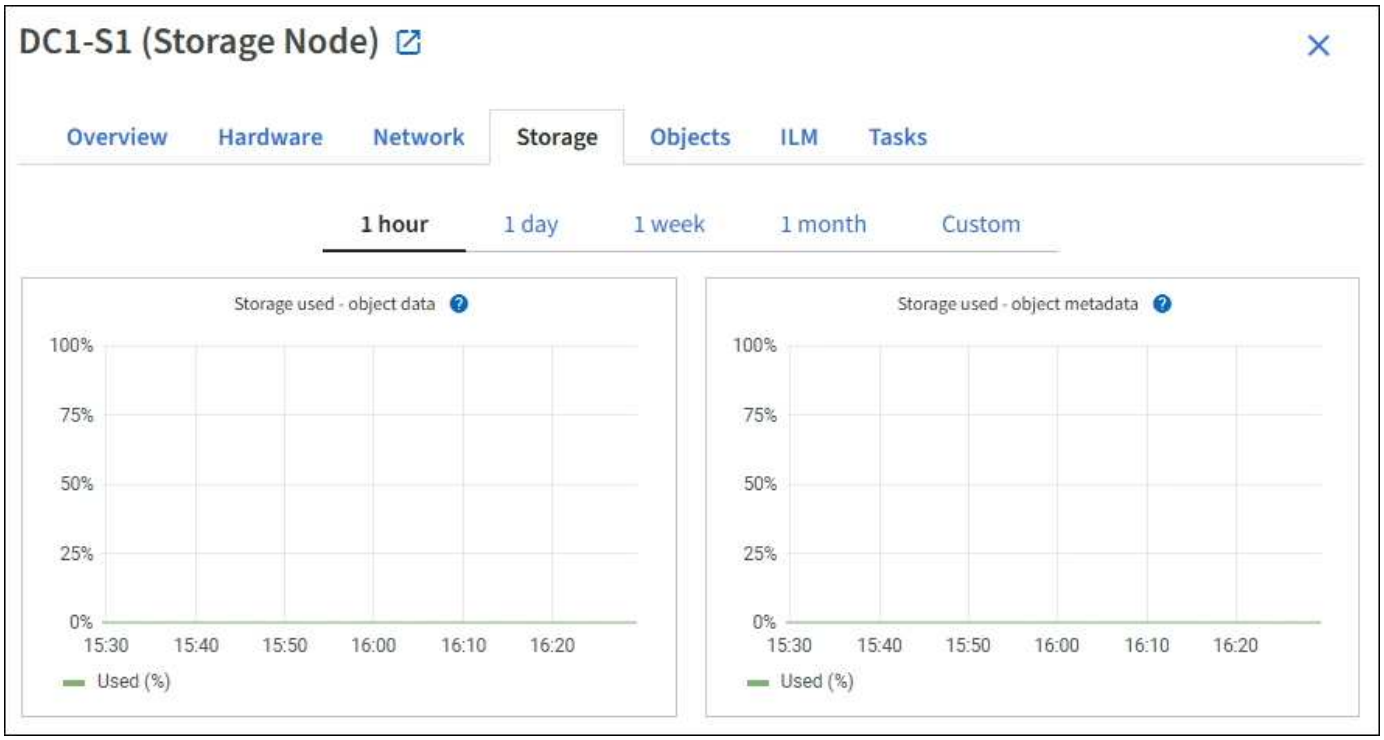
Auf der Registerkarte „Speicher“ werden die Speicherverfügbarkeit und andere Speichermetriken zusammengefasst.

Die Registerkarte „Speicher“ wird für alle Knoten, jeden Standort und das gesamte Raster angezeigt.

Diagramme zum verwendeten Speicher

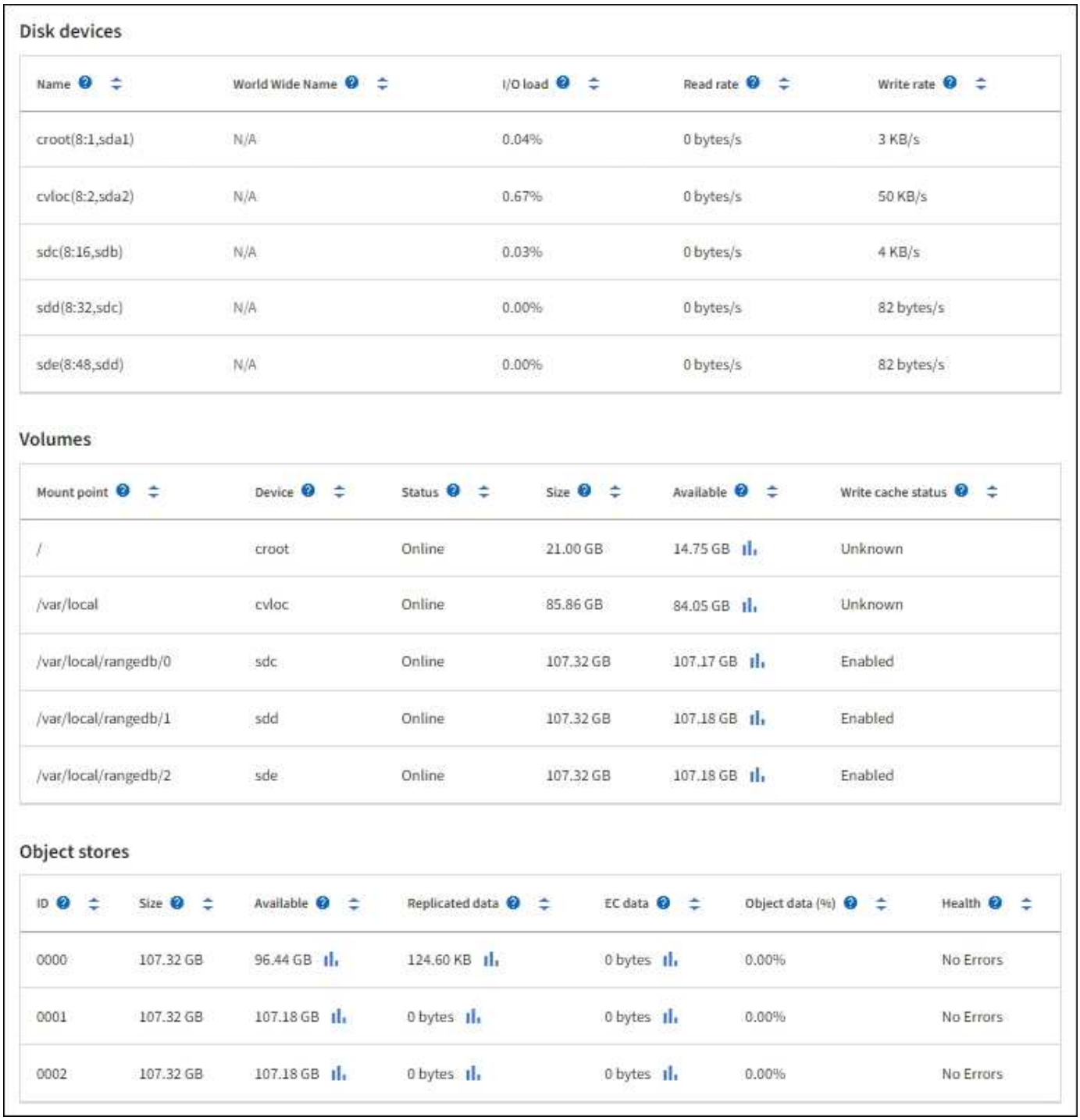
Für Speicherknoten, jeden Standort und das gesamte Raster enthält die Registerkarte „Speicher“ Diagramme, die zeigen, wie viel Speicher im Laufe der Zeit von Objektdaten und Objektmetadaten verwendet wurde.

Wenn ein Knoten nicht mit dem Grid verbunden ist, beispielsweise während eines Upgrades oder in einem getrennten Zustand, sind bestimmte Metriken möglicherweise nicht verfügbar oder aus den Site- und Grid-Gesamtwerten ausgeschlossen. Nachdem ein Knoten die Verbindung zum Netz wiederhergestellt hat, warten Sie einige Minuten, bis sich die Werte stabilisiert haben.



Tabellen für Festplattengeräte, Volumes und Objektspeicher

Für alle Knoten enthält die Registerkarte „Speicher“ Details zu den Festplattengeräten und Volumes auf dem Knoten. Für Speicherknoten enthält die Objektspeichertabelle Informationen zu jedem Speichervolumen.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

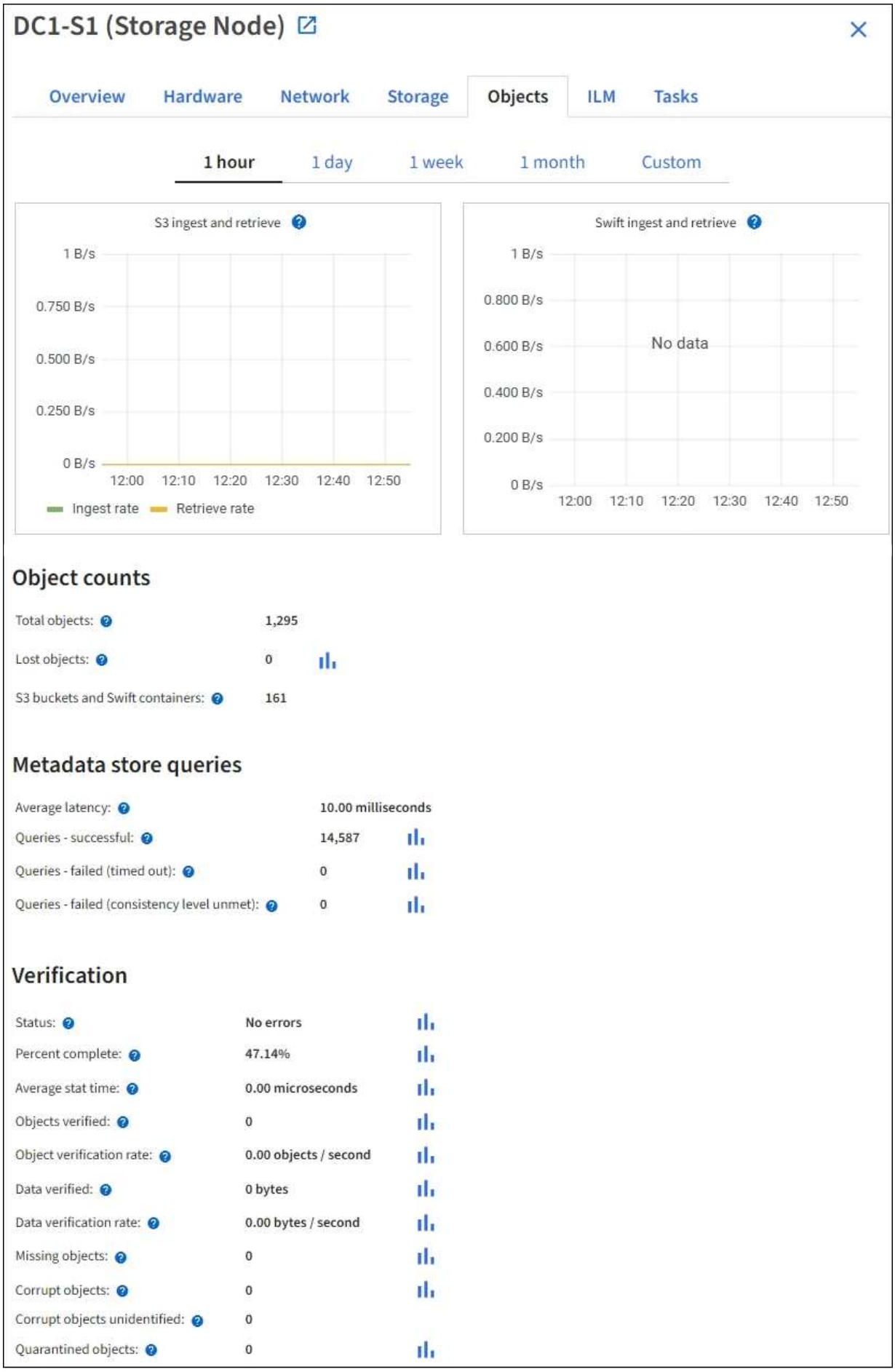
Ähnliche Informationen

"Überwachen der Speicherkapazität"

Anzeigen der Registerkarte „Objekte“

Die Registerkarte Objekte bietet Informationen über"S3-Aufnahme- und Abrufraten" .

Die Registerkarte „Objekte“ wird für jeden Speicherknoten, jede Site und das gesamte Raster angezeigt. Für Speicherknoten bietet die Registerkarte „Objekte“ auch Objektanzahlen und Informationen zu Metadatenabfragen und Hintergrundüberprüfungen.

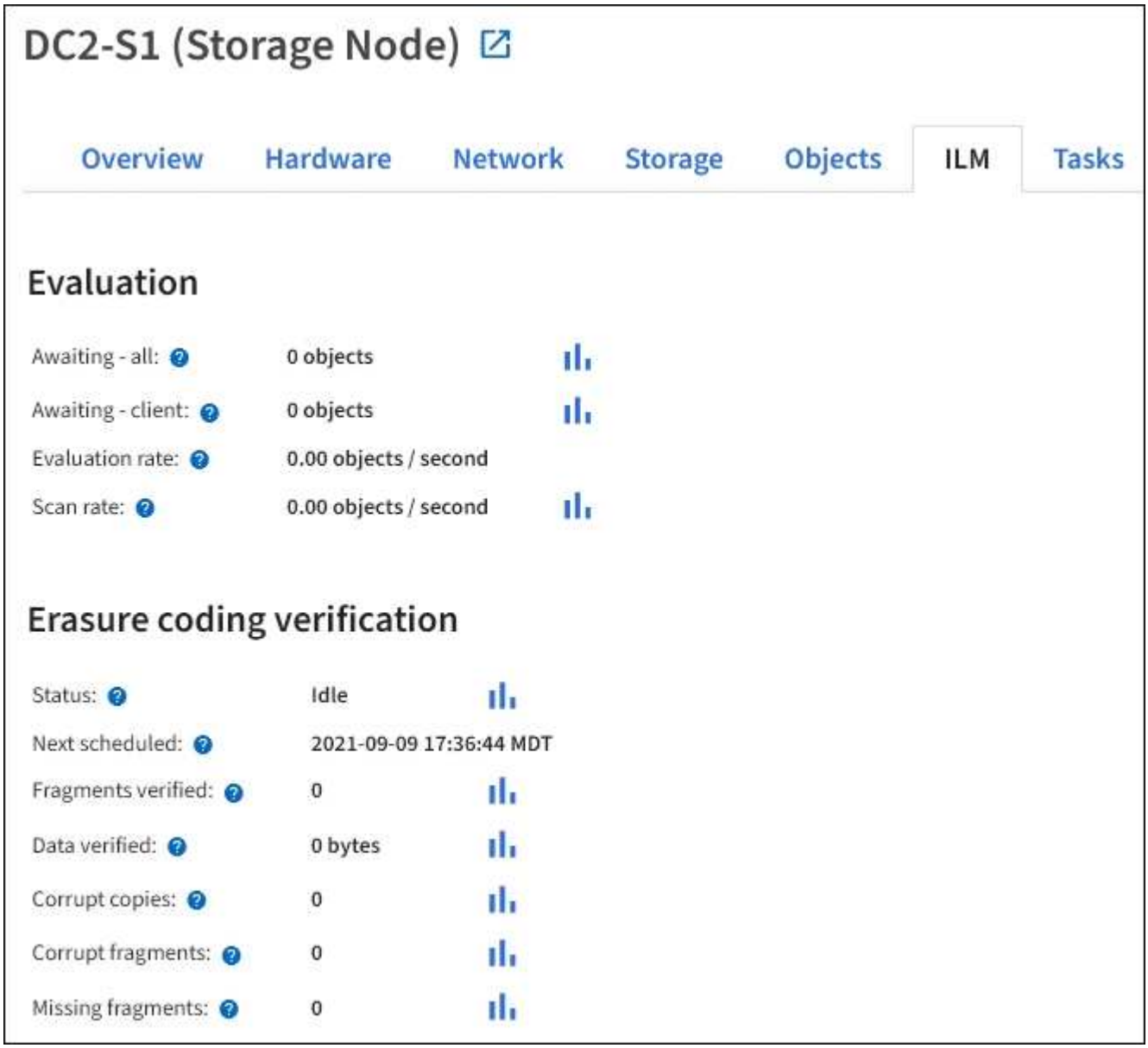

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

Anzeigen der Registerkarte „ILM“

Die Registerkarte „ILM“ bietet Informationen zu Vorgängen im Zusammenhang mit dem Information Lifecycle Management (ILM).

Die ILM-Registerkarte wird für jeden Speicherknoten, jeden Standort und das gesamte Raster angezeigt. Für jeden Standort und jedes Raster wird auf der Registerkarte „ILM“ ein Diagramm der ILM-Warteschlange im Zeitverlauf angezeigt. Für das Raster wird auf dieser Registerkarte auch die geschätzte Zeit angegeben, die zum Abschließen eines vollständigen ILM-Scans aller Objekte benötigt wird.

Für Speicherknoten bietet die Registerkarte „ILM“ Details zur ILM-Auswertung und Hintergrundüberprüfung für Erasure-Codierte Objekte.



Ähnliche Informationen

- "Überwachen Sie das Informationslebenszyklusmanagement"
- "StorageGRID verwalten"

Verwenden Sie die Registerkarte Aufgaben

Die Registerkarte „Aufgaben“ wird für alle Knoten angezeigt. Sie können diese Registerkarte verwenden, um einen Knoten umzubenennen oder neu zu starten oder um einen Appliance-Knoten in den Wartungsmodus zu versetzen.

Die vollständigen Anforderungen und Anweisungen für jede Option auf dieser Registerkarte finden Sie hier:

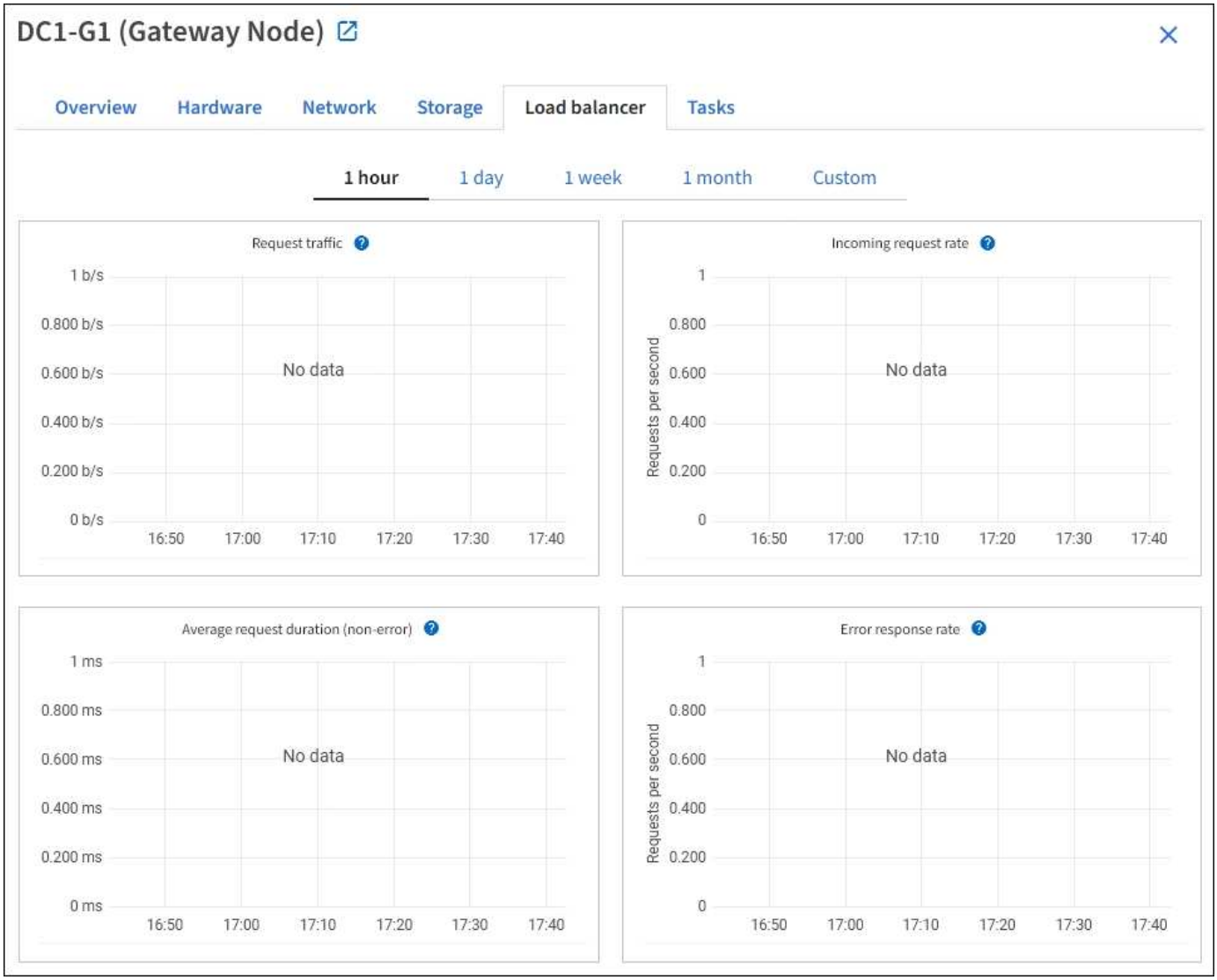
- "Raster, Sites und Knoten umbenennen"
- "Grid-Knoten neu starten"
- "Gerät in den Wartungsmodus versetzen"

Registerkarte „Load Balancer“ anzeigen

Die Registerkarte „Load Balancer“ enthält Leistungs- und Diagnosediagramme zum Betrieb des Load Balancer-Dienstes.

Die Registerkarte „Load Balancer“ wird für Admin-Knoten und Gateway-Knoten, jede Site und das gesamte Grid angezeigt. Für jeden Standort bietet die Registerkarte „Load Balancer“ eine aggregierte Zusammenfassung der Statistiken für alle Knoten an diesem Standort. Für das gesamte Raster bietet die Registerkarte „Load Balancer“ eine aggregierte Zusammenfassung der Statistiken für alle Sites.

Wenn über den Load Balancer-Dienst keine E/A ausgeführt wird oder kein Load Balancer konfiguriert ist, wird in den Diagrammen „Keine Daten“ angezeigt.



Verkehr anfordern

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt des Datendurchsatzes, der zwischen den Endpunkten des Lastenausgleichs und den Clients, die die Anfragen stellen, in Bits pro Sekunde übertragen wird.

> Dieser Wert wird nach Abschluss jeder Anfrage aktualisiert. Daher kann dieser Wert bei niedrigen Anforderungsraten oder sehr langlebigen Anforderungen vom Echtzeitdurchsatz abweichen. Sie können auf der Registerkarte „Netzwerk“ einen realistischeren Überblick über das aktuelle Netzwerkverhalten erhalten.

Rate eingehender Anfragen

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt der Anzahl neuer Anfragen pro Sekunde, aufgeschlüsselt nach Anfragetyp (GET, PUT, HEAD und DELETE). Dieser Wert wird aktualisiert, wenn die Header einer neuen Anfrage validiert wurden.

Durchschnittliche Anfragedauer (ohne Fehler)

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt der Anfragedauer, aufgeschlüsselt nach Anfragetyp (GET, PUT, HEAD und DELETE). Die Dauer jeder Anfrage beginnt, wenn ein Anfrageheader vom

Load Balancer-Dienst analysiert wird, und endet, wenn der vollständige Antworttext an den Client zurückgegeben wird.

Fehlerantwortrate

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt der Anzahl der pro Sekunde an Clients zurückgegebenen Fehlerantworten, aufgeschlüsselt nach Fehlerantwortcode.

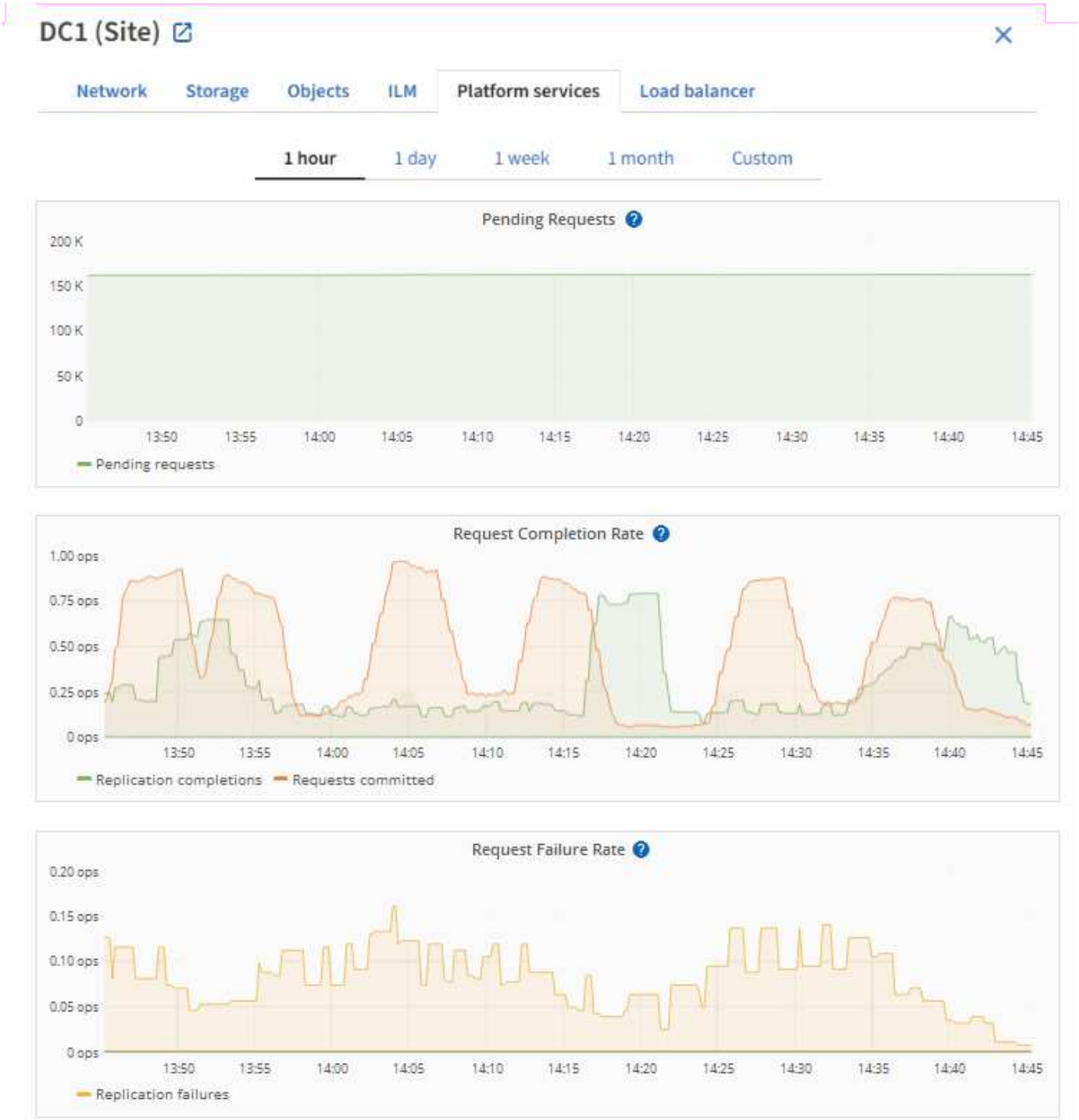
Ähnliche Informationen

- "Überwachen von Lastausgleichsvorgängen"
- "StorageGRID verwalten"

Registerkarte „Plattformdienste“ anzeigen

Die Registerkarte „Plattformdienste“ bietet Informationen zu allen S3-Plattformdienstvorgängen an einem Standort.

Die Registerkarte „Plattformdienste“ wird für jede Site angezeigt. Diese Registerkarte bietet Informationen zu S3-Plattformdiensten, wie z. B. CloudMirror-Replikation und Suchintegrationsdienst. Die Diagramme auf dieser Registerkarte zeigen Kennzahlen wie die Anzahl ausstehender Anfragen, die Anfrageabschlussrate und die Anfragefehlerrate an.



Weitere Informationen zu den S3-Plattformdiensten, einschließlich Details zur Fehlerbehebung, finden Sie im"Anweisungen zur Administration von StorageGRID" .

Anzeigen der Registerkarte „Laufwerke verwalten“

Über die Registerkarte „Laufwerke verwalten“ können Sie auf Details zugreifen und Fehlerbehebungs- und Wartungsaufgaben an Laufwerken in den Appliances durchführen, die diese Funktion unterstützen.

Über die Registerkarte „Laufwerke verwalten“ können Sie Folgendes tun:

- Anzeigen eines Layouts der Datenspeicherlaufwerke im Gerät
- Zeigen Sie eine Tabelle an, in der die einzelnen Laufwerksstandorte, Typen, Status, Firmware-Versionen und Seriennummern aufgeführt sind.
- Führen Sie an jedem Laufwerk Fehlerbehebungs- und Wartungsfunktionen durch

Um auf die Registerkarte Laufwerke verwalten zuzugreifen, müssen Sie über die"Speichergeräteadministrator oder Root-Zugriffsberechtigung" .

Informationen zur Verwendung der Registerkarte „Laufwerke verwalten“ finden Sie unter "Verwenden Sie die Registerkarte „Laufwerke verwalten“" .

Registerkarte „ SANtricity System Manager“ anzeigen (nur E-Serie)

Über die Registerkarte „SANtricity System Manager“ können Sie auf den SANtricity System Manager zugreifen, ohne den Verwaltungsport des Speichergeräts konfigurieren oder verbinden zu müssen. Auf dieser Registerkarte können Sie Hardwarediagnose- und Umgebungsinformationen sowie Probleme im Zusammenhang mit den Laufwerken überprüfen.

> Der Zugriff auf den SANtricity System Manager vom Grid Manager aus dient im Allgemeinen nur der Überwachung der Gerätehardware und der Konfiguration von E-Series AutoSupport. Viele Funktionen und Vorgänge im SANtricity System Manager, wie z. B. das Aktualisieren der Firmware, gelten nicht für die Überwachung Ihres StorageGRID Geräts. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Wartungsanweisungen für Ihr Gerät. Informationen zum Upgrade der SANtricity -Firmware finden Sie im "Wartungskonfigurationsverfahren" für Ihr Speichergerät.

> Die Registerkarte „SANtricity System Manager“ wird nur für Speichergeräteknoten angezeigt, die E-Series-Hardware verwenden.

Mit SANtricity System Manager können Sie Folgendes tun:

- Zeigen Sie Leistungsdaten wie Leistung auf Speicherarrayebene, E/A-Latenz, CPU-Auslastung des Speichercontrollers und Durchsatz an.
- Überprüfen Sie den Status der Hardwarekomponenten.
- Führen Sie Supportfunktionen aus, einschließlich der Anzeige von Diagnosedaten und der Konfiguration von E-Series AutoSupport.

> Informationen zur Verwendung von SANtricity System Manager zum Konfigurieren eines Proxys für E-Series AutoSupport finden Sie unter"Senden Sie E-Series AutoSupport -Pakete über StorageGRID" .

Um über Grid Manager auf SANtricity System Manager zuzugreifen, benötigen Sie die"Speichergeräteadministrator oder Root-Zugriffsberechtigung" .

> Sie müssen über die SANtricity -Firmware 8.70 oder höher verfügen, um über den Grid Manager auf den SANtricity System Manager zugreifen zu können.

Die Registerkarte zeigt die Homepage von SANtricity System Manager an.

Sie können den SANtricity System Manager-Link verwenden, um den SANtricity System Manager zur einfacheren Anzeige in einem neuen Browserfenster zu öffnen.

Um Details zur Leistung und Kapazitätsnutzung auf Speicher-Array-Ebene anzuzeigen, positionieren Sie den Cursor über jedem Diagramm.

Weitere Informationen zum Anzeigen der Informationen, die über die Registerkarte SANtricity System Manager zugänglich sind, finden Sie unter "Dokumentation zu NetApp E-Series und SANtricity" .

Regelmäßig zu überwachende Informationen

Was und wann zu überwachen ist

Auch wenn das StorageGRID -System weiterbetrieben werden kann, wenn Fehler auftreten oder Teile des Netzes nicht verfügbar sind, sollten Sie potenzielle Probleme überwachen und beheben, bevor sie die Effizienz oder Verfügbarkeit des Netzes beeinträchtigen.

Bevor Sie beginnen

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

Informationen zu Überwachungsaufgaben

Ein ausgelastetes System erzeugt große Mengen an Informationen. Die folgende Liste enthält Hinweise zu den wichtigsten Informationen, die kontinuierlich überwacht werden müssen.

Was zu überwachen ist	Frequenz
"Systemintegritätsstatus"	Täglich
Rate, mit der"Speicherknotenobjekt- und Metadatenkapazität" wird konsumiert	Wöchentlich
"Vorgänge zur Verwaltung des Informationslebenszyklus"	Wöchentlich
"Netzwerk- und Systemressourcen"	Wöchentlich
"Mieteraktivität"	Wöchentlich
"S3-Clientvorgänge"	Wöchentlich
"Lastausgleichsvorgänge"	Nach der Erstkonfiguration und nach allen Konfigurationsänderungen
"Grid-Föderation-Verbindungen"	Wöchentlich

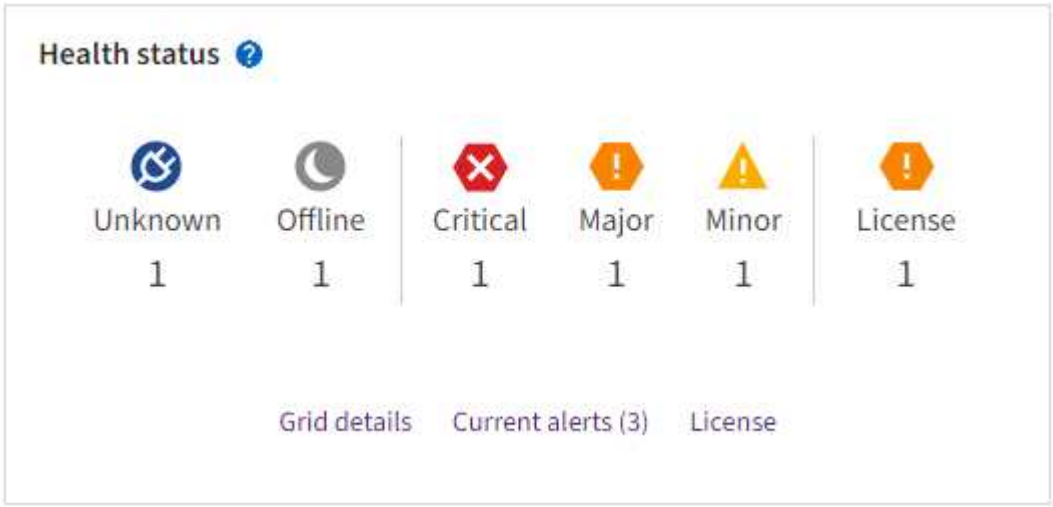
Überwachen Sie den Systemzustand

Überwachen Sie täglich den Gesamtzustand Ihres StorageGRID -Systems.

Informationen zu diesem Vorgang

Das StorageGRID -System kann weiterbetrieben werden, wenn Teile des Netzes nicht verfügbar sind. Bei den durch Warnungen angezeigten potenziellen Problemen handelt es sich nicht unbedingt um Probleme mit dem Systembetrieb. Untersuchen Sie die auf der Integritätsstatuskarte des Grid Manager-Dashboards zusammengefassten Probleme.

Um über Alarme informiert zu werden, sobald diese ausgelöst werden, können Sie "E-Mail-Benachrichtigungen für Warnungen einrichten" oder"SNMP-Traps konfigurieren" .



Wenn Probleme vorliegen, werden Links angezeigt, über die Sie weitere Details anzeigen können:

Link	Erscheint, wenn…
Rasterdetails	Alle Knoten sind getrennt (Verbindungsstatus „Unbekannt“ oder „Administrativ deaktiviert“).
Aktuelle Warnungen (Kritisch, Schwerwiegend, Geringfügig)	Warnungen sindderzeit aktiv .
Kürzlich gelöste Warnungen	In der letzten Woche ausgelöste Warnungensind nun gelöst .
Lizenz	Es gibt ein Problem mit der Softwarelizenz für dieses StorageGRID -System. Sie können "Aktualisieren Sie die Lizenzinformationen nach Bedarf" .

Überwachen Sie den Verbindungsstatus des Knotens

Wenn ein oder mehrere Knoten vom Netz getrennt werden, können kritische StorageGRID Vorgänge beeinträchtigt werden. Überwachen Sie den Verbindungsstatus der Knoten und beheben Sie etwaige Probleme umgehend.

Symbol	Beschreibung	Handlungsbedarf
	**Nicht verbunden – Unbekannt** Aus einem unbekannten Grund wird die Verbindung zu einem Knoten getrennt oder die Dienste auf dem Knoten fallen unerwartet aus. Beispielsweise könnte ein Dienst auf dem Knoten gestoppt worden sein oder der Knoten könnte aufgrund eines Stromausfalls oder einer unerwarteten Störung seine Netzwerkverbindung verloren haben. Möglicherweise wird auch die Warnung **Kommunikation mit Knoten nicht möglich** ausgelöst. Möglicherweise sind auch andere Warnungen aktiv.	Erfordert sofortige Aufmerksamkeit. Wählen Sie jede Warnung aus und befolgen Sie die empfohlenen Maßnahmen. Beispielsweise müssen Sie möglicherweise einen angehaltenen Dienst neu starten oder den Host für den Knoten neu starten. **Hinweis**: Während verwalteter Herunterfahrvorgänge kann ein Knoten als „Unbekannt“ angezeigt werden. In diesen Fällen können Sie den Status „Unbekannt“ ignorieren.
	**Nicht verbunden – Administrator-Ausfall** Aus einem erwarteten Grund ist der Knoten nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Möglicherweise sind auch eine oder mehrere Warnungen aktiv. Je nach zugrunde liegendem Problem gehen diese Knoten häufig ohne Eingriff wieder online.	Stellen Sie fest, ob dieser Knoten von Warnungen betroffen ist. Wenn eine oder mehrere Warnungen aktiv sind,Wählen Sie jeden Alarm aus und befolgen Sie die empfohlenen Maßnahmen.
	**Verbunden** Der Knoten ist mit dem Netz verbunden.	Keine Aktion erforderlich.

Aktuelle und gelöste Warnmeldungen anzeigen

Aktuelle Warnungen: Wenn eine Warnung ausgelöst wird, wird auf dem Dashboard ein Warnsymbol angezeigt. Auf der Seite „Knoten“ wird für den Knoten außerdem ein Warnsymbol angezeigt. Wenn"E-Mail-Benachrichtigungen sind konfiguriert" , wird auch eine E-Mail-Benachrichtigung gesendet, sofern der Alarm nicht stummgeschaltet wurde.

Behobene Warnungen: Sie können einen Verlauf der behobenen Warnungen suchen und anzeigen.

Optional haben Sie das Video angesehen: "Video: Übersicht über Warnungen"

Die folgende Tabelle beschreibt die im Grid Manager angezeigten Informationen für aktuelle und gelöste Warnungen.

Spaltenüberschrift	Beschreibung
Name oder Titel	Der Name der Warnung und ihre Beschreibung.
Schwere	Der Schweregrad der Warnung. Bei aktuellen Warnungen zeigt die Titelzeile, wenn mehrere Warnungen gruppiert sind, wie viele Instanzen dieser Warnung bei jedem Schweregrad auftreten. **Kritisch**: Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort angehen. Wenn das Problem nicht behoben wird, kann es zu Dienstunterbrechungen und Datenverlust kommen. **Schwerwiegend**: Es liegt ein anormaler Zustand vor, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten wichtige Warnungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder -Dienstes nicht stoppt. **Geringfügig**: Das System funktioniert normal, es liegt jedoch ein anormaler Zustand vor, der die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn er anhält. Sie sollten kleinere Warnungen, die nicht von selbst verschwinden, überwachen und beheben, um sicherzustellen, dass sie nicht zu einem ernsteren Problem führen.
Zeitgesteuert	**Aktuelle Warnungen**: Datum und Uhrzeit der Auslösung der Warnung in Ihrer Ortszeit und in UTC. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile die Zeiten für die jüngste Instanz der Warnung (*neueste*) und die älteste Instanz der Warnung (*älteste*) an. **Behobene Warnungen**: Wie lange es her ist, dass die Warnung ausgelöst wurde.
Site/Knoten	Der Name der Site und des Knotens, an dem der Alarm auftritt oder aufgetreten ist.

Spaltenüberschrift	Beschreibung
Status	Ob der Alarm aktiv, stummgeschaltet oder behoben ist. Wenn mehrere Warnungen gruppiert sind und im Dropdown-Menü „Alle Warnungen“ ausgewählt ist, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung aktiv sind und wie viele Instanzen stummgeschaltet wurden.
Zeit bis zur Lösung (nur gelöste Warnungen)	Wie lange es her ist, dass die Warnung behoben wurde.
Aktuelle Werte oder *Datenwerte*	Der Wert der Metrik, die zur Auslösung der Warnung geführt hat. Bei einigen Warnungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnung zu verstehen und zu untersuchen. Die für die Warnung **Geringer Objektdatenspeicher** angezeigten Werte umfassen beispielsweise den Prozentsatz des verwendeten Speicherplatzes, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Speicherplatzes. **Hinweis:** Wenn mehrere aktuelle Warnungen gruppiert sind, werden die aktuellen Werte nicht in der Titelzeile angezeigt.
Ausgelöste Werte (nur gelöste Warnungen)	Der Wert der Metrik, die zur Auslösung der Warnung geführt hat. Bei einigen Warnungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnung zu verstehen und zu untersuchen. Die für die Warnung **Geringer Objektdatenspeicher** angezeigten Werte umfassen beispielsweise den Prozentsatz des verwendeten Speicherplatzes, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Speicherplatzes.

Schritte

1. Wählen Sie den Link **Aktuelle Warnungen** oder **Behobene Warnungen** aus, um eine Liste der Warnungen in diesen Kategorien anzuzeigen. Sie können die Details einer Warnung auch anzeigen, indem Sie **Knoten** > ***Knoten*** > **Übersicht** auswählen und dann die Warnung aus der Tabelle „Warnungen“ auswählen.

   Aktuelle Warnungen werden standardmäßig wie folgt angezeigt:

   - Die zuletzt ausgelösten Warnungen werden zuerst angezeigt.
   - Mehrere Warnungen desselben Typs werden als Gruppe angezeigt.
   - Stummgeschaltete Warnungen werden nicht angezeigt.
   - Wenn für eine bestimmte Warnung auf einem bestimmten Knoten die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird nur die Warnung mit dem höchsten Schweregrad angezeigt. Das heißt, wenn Warnschwellenwerte für die Schweregrade „geringfügig“, „schwerwiegend“ und „kritisch“ erreicht werden, wird nur die kritische Warnung angezeigt.

     Die Seite „Aktuelle Warnungen“ wird alle zwei Minuten aktualisiert.

2. Um Gruppen von Warnungen zu erweitern, wählen Sie das Abwärtspfeilzeichen . Um einzelne Warnungen in einer Gruppe auszublenden, wählen Sie das Aufwärts-Caret , oder wählen Sie den Namen der Gruppe aus.
3. Um einzelne Warnungen statt Warnungsgruppen anzuzeigen, deaktivieren Sie das Kontrollkästchen **Warnungen gruppieren**.

4. Um aktuelle Warnungen oder Warnungsgruppen zu sortieren, wählen Sie die Aufwärts-/Abwärtspfeile in jeder Spaltenüberschrift.
   - Wenn **Gruppenwarnungen** ausgewählt ist, werden sowohl die Warnungsgruppen als auch die einzelnen Warnungen innerhalb jeder Gruppe sortiert. Beispielsweise möchten Sie möglicherweise die Warnungen in einer Gruppe nach **Auslösezeit** sortieren, um die aktuellste Instanz einer bestimmten Warnung zu finden.
   - Wenn **Gruppenwarnungen** gelöscht wird, wird die gesamte Liste der Warnungen sortiert. Sie möchten beispielsweise möglicherweise alle Warnungen nach **Knoten/Site** sortieren, um alle Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.
5. Um aktuelle Warnungen nach Status (**Alle Warnungen**, **Aktiv** oder **Stummgeschaltet**) zu filtern, verwenden Sie das Dropdown-Menü oben in der Tabelle.

   Sehen "Warnmeldungen stummschalten" .
6. So sortieren Sie gelöste Warnungen:
   - Wählen Sie einen Zeitraum aus dem Dropdown-Menü **Bei Auslösung** aus.
   - Wählen Sie einen oder mehrere Schweregrade aus dem Dropdown-Menü **Schweregrad** aus.
   - Wählen Sie aus dem Dropdown-Menü **Alarmregel** eine oder mehrere standardmäßige oder benutzerdefinierte Alarmregeln aus, um nach gelösten Alarmen zu filtern, die sich auf eine bestimmte Alarmregel beziehen.
   - Wählen Sie einen oder mehrere Knoten aus dem Dropdown-Menü **Knoten** aus, um nach gelösten Warnungen zu filtern, die sich auf einen bestimmten Knoten beziehen.
7. Um Details zu einer bestimmten Warnung anzuzeigen, wählen Sie die Warnung aus. Ein Dialogfeld enthält Details und empfohlene Maßnahmen für die von Ihnen ausgewählte Warnung.
8. (Optional) Wählen Sie für eine bestimmte Warnung „Diese Warnung stummschalten“ aus, um die Warnungsregel stummzuschalten, die die Auslösung dieser Warnung verursacht hat.

   Sie müssen über die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" um eine Warnregel stummzuschalten.

   > Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel stummzuschalten. Wenn eine Warnregel stummgeschaltet wird, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.
9. So zeigen Sie die aktuellen Bedingungen für die Warnregel an:
   a. Wählen Sie in den Alarmdetails **Bedingungen anzeigen** aus.

      Es wird ein Popup-Fenster angezeigt, in dem der Prometheus-Ausdruck für jeden definierten Schweregrad aufgelistet ist.

   b. Um das Popup zu schließen, klicken Sie irgendwo außerhalb des Popups.
10. Wählen Sie optional **Regel bearbeiten** aus, um die Warnregel zu bearbeiten, die zur Auslösung dieser Warnung geführt hat.

    Sie müssen über die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" , um eine Warnregel zu bearbeiten.

Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel zu bearbeiten. Wenn Sie Triggerwerte ändern, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

11. Um die Alarmdetails zu schließen, wählen Sie **Schließen**.

Überwachen der Speicherkapazität

Überwachen Sie den insgesamt verfügbaren nutzbaren Speicherplatz, um sicherzustellen, dass dem StorageGRID -System nicht der Speicherplatz für Objekte oder Objektmetadaten ausgeht.

StorageGRID speichert Objektdaten und Objektmetadaten getrennt und reserviert eine bestimmte Menge an Speicherplatz für eine verteilte Cassandra-Datenbank, die Objektmetadaten enthält. Überwachen Sie den Gesamtspeicherplatzverbrauch für Objekte und Objektmetadaten sowie Trends beim jeweiligen Speicherplatzverbrauch. Auf diese Weise können Sie das Hinzufügen von Knoten im Voraus planen und Dienstausfälle vermeiden.

Du kannst"Informationen zur Speicherkapazität anzeigen" für das gesamte Grid, für jeden Standort und für jeden Speicherknoten in Ihrem StorageGRID System.

Speicherkapazität für das gesamte Netz überwachen

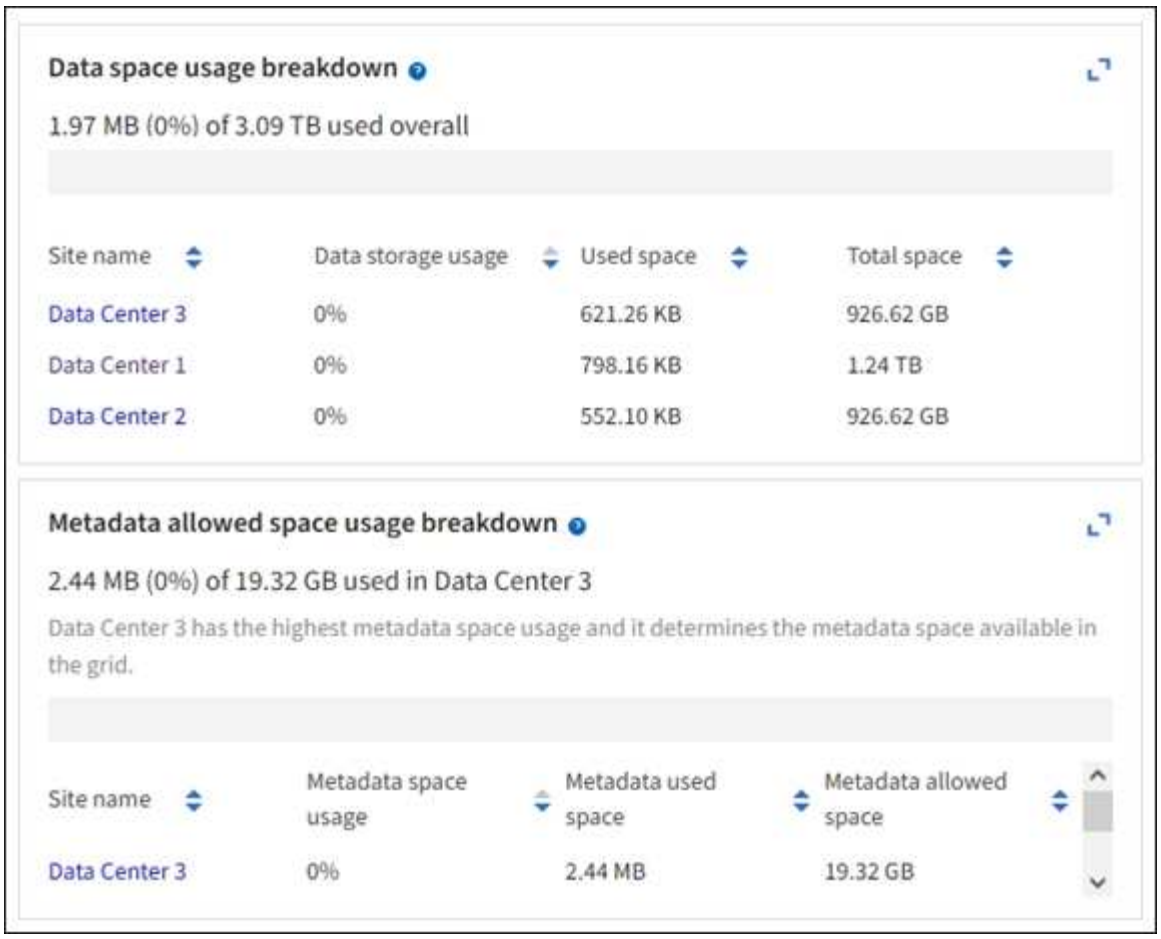
Überwachen Sie die Gesamtspeicherkapazität Ihres Grids, um sicherzustellen, dass ausreichend freier Speicherplatz für Objektdaten und Objektmetadaten verbleibt. Wenn Sie wissen, wie sich die Speicherkapazität im Laufe der Zeit ändert, können Sie das Hinzufügen von Speicherknoten oder Speichervolumes besser planen, bevor die nutzbare Speicherkapazität des Grids verbraucht ist.

Über das Grid Manager-Dashboard können Sie schnell beurteilen, wie viel Speicher für das gesamte Grid und für jedes Rechenzentrum verfügbar ist. Die Seite „Knoten“ bietet detailliertere Werte für Objektdaten und Objektmetadaten.

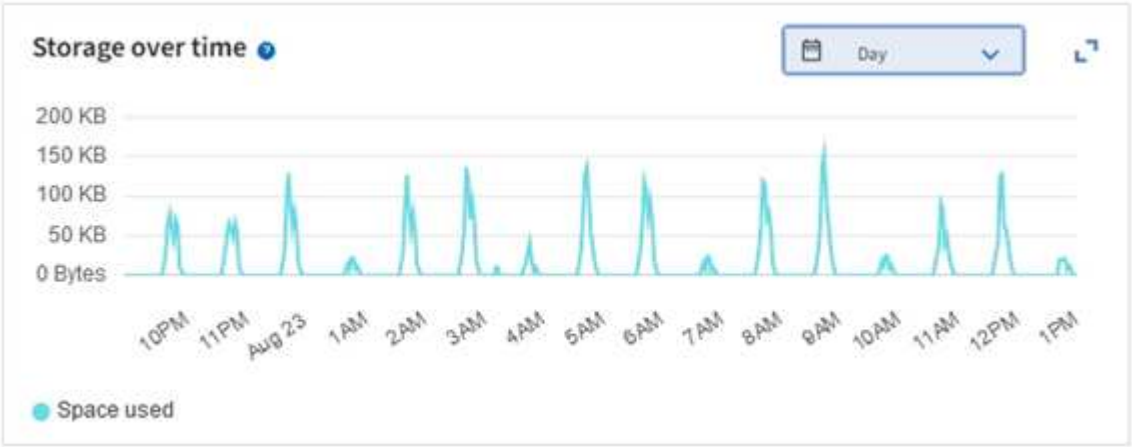
Schritte

1. Bewerten Sie, wie viel Speicher für das gesamte Grid und für jedes Rechenzentrum verfügbar ist.
   a. Wählen Sie **Dashboard > Übersicht**.
   b. Beachten Sie die Werte auf den Karten „Aufschlüsselung der Datenspeicherplatznutzung“ und „Aufschlüsselung der zulässigen Metadatenspeicherplatznutzung“. Auf jeder Karte ist ein Prozentsatz der Speichernutzung, die Kapazität des verwendeten Speicherplatzes und der gesamte verfügbare oder pro Site zulässige Speicherplatz aufgeführt.

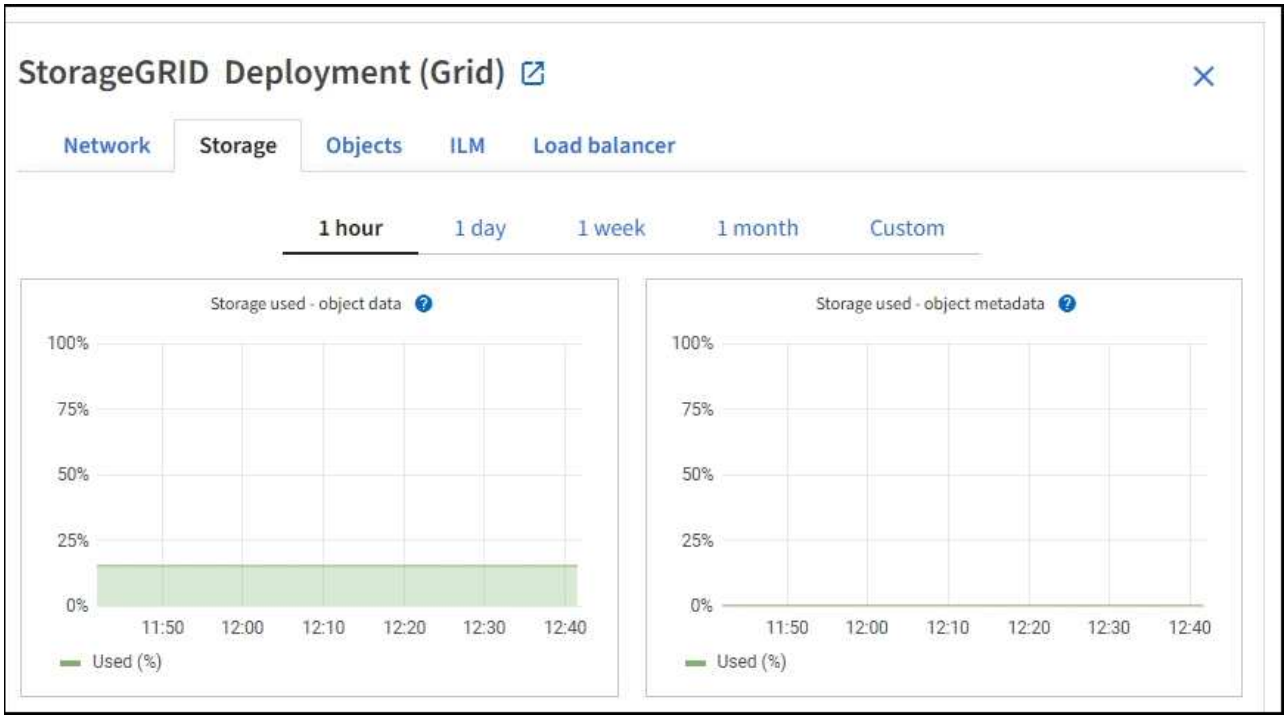
      Die Zusammenfassung umfasst keine Archivmedien.



a. Beachten Sie das Diagramm auf der Karte „Speicherung im Zeitverlauf“. Verwenden Sie das Dropdown-Menü für den Zeitraum, um zu ermitteln, wie schnell der Speicherplatz verbraucht wird.



2. Auf der Seite „Knoten“ finden Sie weitere Einzelheiten dazu, wie viel Speicherplatz verwendet wurde und wie viel Speicherplatz im Raster für Objektdaten und Objektmetadaten noch verfügbar ist.
   a. Wählen Sie **NODES**.
   b. Wählen Sie ***grid*** > **Speicher**.



c. Bewegen Sie den Cursor über die Diagramme **Verwendeter Speicher – Objektdaten** und **Verwendeter Speicher – Objektmetadaten**, um zu sehen, wie viel Objektspeicher und Objektmetadatenspeicher für das gesamte Raster verfügbar ist und wie viel im Laufe der Zeit verwendet wurde.

> Die Gesamtwerte für eine Site oder das Raster umfassen keine Knoten, die seit mindestens fünf Minuten keine Metriken gemeldet haben, beispielsweise Offline-Knoten.

3. Planen Sie eine Erweiterung, um Speicherknoten oder Speichervolumes hinzuzufügen, bevor die nutzbare Speicherkapazität des Grids verbraucht ist.

   Berücksichtigen Sie bei der Planung des Zeitpunkts einer Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Speicher dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, möchten Sie möglicherweise eine Erweiterung vornehmen, wenn vorhandene Speicherknoten zu etwa 70 % belegt sind, um die Anzahl der hinzuzufügenden Knoten zu reduzieren.

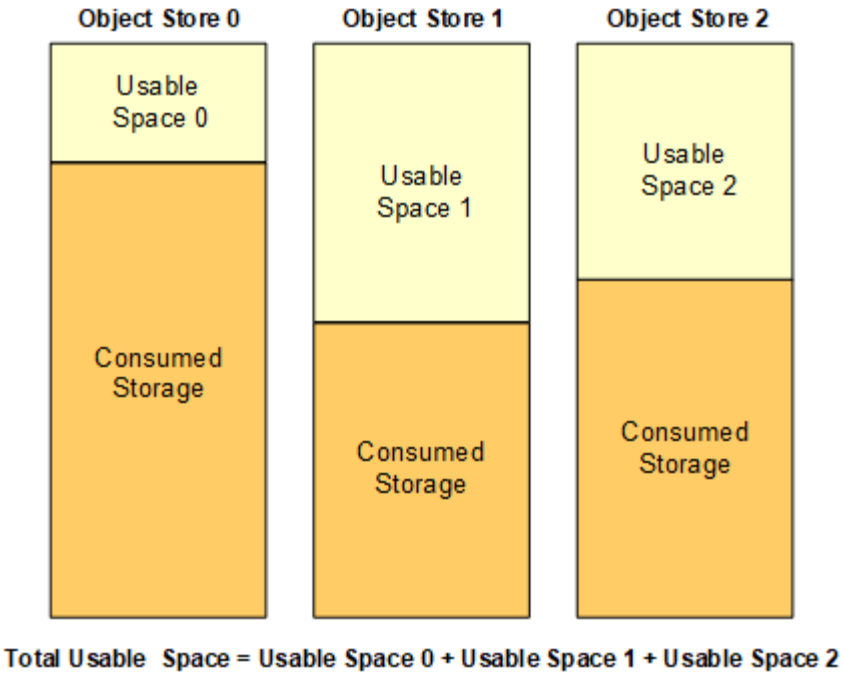
   Weitere Informationen zur Planung einer Speichererweiterung finden Sie im"Anleitung zur Erweiterung von StorageGRID" .

Überwachen Sie die Speicherkapazität für jeden Speicherknoten

Überwachen Sie den gesamten nutzbaren Speicherplatz für jeden Speicherknoten, um sicherzustellen, dass der Knoten über genügend Speicherplatz für neue Objektdaten verfügt.

Informationen zu diesem Vorgang

Der nutzbare Speicherplatz ist die Menge an Speicherplatz, die zum Speichern von Objekten zur Verfügung steht. Der gesamte nutzbare Speicherplatz für einen Speicherknoten wird berechnet, indem der verfügbare Speicherplatz aller Objektspeicher innerhalb des Knotens addiert wird.



Schritte

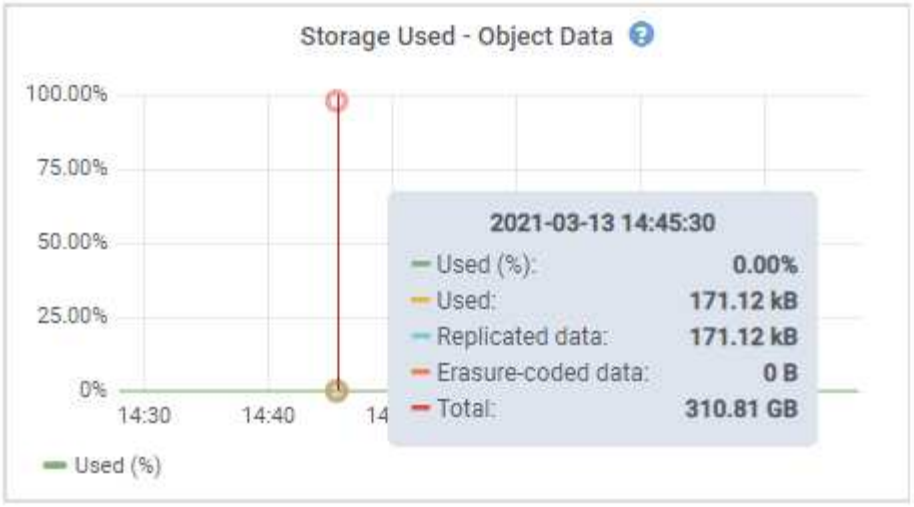
1. Wählen Sie **NODES** > ***Speicherknoten*** > **Speicher**.

   Die Diagramme und Tabellen für den Knoten werden angezeigt.

2. Positionieren Sie den Cursor über dem Datendiagramm „Speicherplatznutzung – Objekt“.

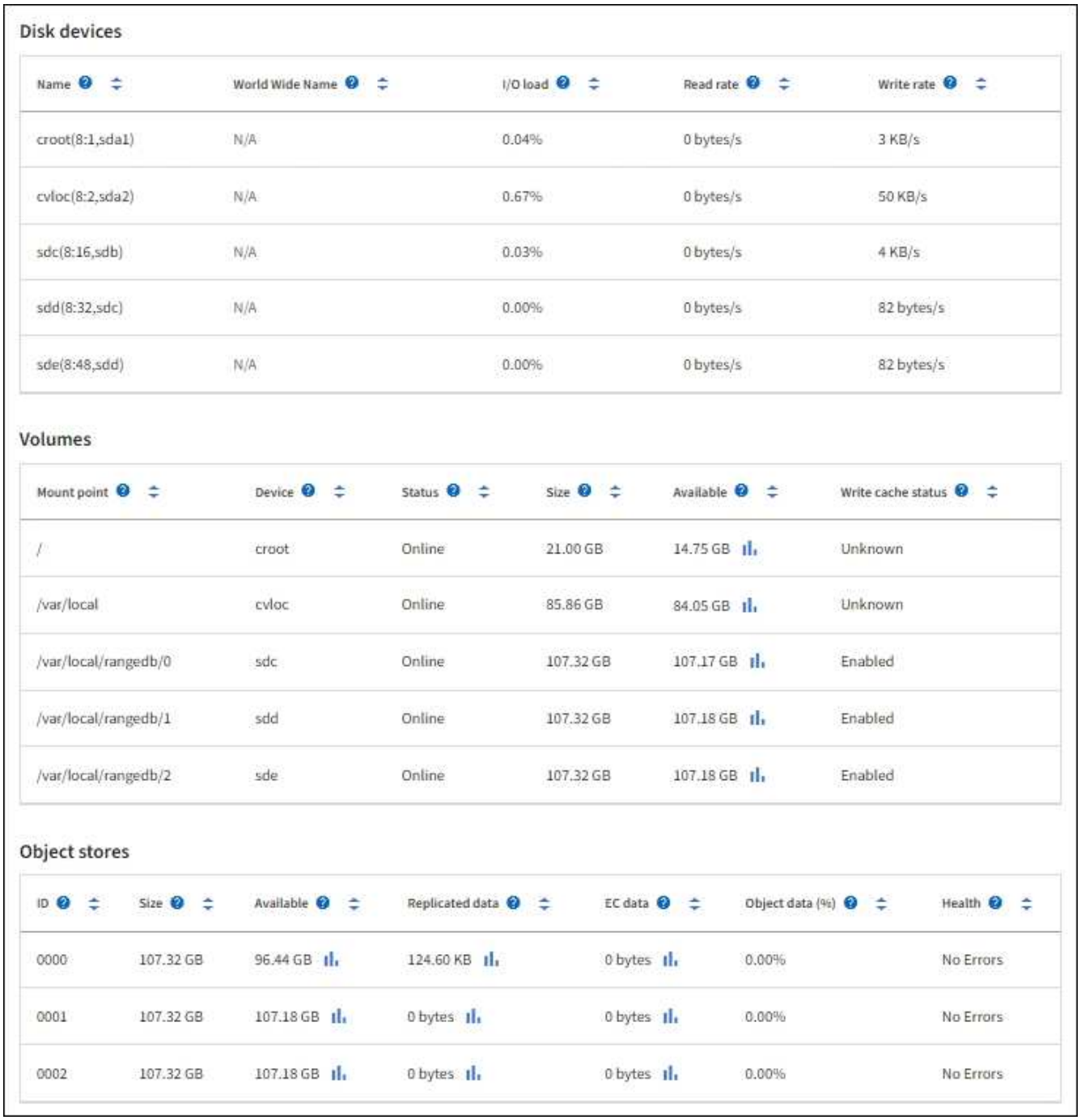
   Es werden folgende Werte angezeigt:

   - **Verwendet (%)**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
   - **Verwendet**: Die Menge des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
   - **Replizierte Daten**: Eine Schätzung der Menge der replizierten Objektdaten auf diesem Knoten, dieser Site oder diesem Raster.
   - **Löschcodierte Daten**: Eine Schätzung der Menge der löschcodierten Objektdaten auf diesem Knoten, dieser Site oder diesem Raster.
   - **Gesamt**: Die Gesamtmenge des nutzbaren Speicherplatzes auf diesem Knoten, dieser Site oder diesem Raster. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` metrisch.



3. Überprüfen Sie die verfügbaren Werte in den Tabellen „Volumes“ und „Objektspeicher“ unter den Diagrammen.

Um Diagramme dieser Werte anzuzeigen, klicken Sie auf die Diagrammsymbole in den Spalten „Verfügbar“.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. Überwachen Sie die Werte im Laufe der Zeit, um die Rate abzuschätzen, mit der nutzbarer Speicherplatz verbraucht wird.
5. Um den normalen Systembetrieb aufrechtzuerhalten, fügen Sie Speicherknoten und Speichervolumes hinzu oder archivieren Sie Objektdaten, bevor der nutzbare Speicherplatz verbraucht ist.

   Berücksichtigen Sie bei der Planung des Zeitpunkts einer Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Speicher dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, möchten Sie möglicherweise eine Erweiterung vornehmen, wenn vorhandene Speicherknoten zu etwa 70 % belegt sind, um die Anzahl der hinzuzufügenden Knoten zu reduzieren.

Weitere Informationen zur Planung einer Speichererweiterung finden Sie im"Anleitung zur Erweiterung von

StorageGRID" .

Der"Geringe Objektdatenspeicherung" Eine Warnung wird ausgelöst, wenn auf einem Speicherknoten nicht genügend Speicherplatz zum Speichern von Objektdaten vorhanden ist.

Überwachen Sie die Objektmetadatenkapazität für jeden Speicherknoten

Überwachen Sie die Metadatennutzung für jeden Speicherknoten, um sicherzustellen, dass ausreichend Speicherplatz für wichtige Datenbankvorgänge verfügbar bleibt. Sie müssen an jedem Standort neue Speicherknoten hinzufügen, bevor die Objektmetadaten 100 % des zulässigen Metadatenspeicherplatzes überschreiten.

Informationen zu diesem Vorgang

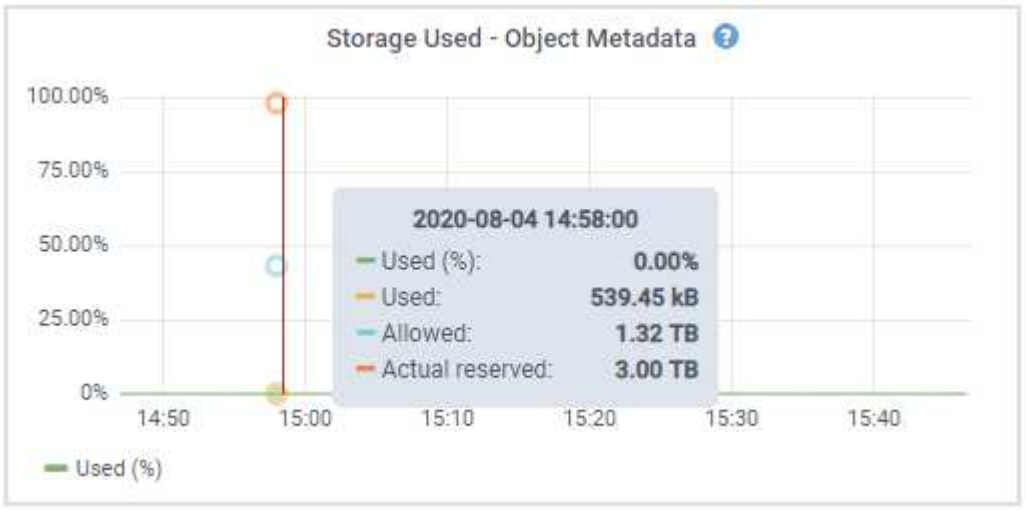
StorageGRID verwaltet an jedem Standort drei Kopien der Objektmetadaten, um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig auf alle Speicherknoten an jedem Standort verteilt, wobei der für Metadaten reservierte Speicherplatz auf Speichervolume 0 jedes Speicherknotens verwendet wird.

In einigen Fällen kann die Objektmetadatenkapazität des Grids schneller verbraucht werden als seine Objektspeicherkapazität. Wenn Sie beispielsweise normalerweise eine große Anzahl kleiner Objekte aufnehmen, müssen Sie möglicherweise Speicherknoten hinzufügen, um die Metadatenkapazität zu erhöhen, obwohl noch ausreichend Objektspeicherkapazität vorhanden ist.

Zu den Faktoren, die die Metadatennutzung erhöhen können, gehören unter anderem die Größe und Menge der Benutzermetadaten und Tags, die Gesamtzahl der Teile in einem mehrteiligen Upload und die Häufigkeit von Änderungen an ILM-Speicherorten.

Schritte

1. Wählen Sie **NODES** > ***Speicherknoten*** > **Speicher**.
2. Positionieren Sie den Cursor über dem Diagramm „Speicherplatznutzung – Objektmetadaten“, um die Werte für einen bestimmten Zeitpunkt anzuzeigen.



Gebraucht (%)

Der Prozentsatz des zulässigen Metadatenspeicherplatzes, der auf diesem Speicherknoten verwendet wurde.

Prometheus-Metriken: `storagegrid_storage_utilization_metadata_bytes` Und

`storagegrid_storage_utilization_metadata_allowed_bytes`

Gebraucht

Die Bytes des zulässigen Metadatenspeichers, die auf diesem Speicherknoten verwendet wurden.

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_bytes`

Erlaubt

Der für Objektmetadaten auf diesem Speicherknoten zulässige Speicherplatz. Um zu erfahren, wie dieser Wert für jeden Speicherknoten ermittelt wird, lesen Sie die"vollständige Beschreibung des zulässigen Metadatenbereichs" .

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_allowed_bytes`

Tatsächlich reserviert

Der tatsächliche Speicherplatz, der auf diesem Speicherknoten für Metadaten reserviert ist. Beinhaltet den zulässigen Speicherplatz und den erforderlichen Speicherplatz für wichtige Metadatenvorgänge. Um zu erfahren, wie dieser Wert für jeden Speicherknoten berechnet wird, lesen Sie die"vollständige Beschreibung des tatsächlich reservierten Speicherplatzes für Metadaten" .

Die Prometheus-Metrik wird in einer zukünftigen Version hinzugefügt.

Die Gesamtwerte für eine Site oder das Raster umfassen keine Knoten, die seit mindestens fünf Minuten keine Metriken gemeldet haben, beispielsweise Offline-Knoten.

3. Wenn der Wert **Verwendet (%)** 70 % oder höher ist, erweitern Sie Ihr StorageGRID -System, indem Sie jedem Standort Speicherknoten hinzufügen.

Die Warnung **Geringer Metadatenspeicher** wird ausgelöst, wenn der Wert **Verwendet (%)** bestimmte Schwellenwerte erreicht. Wenn die Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes belegen, können unerwünschte Ergebnisse auftreten.

Wenn Sie die neuen Knoten hinzufügen, gleicht das System die Objektmetadaten automatisch über alle Speicherknoten innerhalb der Site aus. Siehe die"Anleitung zur Erweiterung eines StorageGRID -Systems" .

Überwachen Sie Prognosen zur Speicherplatznutzung

Überwachen Sie die Speichernutzungsprognosen für Benutzerdaten und Metadaten, um abzuschätzen, wann Sie"ein Raster erweitern" .

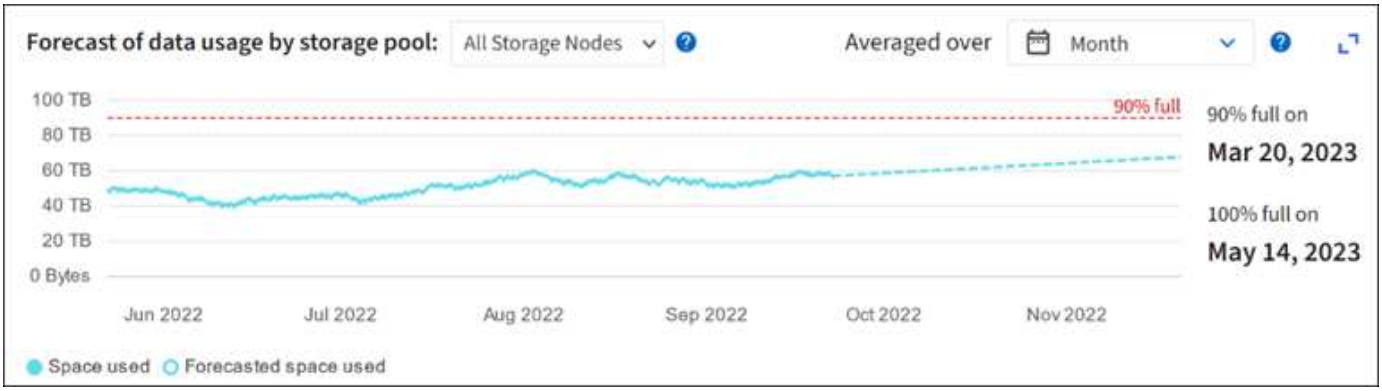
Wenn Sie feststellen, dass sich die Verbrauchsrate im Laufe der Zeit ändert, wählen Sie im Pulldown-Menü „**Durchschnitt über**“ einen kürzeren Bereich aus, um nur die aktuellsten Aufnahmemuster anzuzeigen. Wenn Sie saisonale Muster erkennen, wählen Sie einen längeren Bereich.

Wenn Sie eine neue StorageGRID Installation haben, warten Sie, bis sich Daten und Metadaten angesammelt haben, bevor Sie die Prognosen zur Speicherplatznutzung auswerten.

Schritte

1. Wählen Sie im Dashboard **Speicher** aus.
2. Zeigen Sie die Dashboard-Karten, die Prognose der Datennutzung nach Speicherpool und die Prognose der Metadatennutzung nach Site an.

3. Verwenden Sie diese Werte, um abzuschätzen, wann Sie neue Speicherknoten zur Daten- und Metadatenspeicherung hinzufügen müssen.



Überwachen Sie das Informationslebenszyklusmanagement

Das Information Lifecycle Management (ILM)-System bietet Datenverwaltung für alle im Grid gespeicherten Objekte. Sie müssen die ILM-Vorgänge überwachen, um zu wissen, ob das Grid die aktuelle Last bewältigen kann oder ob mehr Ressourcen benötigt werden.

Informationen zu diesem Vorgang

Das StorageGRID -System verwaltet Objekte durch Anwendung der aktiven ILM-Richtlinien. Die ILM-Richtlinien und die zugehörigen ILM-Regeln bestimmen, wie viele Kopien erstellt werden, welche Art von Kopien erstellt werden, wo die Kopien abgelegt werden und wie lange jede Kopie aufbewahrt wird.

Die Objektaufnahme und andere objektbezogene Aktivitäten können die Rate überschreiten, mit der StorageGRID ILM auswerten kann. Dies führt dazu, dass das System Objekte in die Warteschlange stellt, deren ILM-Platzierungsanweisungen nicht nahezu in Echtzeit erfüllt werden können. Sie sollten überwachen, ob StorageGRID mit den Client-Aktionen Schritt hält.

Verwenden Sie die Dashboard-Registerkarte des Grid Managers

Schritte

Verwenden Sie die Registerkarte „ILM“ im Grid Manager-Dashboard, um ILM-Vorgänge zu überwachen:

1. Sign in .
2. Wählen Sie im Dashboard die Registerkarte „ILM“ aus und notieren Sie sich die Werte auf der Karte „ILM-Warteschlange (Objekte)“ und der Karte „ILM-Auswertungstarif“.

   Es ist mit vorübergehenden Spitzen in der ILM-Warteschlangenkarte (Objekte) auf dem Dashboard zu rechnen. Wenn die Warteschlange jedoch weiter zunimmt und nicht abnimmt, benötigt das Grid mehr Ressourcen, um effizient zu arbeiten: entweder mehr Speicherknoten oder, wenn die ILM-Richtlinie Objekte an entfernten Standorten platziert, mehr Netzwerkbandbreite.

Verwenden der NODES-Seite

Schritte

Untersuchen Sie außerdem ILM-Warteschlangen mithilfe der Seite **NODES**:

Die Diagramme auf der Seite **NODES** werden in einer zukünftigen StorageGRID Version durch die entsprechenden Dashboard-Karten ersetzt.

1. Wählen Sie **NODES**.
2. Wählen Sie ***Gridname*** > **ILM**.
3. Positionieren Sie den Cursor über dem ILM-Warteschlangendiagramm, um den Wert der folgenden Attribute zu einem bestimmten Zeitpunkt anzuzeigen:
   - **In die Warteschlange gestellte Objekte (aus Clientvorgängen)**: Die Gesamtzahl der Objekte, die aufgrund von Clientvorgängen (z. B. Aufnahme) auf eine ILM-Auswertung warten.
   - **In die Warteschlange gestellte Objekte (aus allen Vorgängen)**: Die Gesamtzahl der Objekte, die auf die ILM-Auswertung warten.
   - **Scanrate (Objekte/Sek.)**: Die Rate, mit der Objekte im Raster gescannt und für ILM in die Warteschlange gestellt werden.
   - **Auswertungsrate (Objekte/Sek.)**: Die aktuelle Rate, mit der Objekte im Grid anhand der ILM-Richtlinie ausgewertet werden.
4. Sehen Sie sich im Abschnitt „ILM-Warteschlange“ die folgenden Attribute an.

   Der ILM-Warteschlangenabschnitt ist nur für das Raster enthalten. Diese Informationen werden auf der ILM-Registerkarte für eine Site oder einen Speicherknoten nicht angezeigt.

   - **Scanzeitraum – geschätzt**: Die geschätzte Zeit, die zum Abschließen eines vollständigen ILM-Scans aller Objekte benötigt wird.

     Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde.

   - **Versuchte Reparaturen**: Die Gesamtzahl der Objektreparaturvorgänge für replizierte Daten, die versucht wurden. Dieser Zähler erhöht sich jedes Mal, wenn ein Speicherknoten versucht, ein Hochrisikoobjekt zu reparieren. Bei einer Netzüberlastung werden ILM-Reparaturen mit hohem Risiko priorisiert.

     Die gleiche Objektreparatur kann erneut inkrementiert werden, wenn die Replikation nach der Reparatur fehlgeschlagen ist.

   Diese Attribute können nützlich sein, wenn Sie den Fortschritt der Wiederherstellung des Storage Node-Volumes überwachen. Wenn die Anzahl der Reparaturversuche nicht mehr zunimmt und ein vollständiger Scan abgeschlossen wurde, ist die Reparatur wahrscheinlich abgeschlossen.

Überwachen Sie Netzwerk- und Systemressourcen

Die Integrität und Bandbreite des Netzwerks zwischen Knoten und Standorten sowie die Ressourcennutzung durch einzelne Grid-Knoten sind für einen effizienten Betrieb von entscheidender Bedeutung.

Überwachen Sie Netzwerkverbindungen und Leistung

Netzwerkkonnektivität und Bandbreite sind besonders wichtig, wenn Ihre ILM-Richtlinie (Information Lifecycle Management) replizierte Objekte zwischen Standorten kopiert oder löschcodierte Objekte mithilfe eines Schemas speichert, das Schutz vor Standortverlust bietet. Wenn das Netzwerk zwischen den Standorten nicht

verfügbar ist, die Netzwerklatenz zu hoch ist oder die Netzwerkbandbreite nicht ausreicht, können einige ILM-Regeln Objekte möglicherweise nicht an der erwarteten Stelle platzieren. Dies kann zu Aufnahmefehlern (wenn für ILM-Regeln die Option „Strenge Aufnahme“ ausgewählt ist) oder zu einer schlechten Aufnahmeleistung und ILM-Rückständen führen.

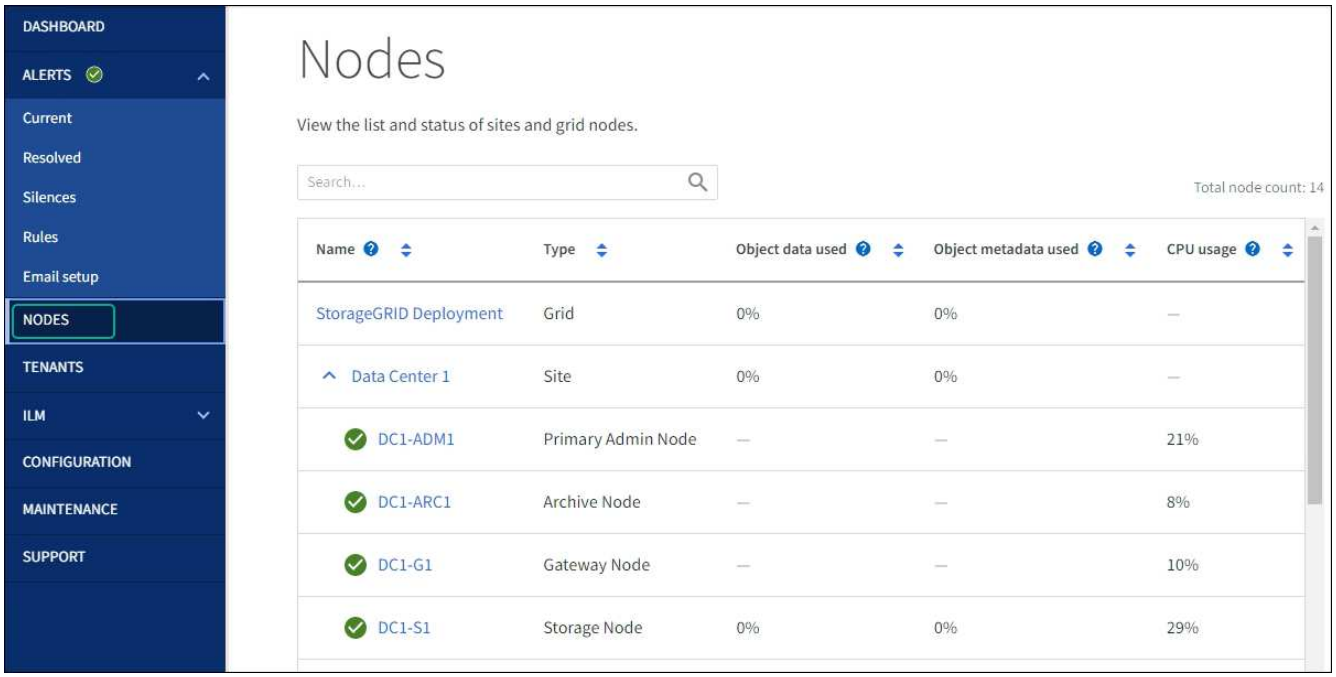
Verwenden Sie den Grid Manager, um die Konnektivität und Netzwerkleistung zu überwachen, damit Sie etwaige Probleme umgehend beheben können.

Darüber hinaus sollten Sie"Erstellen von Richtlinien zur Klassifizierung des Netzwerkverkehrs" damit Sie den Datenverkehr im Zusammenhang mit bestimmten Mandanten, Buckets, Subnetzen oder Load Balancer-Endpunkten überwachen können. Sie können bei Bedarf Richtlinien zur Verkehrsbeschränkung festlegen.

Schritte

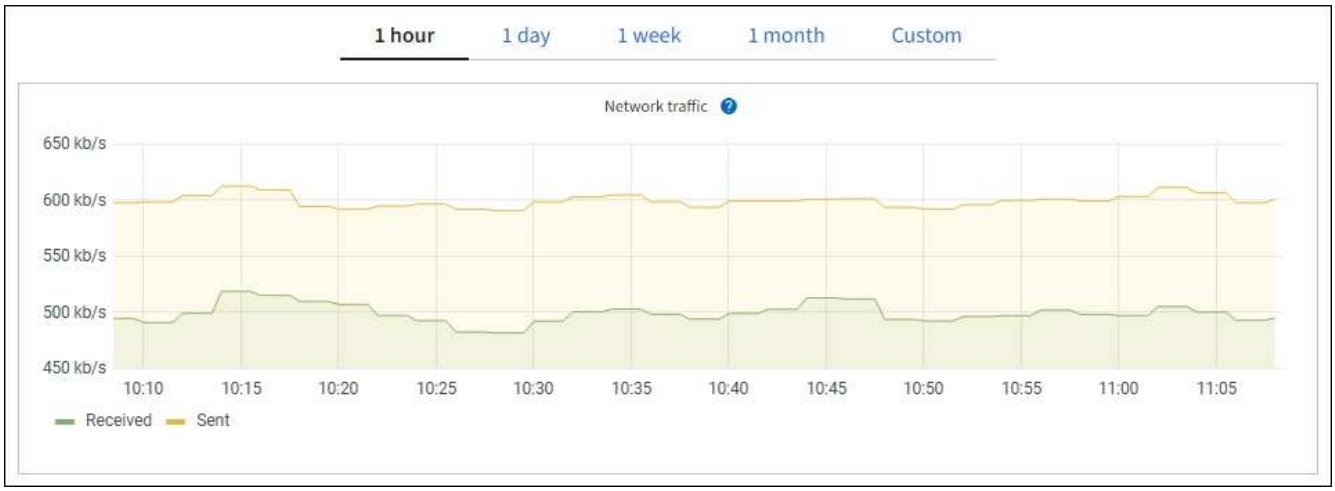
1. Wählen Sie **NODES**.

   Die Seite „Knoten“ wird angezeigt. Jeder Knoten im Raster wird im Tabellenformat aufgelistet.



2. Wählen Sie den Grid-Namen, einen bestimmten Rechenzentrumsstandort oder einen Grid-Knoten aus und wählen Sie dann die Registerkarte **Netzwerk**.

   Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs für das gesamte Grid, den Rechenzentrumsstandort oder den Knoten.



a. Wenn Sie einen Grid-Knoten ausgewählt haben, scrollen Sie nach unten, um den Abschnitt **Netzwerkschnittstellen** der Seite zu überprüfen.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

b. Scrollen Sie für Grid-Knoten nach unten, um den Abschnitt **Netzwerkkommunikation** der Seite zu lesen.

Die Empfangs- und Sendetabellen zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Sendemetriken.

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

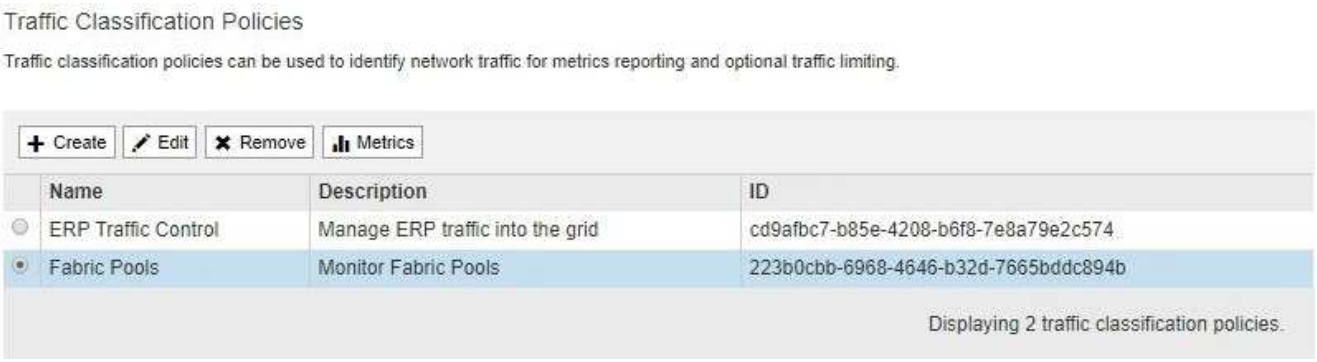
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

3. Verwenden Sie die mit Ihren Richtlinien zur Verkehrsklassifizierung verknüpften Metriken, um den Netzwerkverkehr zu überwachen.

a. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.

Die Seite „Richtlinien zur Verkehrsklassifizierung“ wird angezeigt und die vorhandenen Richtlinien werden in der Tabelle aufgelistet.



a. Um Diagramme anzuzeigen, die die mit einer Richtlinie verknüpften Netzwerkmetriken zeigen, wählen Sie das Optionsfeld links neben der Richtlinie aus und klicken Sie dann auf **Metriken**.

b. Sehen Sie sich die Diagramme an, um den mit der Richtlinie verbundenen Netzwerkverkehr zu verstehen.

   Wenn eine Datenverkehrsklassifizierungsrichtlinie darauf ausgelegt ist, den Netzwerkdatenverkehr zu begrenzen, analysieren Sie, wie oft der Datenverkehr begrenzt wird, und entscheiden Sie, ob die Richtlinie weiterhin Ihren Anforderungen entspricht. Von Zeit zu Zeit,"Passen Sie jede Verkehrsklassifizierungsrichtlinie nach Bedarf an" .

Ähnliche Informationen

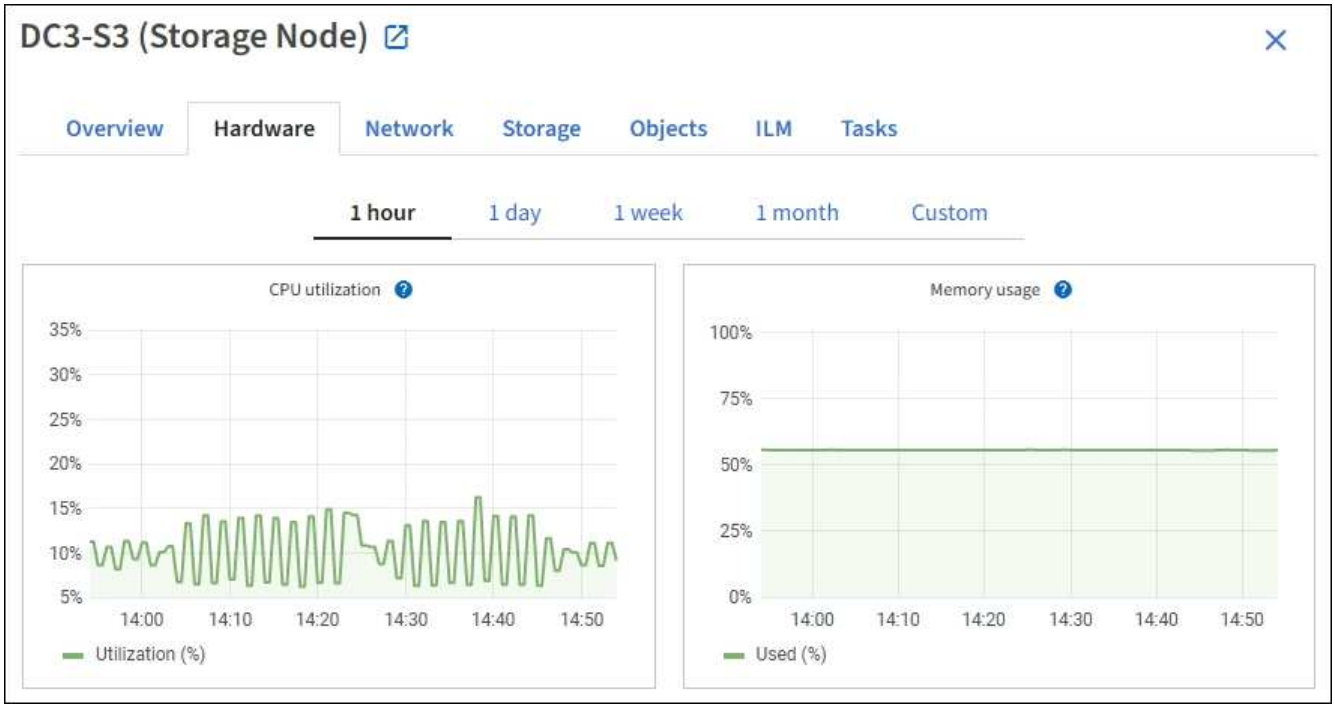
- "Anzeigen der Registerkarte „Netzwerk“"
- "Überwachen Sie den Verbindungsstatus des Knotens"

Überwachen von Ressourcen auf Knotenebene

Überwachen Sie einzelne Grid-Knoten, um deren Ressourcennutzungsgrade zu überprüfen. Wenn Knoten ständig überlastet sind, sind für einen effizienten Betrieb möglicherweise mehr Knoten erforderlich.

Schritte

1. Wählen Sie auf der Seite **NODES** den Knoten aus.
2. Wählen Sie die Registerkarte **Hardware**, um Diagramme zur CPU-Auslastung und Speichernutzung anzuzeigen.



3. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.
4. Wenn der Knoten auf einem Speichergerät oder einem Servicegerät gehostet wird, scrollen Sie nach unten, um die Komponententabellen anzuzeigen. Der Status aller Komponenten sollte „Nominal“ sein. Untersuchen Sie Komponenten mit einem anderen Status.

Ähnliche Informationen

- "Informationen zu Appliance-Speicherknoten anzeigen"
- "Informationen zu Appliance-Admin-Knoten und Gateway-Knoten anzeigen"

Überwachen Sie die Mieteraktivität

Alle S3-Client-Aktivitäten sind mit StorageGRID Mandantenkonten verknüpft. Mit dem Grid Manager können Sie die Speichernutzung oder den Netzwerkverkehr für alle oder einen bestimmten Mandanten überwachen. Sie können das Prüfprotokoll oder die Grafana-Dashboards verwenden, um detailliertere Informationen darüber zu sammeln, wie Mieter StorageGRID verwenden.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriff oder Mandantenkontenberechtigung" .

Alle Mieter anzeigen

Auf der Seite „Mieter“ werden grundlegende Informationen zu allen aktuellen Mieterkonten angezeigt.

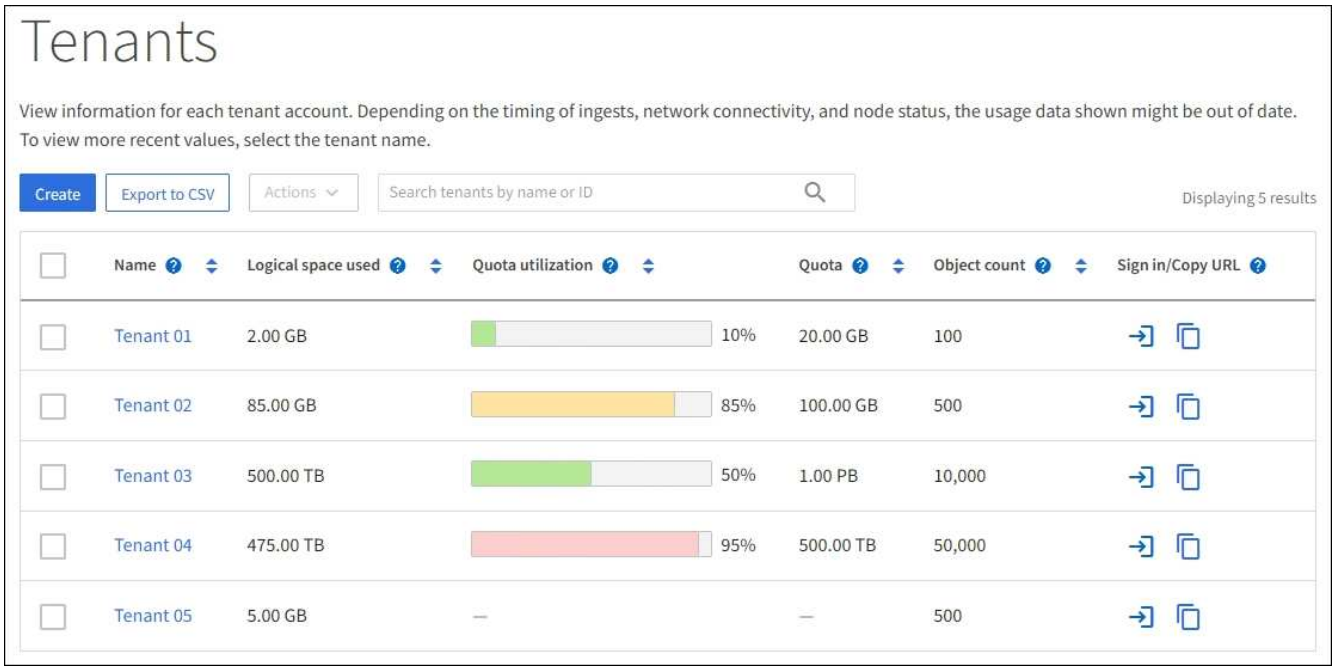
Schritte

1. Wählen Sie **MIETER** aus.

2. Überprüfen Sie die auf den Mieterseiten angezeigten Informationen.

   Für jeden Mandanten werden der verwendete logische Speicherplatz, die Kontingentnutzung, das Kontingent und die Objektanzahl aufgelistet. Wenn für einen Mandanten kein Kontingent festgelegt ist, enthalten die Felder „Kontingentnutzung“ und „Kontingent“ einen Bindestrich (—).

   > Bei den Angaben zum belegten Speicherplatz handelt es sich um Schätzwerte. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst.



3. Optional können Sie sich bei einem Mandantenkonto anmelden, indem Sie den Anmeldelink auswählen. in der Spalte * Sign in/ URL kopieren *.
4. Kopieren Sie optional die URL für die Anmeldeseite eines Mandanten, indem Sie den Link „URL kopieren“ auswählen. in der Spalte * Sign in/ URL kopieren *.
5. Wählen Sie optional **Exportieren nach CSV**, um eine `.csv` Datei mit den Nutzungswerten für alle Mandanten.

   Sie werden aufgefordert, die `.csv` Datei.

   Der Inhalt der `.csv` Die Datei sieht wie im folgenden Beispiel aus:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

   Sie können das `.csv` Datei in einer Tabellenkalkulationsanwendung oder verwenden Sie sie in der Automatisierung.

6. Wenn keine Objekte aufgelistet sind, wählen Sie optional **Aktionen** > **Löschen** aus, um einen oder mehrere Mandanten zu entfernen. Sehen "Mieterkonto löschen" .

Sie können ein Mandantenkonto nicht entfernen, wenn das Konto Buckets oder Container enthält.

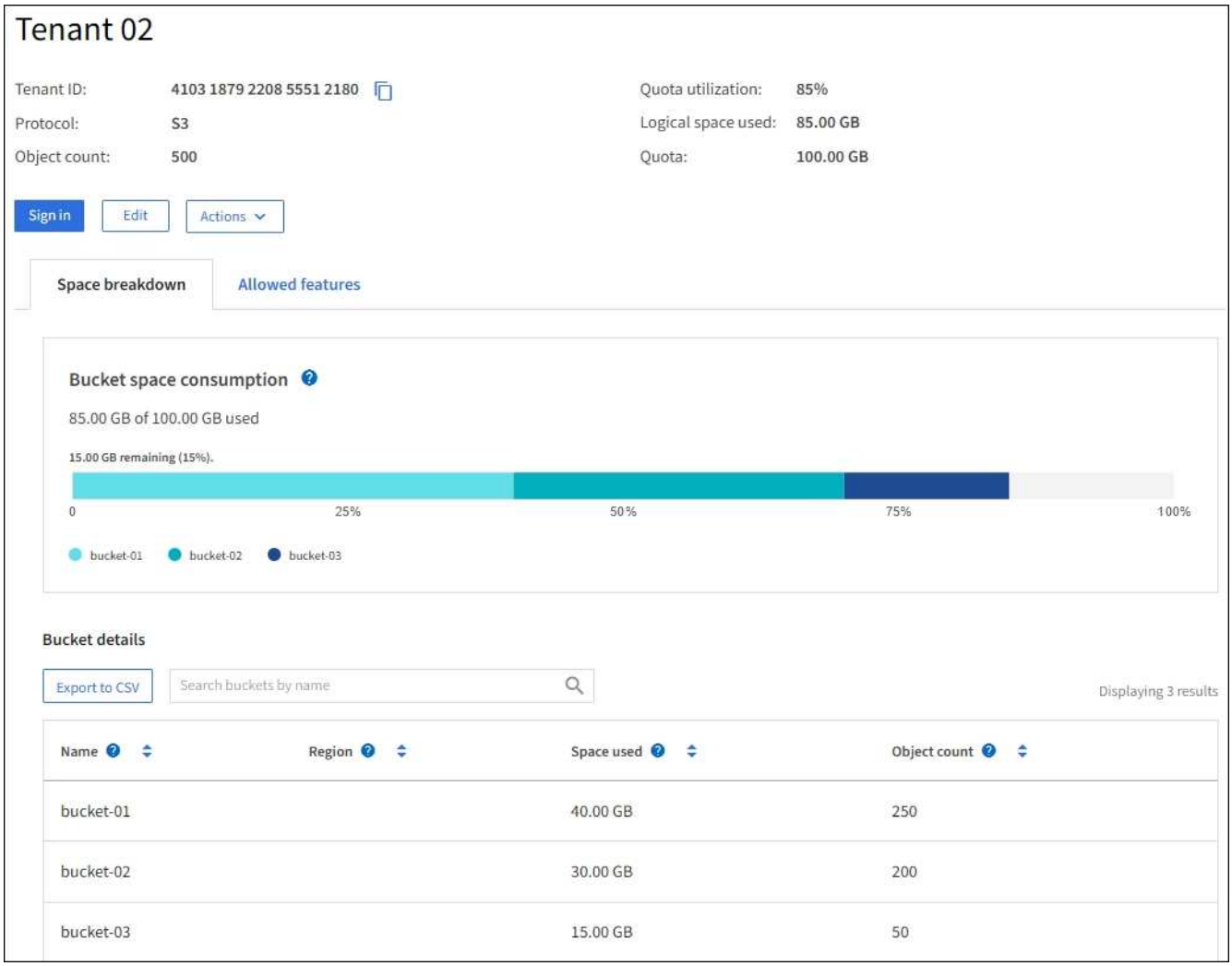
Einen bestimmten Mandanten anzeigen

Sie können Details zu einem bestimmten Mieter anzeigen.

Schritte

1. Wählen Sie den Mandantennamen auf der Seite „Mandanten“ aus.

   Die Seite mit den Mieterdetails wird angezeigt.



2. Sehen Sie sich die Mieterübersicht oben auf der Seite an.

   Dieser Abschnitt der Detailseite enthält zusammenfassende Informationen zum Mandanten, darunter die Objektanzahl des Mandanten, die Kontingentnutzung, den verwendeten logischen Speicherplatz und die Kontingenteinstellung.

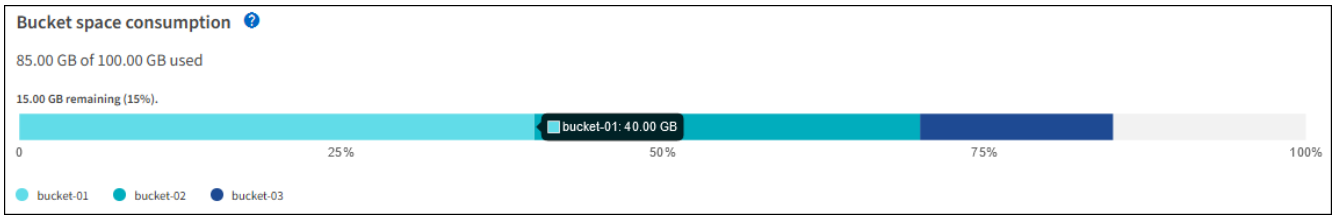
3. Überprüfen Sie auf der Registerkarte **Speicherplatzaufschlüsselung** das Diagramm **Speicherplatzverbrauch**.

   Dieses Diagramm zeigt den gesamten Speicherplatzverbrauch für alle S3-Buckets des Mandanten.

   Wenn für diesen Mandanten ein Kontingent festgelegt wurde, wird die Menge des verwendeten und

verbleibenden Kontingents als Text angezeigt (z. B. `85.00 GB of 100 GB used`). Wenn kein Kontingent festgelegt wurde, verfügt der Mandant über ein unbegrenztes Kontingent und der Text enthält nur die Menge des verwendeten Speicherplatzes (z. B. `85.00 GB used`). Das Balkendiagramm zeigt den Prozentsatz der Quote in jedem Bucket oder Container. Wenn der Mandant das Speicherkontingent um mehr als 1 % und mindestens 1 GB überschritten hat, zeigt das Diagramm das Gesamtkontingent und den Überschussbetrag an.

Sie können den Cursor über das Balkendiagramm bewegen, um den von jedem Bucket oder Container verwendeten Speicherplatz anzuzeigen. Sie können den Cursor über das Segment „Freier Speicherplatz“ bewegen, um die verbleibende Speicherquote anzuzeigen.



> Die Kontingentnutzung basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. Beispielsweise überprüft StorageGRID das Kontingent, wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen ab, wenn der Mandant das Kontingent überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kontingent überschritten wurde. Wenn Objekte gelöscht werden, kann es sein, dass ein Mandant vorübergehend daran gehindert wird, neue Objekte hochzuladen, bis die Kontingentnutzung neu berechnet wird. Die Berechnung der Kontingentnutzung kann 10 Minuten oder länger dauern.

> Die Kontingentnutzung eines Mandanten gibt die Gesamtmenge der Objektdaten an, die der Mandant in StorageGRID hochgeladen hat (logische Größe). Die Kontingentnutzung stellt nicht den Speicherplatz dar, der zum Speichern von Kopien dieser Objekte und ihrer Metadaten (physische Größe) verwendet wird.

> Sie können die Warnregel „Hohe Kontingentnutzung des Mandanten“ aktivieren, um festzustellen, ob Mandanten ihre Kontingente verbrauchen. Wenn diese Option aktiviert ist, wird diese Warnung ausgelöst, wenn ein Mandant 90 % seines Kontingents genutzt hat. Anweisungen hierzu finden Sie unter"Alarmregeln bearbeiten" .

4. Überprüfen Sie auf der Registerkarte **Speicherplatzaufschlüsselung** die **Bucket-Details**.

   Diese Tabelle listet die S3-Buckets für den Mandanten auf. Der verwendete Speicherplatz ist die Gesamtmenge der Objektdaten im Bucket oder Container. Dieser Wert stellt nicht den für ILM-Kopien und Objektmetadaten erforderlichen Speicherplatz dar.

5. Wählen Sie optional **In CSV exportieren** aus, um eine CSV-Datei mit den Nutzungswerten für jeden Bucket oder Container anzuzeigen und zu exportieren.

   Der Inhalt eines einzelnen S3-Tenants `.csv` Die Datei sieht wie im folgenden Beispiel aus:

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

Sie können das `.csv` Datei in einer Tabellenkalkulationsanwendung oder verwenden Sie sie in der Automatisierung.

6. Wählen Sie optional die Registerkarte **Zugelassene Funktionen** aus, um eine Liste der Berechtigungen und Funktionen anzuzeigen, die für den Mandanten aktiviert sind. Sehen"Mieterkonto bearbeiten" wenn Sie eine dieser Einstellungen ändern müssen.
7. Wenn der Mandant über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, wählen Sie optional die Registerkarte **Grid-Föderation** aus, um mehr über die Verbindung zu erfahren.

   Sehen"Was ist Grid-Föderation?" Und"Verwalten der zulässigen Mandanten für die Grid-Föderation" .

Netzwerkverkehr anzeigen

Wenn für einen Mandanten Richtlinien zur Verkehrsklassifizierung gelten, überprüfen Sie den Netzwerkverkehr für diesen Mandanten.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.

   Die Seite „Richtlinien zur Verkehrsklassifizierung“ wird angezeigt und die vorhandenen Richtlinien werden in der Tabelle aufgelistet.

2. Überprüfen Sie die Liste der Richtlinien, um diejenigen zu ermitteln, die für einen bestimmten Mieter gelten.
3. Um die mit einer Richtlinie verknüpften Metriken anzuzeigen, wählen Sie das Optionsfeld links neben der Richtlinie aus und wählen Sie **Metriken**.
4. Analysieren Sie die Diagramme, um festzustellen, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

Sehen "Verwalten von Richtlinien zur Datenverkehrsklassifizierung" für weitere Informationen.

Verwenden des Überwachungsprotokolls

Optional können Sie das Überwachungsprotokoll für eine detailliertere Überwachung der Aktivitäten eines Mandanten verwenden.

Sie können beispielsweise die folgenden Arten von Informationen überwachen:

- Bestimmte Clientvorgänge, wie z. B. PUT, GET oder DELETE
- Objektgrößen
- Die ILM-Regel für Objekte
- Die Quell-IP der Client-Anfragen

Prüfprotokolle werden in Textdateien geschrieben, die Sie mit einem Protokollanalysetool Ihrer Wahl analysieren können. Dadurch können Sie die Aktivitäten Ihrer Kunden besser nachvollziehen oder ausgefeilte Chargeback- und Abrechnungsmodelle implementieren.

Sehen "Überprüfen der Überwachungsprotokolle" für weitere Informationen.

Verwenden Sie Prometheus-Metriken

Verwenden Sie optional Prometheus-Metriken, um Berichte zur Mieteraktivität zu erstellen.

- Wählen Sie im Grid Manager **SUPPORT** > **Tools** > **Metriken**. Sie können vorhandene Dashboards wie S3 Overview verwenden, um Clientaktivitäten zu überprüfen.

> Die auf der Seite „Metriken“ verfügbaren Tools sind in erster Linie für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig.

- Wählen Sie oben im Grid Manager das Hilfesymbol und dann **API-Dokumentation** aus. Sie können die Metriken im Abschnitt „Metriken“ der Grid Management-API verwenden, um benutzerdefinierte Warnregeln und Dashboards für die Mieteraktivität zu erstellen.

Sehen "Überprüfen der Supportmetriken" für weitere Informationen.

Überwachen Sie S3-Clientvorgänge

Sie können die Aufnahme- und Abrufraten von Objekten sowie Metriken für Objektanzahl, Abfragen und Überprüfung überwachen. Sie können die Anzahl der erfolgreichen und fehlgeschlagenen Versuche von Clientanwendungen anzeigen, Objekte im StorageGRID -System zu lesen, zu schreiben und zu ändern.

Bevor Sie beginnen

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

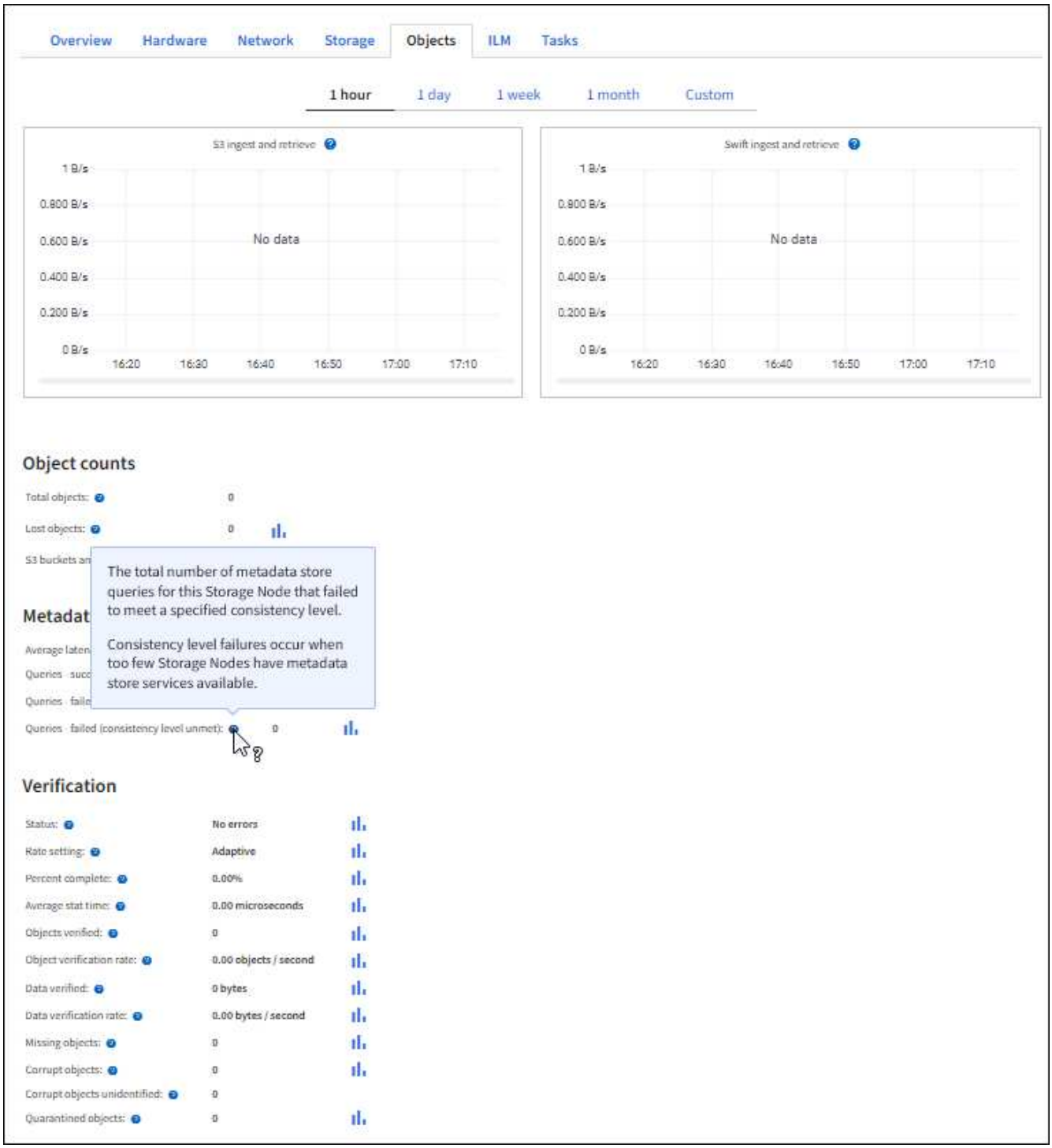
Schritte

1. Wählen Sie im Dashboard die Registerkarte **Leistung** aus.
2. Sehen Sie sich die S3-Diagramme an, die die Anzahl der von Speicherknoten ausgeführten Clientvorgänge und die Anzahl der von Speicherknoten empfangenen API-Anfragen während des ausgewählten Zeitraums zusammenfassen.
3. Wählen Sie **NODES**, um auf die Knotenseite zuzugreifen.
4. Wählen Sie auf der Nodes-Startseite (Rasterebene) die Registerkarte **Objekte** aus.

   Das Diagramm zeigt die S3-Aufnahme- und Abrufraten für Ihr gesamtes StorageGRID System in Bytes pro Sekunde und die Menge der aufgenommenen oder abgerufenen Daten. Sie können ein Zeitintervall auswählen oder ein benutzerdefiniertes Intervall anwenden.

5. Um Informationen zu einem bestimmten Speicherknoten anzuzeigen, wählen Sie den Knoten aus der Liste links aus und wählen Sie die Registerkarte **Objekte**.

   Das Diagramm zeigt die Aufnahme- und Abrufraten für den Knoten. Die Registerkarte enthält auch Metriken für Objektzählungen, Metadatenabfragen und Überprüfungsvorgänge.



Überwachen von Lastausgleichsvorgängen

Wenn Sie einen Load Balancer zum Verwalten von Clientverbindungen zu StorageGRID verwenden, sollten Sie die Load Balancing-Vorgänge überwachen, nachdem Sie das System zum ersten Mal konfiguriert haben und nachdem Sie Konfigurationsänderungen vorgenommen oder eine Erweiterung durchgeführt haben.

Informationen zu diesem Vorgang

Sie können den Load Balancer-Dienst auf Admin-Knoten oder Gateway-Knoten oder einen externen Load Balancer eines Drittanbieters verwenden, um Clientanforderungen auf mehrere Speicherknoten zu verteilen.

Nachdem Sie den Lastenausgleich konfiguriert haben, sollten Sie sicherstellen, dass die Vorgänge zum Aufnehmen und Abrufen von Objekten gleichmäßig auf die Speicherknoten verteilt werden. Durch gleichmäßig verteilte Anfragen wird sichergestellt, dass StorageGRID auch unter Last auf Clientanfragen reagiert und zur Aufrechterhaltung der Clientleistung beitragen kann.

Wenn Sie eine Hochverfügbarkeitsgruppe (HA) aus Gateway-Knoten oder Admin-Knoten im Active-Backup-Modus konfiguriert haben, verteilt nur ein Knoten in der Gruppe aktiv Client-Anfragen.

Weitere Informationen finden Sie unter "Konfigurieren von S3-Clientverbindungen" .

Schritte

1. Wenn S3-Clients über den Load Balancer-Dienst eine Verbindung herstellen, überprüfen Sie, ob Admin-Knoten oder Gateway-Knoten den Datenverkehr wie erwartet aktiv verteilen:
   a. Wählen Sie **NODES**.
   b. Wählen Sie einen Gateway-Knoten oder Admin-Knoten aus.
   c. Überprüfen Sie auf der Registerkarte **Übersicht**, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle „Primär“ hat.

      Knoten mit der Rolle „Primär“ und Knoten, die nicht zu einer HA-Gruppe gehören, sollten Anfragen aktiv an Clients verteilen.

   d. Wählen Sie für jeden Knoten, der aktiv Client-Anfragen verteilen soll, die Option"Registerkarte „Load Balancer“" .
   e. Überprüfen Sie das Diagramm des Load Balancer-Anforderungsverkehrs der letzten Woche, um sicherzustellen, dass der Knoten aktiv Anforderungen verteilt hat.

      Knoten in einer Active-Backup-HA-Gruppe können von Zeit zu Zeit die Backup-Rolle übernehmen. Während dieser Zeit verteilen die Knoten keine Clientanforderungen.

   f. Überprüfen Sie das Diagramm der eingehenden Anforderungsrate des Load Balancers für die letzte Woche, um den Objektdurchsatz des Knotens zu überprüfen.
   g. Wiederholen Sie diese Schritte für jeden Admin-Knoten oder Gateway-Knoten im StorageGRID System.
   h. Verwenden Sie optional Richtlinien zur Verkehrsklassifizierung, um eine detailliertere Analyse des vom Load Balancer-Dienst bereitgestellten Verkehrs anzuzeigen.
2. Stellen Sie sicher, dass diese Anfragen gleichmäßig auf die Speicherknoten verteilt werden.
   a. Wählen Sie ***Speicherknoten*** > **LDR** > **HTTP**.
   b. Überprüfen Sie die Anzahl der **derzeit eingerichteten eingehenden Sitzungen**.
   c. Wiederholen Sie dies für jeden Speicherknoten im Raster.

      Die Anzahl der Sitzungen sollte auf allen Speicherknoten ungefähr gleich sein.

Überwachen von Grid-Föderation-Verbindungen

Sie können grundlegende Informationen zu allen"Grid-Föderation-Verbindungen" , detaillierte Informationen zu einer bestimmten Verbindung oder Prometheus-Metriken zu Cross-Grid-Replikationsvorgängen. Sie können eine Verbindung von beiden Rastern aus überwachen.

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.

Alle Verbindungen anzeigen

Auf der Seite „Grid-Föderation“ werden grundlegende Informationen zu allen Grid-Föderationsverbindungen und zu allen Mandantenkonten angezeigt, die Grid-Föderationsverbindungen verwenden dürfen.

Schritte

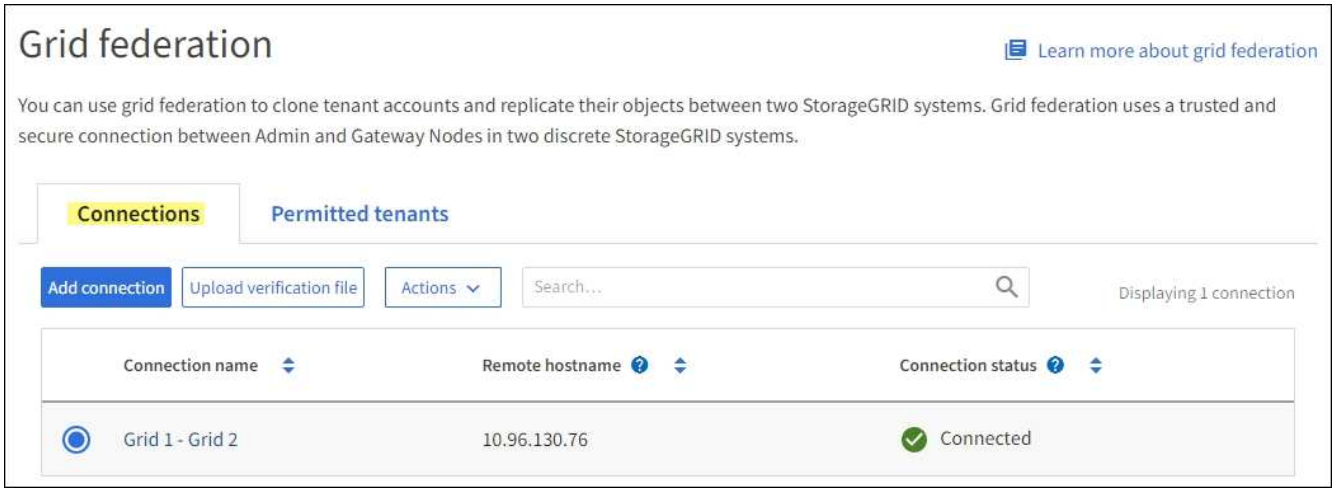
1. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.

   Die Seite „Grid-Föderation“ wird angezeigt.

2. Um grundlegende Informationen zu allen Verbindungen in diesem Raster anzuzeigen, wählen Sie die Registerkarte **Verbindungen**.

   Auf dieser Registerkarte können Sie:

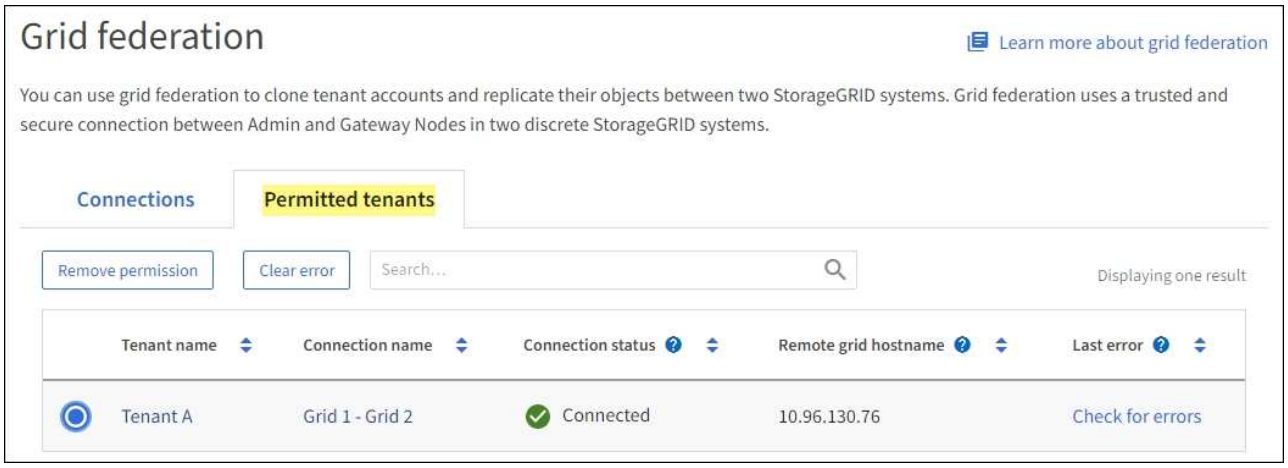
   - "Erstellen einer neuen Verbindung" .
   - Wählen Sie eine bestehende Verbindung aus, um"bearbeiten oder testen" .



3. Um grundlegende Informationen zu allen Mandantenkonten in diesem Raster anzuzeigen, die über die Berechtigung **Rasterföderationsverbindung verwenden** verfügen, wählen Sie die Registerkarte **Zugelassene Mandanten** aus.

   Auf dieser Registerkarte können Sie:

   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an" .
   - Zeigen Sie die Detailseite für jede Verbindung an. Sehen Anzeigen einer bestimmten Verbindung .
   - Wählen Sie einen zulässigen Mieter aus und"die Berechtigung entfernen" .
   - Suchen Sie nach Cross-Grid-Replikationsfehlern und beheben Sie gegebenenfalls den letzten Fehler. Sehen "Beheben von Grid-Föderationsfehlern" .



Eine bestimmte Verbindung anzeigen

Sie können Details zu einer bestimmten Grid-Föderation-Verbindung anzeigen.

Schritte

1. Wählen Sie auf der Grid-Föderationsseite eine der Registerkarten aus und wählen Sie dann den Verbindungsnamen aus der Tabelle aus.

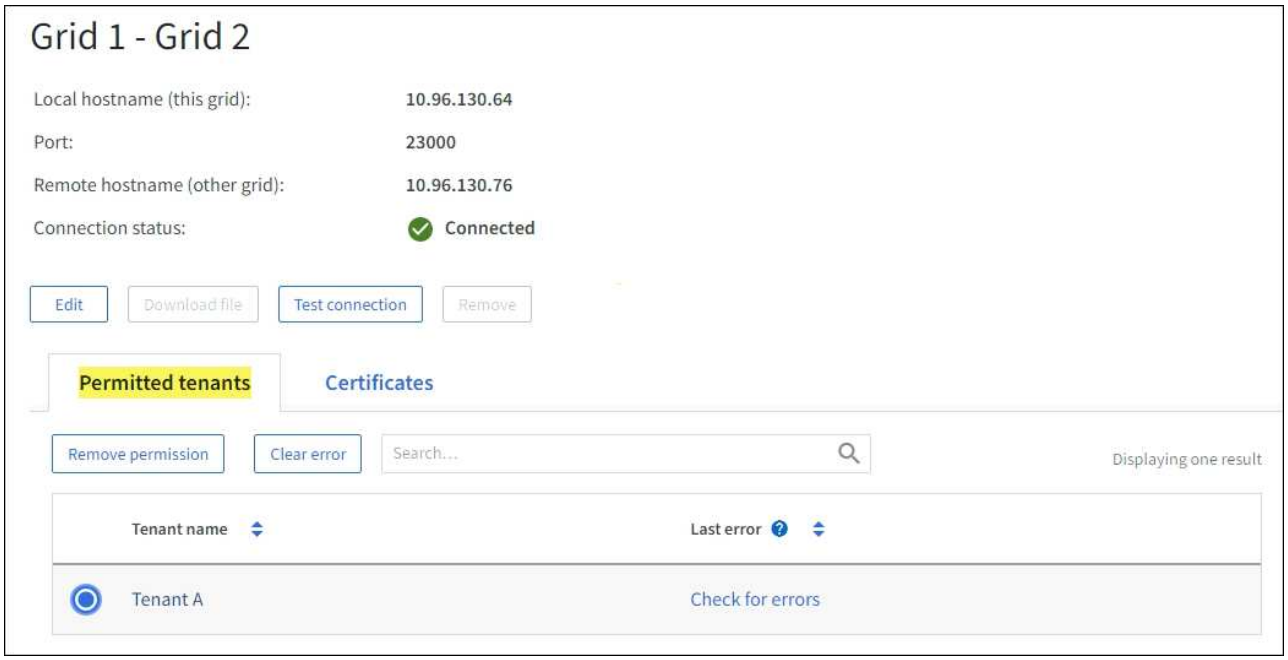
   Auf der Detailseite der Verbindung können Sie:

   - Sehen Sie sich grundlegende Statusinformationen zur Verbindung an, einschließlich der lokalen und Remote-Hostnamen, des Ports und des Verbindungsstatus.
   - Wählen Sie eine Verbindung zu"bearbeiten, testen oder entfernen" .

2. Wählen Sie beim Anzeigen einer bestimmten Verbindung die Registerkarte **Zulässige Mandanten** aus, um Details zu den zulässigen Mandanten für die Verbindung anzuzeigen.

   Auf dieser Registerkarte können Sie:

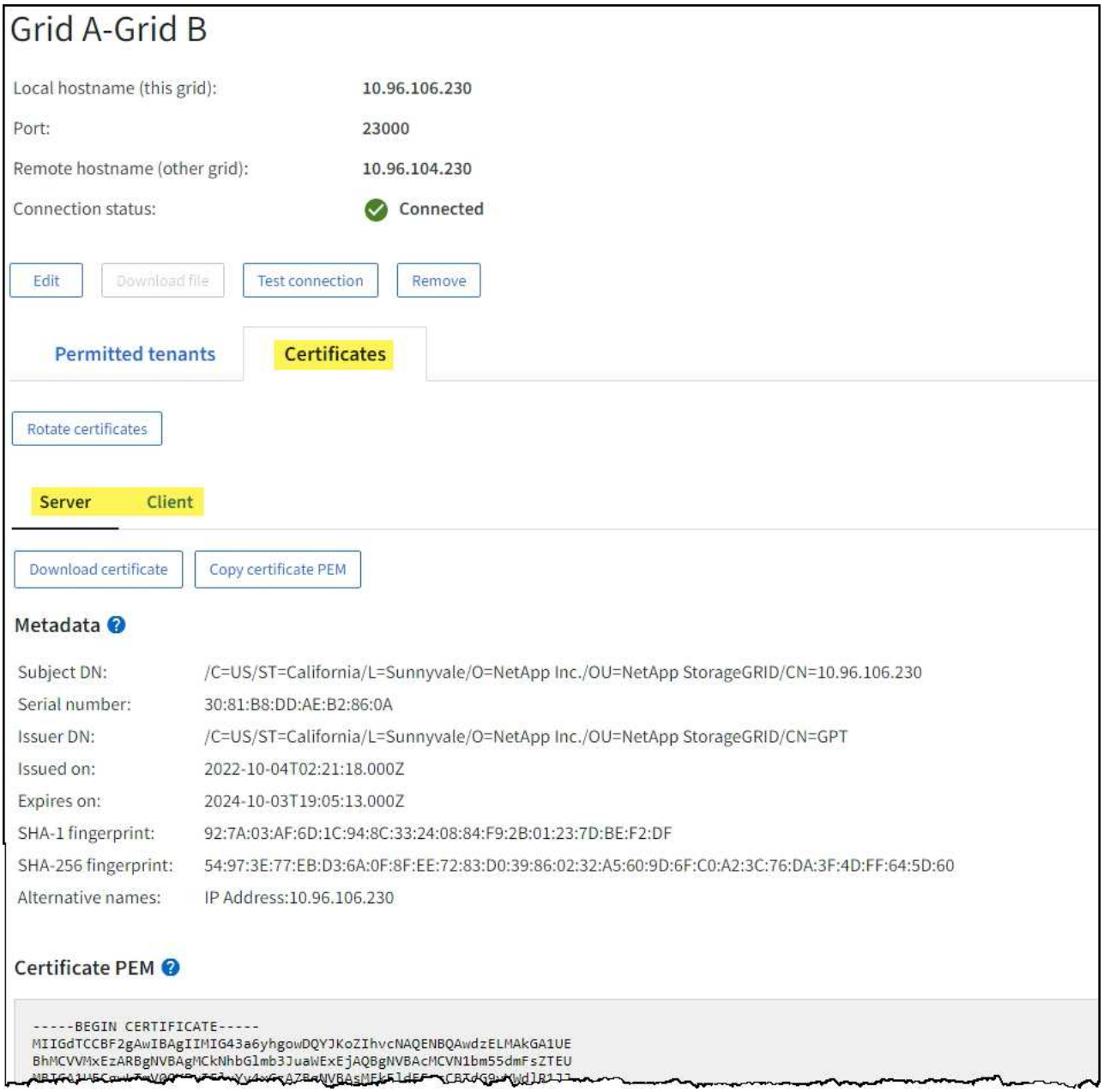
   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an" .
   - "Entfernen der Berechtigung eines Mandanten"um die Verbindung zu nutzen.
   - Suchen Sie nach Cross-Grid-Replikationsfehlern und beheben Sie den letzten Fehler. Sehen "Beheben von Grid-Föderationsfehlern" .



3. Wählen Sie beim Anzeigen einer bestimmten Verbindung die Registerkarte **Zertifikate** aus, um die vom System generierten Server- und Client-Zertifikate für diese Verbindung anzuzeigen.

   Auf dieser Registerkarte können Sie:

   - "Verbindungszertifikate rotieren" .
   - Wählen Sie **Server** oder **Client**, um das zugehörige Zertifikat anzuzeigen oder herunterzuladen oder das Zertifikat PEM zu kopieren.



Überprüfen der Cross-Grid-Replikationsmetriken

Sie können das Cross-Grid-Replication-Dashboard in Grafana verwenden, um Prometheus-Metriken zu Cross-Grid-Replikationsvorgängen in Ihrem Grid anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **SUPPORT** > **Tools** > **Metriken**.

   Die auf der Seite „Metriken“ verfügbaren Tools sind für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe die Liste der"häufig verwendete Prometheus-Metriken" .

2. Wählen Sie im Abschnitt „Grafana“ der Seite **Cross Grid Replication** aus.

   Ausführliche Anweisungen finden Sie unter"Überprüfen der Supportmetriken" .

3. Um die Replikation von Objekten, deren Replikation fehlgeschlagen ist, erneut zu versuchen, siehe"Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge" .

Verwalten von Warnungen

Verwalten von Warnungen

Das Warnsystem bietet eine benutzerfreundliche Schnittstelle zum Erkennen, Bewerten und Beheben von Problemen, die während des StorageGRID -Betriebs auftreten können.

Warnungen werden bei bestimmten Schweregraden ausgelöst, wenn die Bedingungen der Warnungsregel als wahr ausgewertet werden. Wenn eine Warnung ausgelöst wird, werden die folgenden Aktionen ausgeführt:

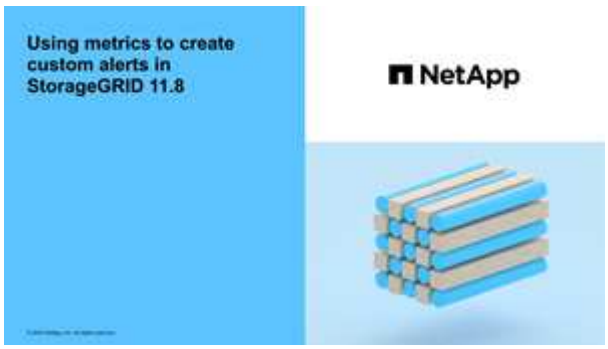
- Auf dem Dashboard im Grid Manager wird ein Symbol für den Schweregrad der Warnung angezeigt und die Anzahl der aktuellen Warnungen wird erhöht.
- Die Warnung wird auf der Übersichtsseite **NODES** und auf der Registerkarte **NODES** > ***node*** > **Übersicht** angezeigt.
- Vorausgesetzt, Sie haben einen SMTP-Server konfiguriert und E-Mail-Adressen für die Empfänger angegeben, wird eine E-Mail-Benachrichtigung gesendet.
- Vorausgesetzt, Sie haben den StorageGRID SNMP-Agenten konfiguriert, wird eine SNMP-Benachrichtigung (Simple Network Management Protocol) gesendet.

Sie können benutzerdefinierte Warnungen erstellen, Warnungen bearbeiten oder deaktivieren und Warnbenachrichtigungen verwalten.

Weitere Informationen:

- Sehen Sie sich das Video an: "Video: Übersicht über Warnungen"

- Sehen Sie sich das Video an: "Video: Benutzerdefinierte Benachrichtigungen"



- Siehe die"Warnungsreferenz" .

Anzeigen von Warnregeln

Warnregeln definieren die Bedingungen, die auslösen"spezifische Warnungen" . StorageGRID enthält eine Reihe von Standard-Alarmregeln, die Sie unverändert verwenden oder ändern können, oder Sie können benutzerdefinierte Alarmregeln erstellen.

Sie können die Liste aller standardmäßigen und benutzerdefinierten Warnregeln anzeigen, um zu erfahren, welche Bedingungen die einzelnen Warnmeldungen auslösen und um zu sehen, ob Warnmeldungen deaktiviert sind.

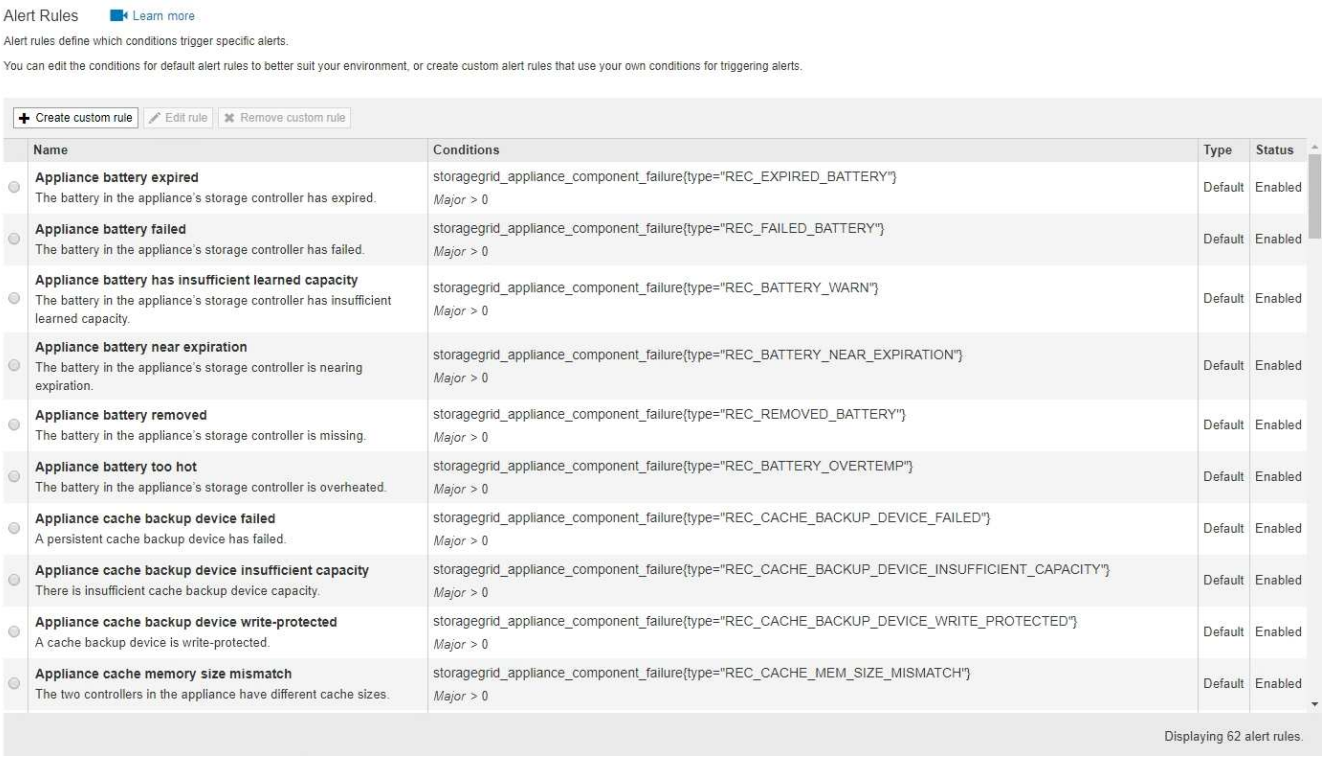
Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .
- Optional haben Sie das Video angesehen: "Video: Übersicht über Warnungen"

Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.



2. Überprüfen Sie die Informationen in der Tabelle mit den Warnregeln:

Spaltenüberschrift	Beschreibung
Name	Der eindeutige Name und die Beschreibung der Warnregel. Benutzerdefinierte Warnregeln werden zuerst aufgeführt, gefolgt von Standardwarnregeln. Der Name der Warnregel ist der Betreff für E-Mail-Benachrichtigungen.

Spaltenüberschrift	Beschreibung
Bedingungen	Die Prometheus-Ausdrücke, die bestimmen, wann dieser Alarm ausgelöst wird. Ein Alarm kann bei einem oder mehreren der folgenden Schweregrade ausgelöst werden, es ist jedoch nicht für jeden Schweregrad eine Bedingung erforderlich. • *Kritisch* : Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort angehen. Wenn das Problem nicht behoben wird, kann es zu Dienstunterbrechungen und Datenverlust kommen. • *Wesentlich* : Es liegt ein anormaler Zustand vor, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten wichtige Warnungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder -Dienstes nicht stoppt. • *Unerheblich* : Das System funktioniert normal, es liegt jedoch ein anormaler Zustand vor, der die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn er anhält. Sie sollten kleinere Warnungen, die nicht von selbst verschwinden, überwachen und beheben, um sicherzustellen, dass sie nicht zu einem ernsteren Problem führen.
Typ	Der Typ der Warnregel: • **Standard**: Eine mit dem System bereitgestellte Warnregel. Sie können eine Standardwarnregel deaktivieren oder die Bedingungen und die Dauer einer Standardwarnregel bearbeiten. Sie können eine Standardwarnregel nicht entfernen. • **Standard***: Eine Standardwarnregel, die eine bearbeitete Bedingung oder Dauer enthält. Bei Bedarf können Sie einen geänderten Zustand problemlos wieder auf den ursprünglichen Standard zurücksetzen. • **Benutzerdefiniert**: Eine von Ihnen erstellte Warnregel. Sie können benutzerdefinierte Warnregeln deaktivieren, bearbeiten und entfernen.
Status	Ob diese Warnregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnregeln werden nicht ausgewertet, daher werden keine Warnmeldungen ausgelöst.

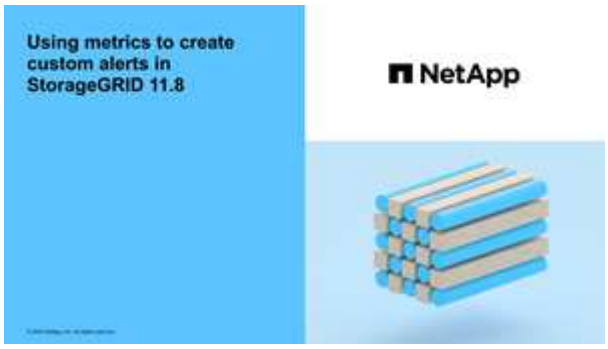
Erstellen Sie benutzerdefinierte Warnregeln

Sie können benutzerdefinierte Warnregeln erstellen, um Ihre eigenen Bedingungen zum Auslösen von Warnmeldungen festzulegen.

Bevor Sie beginnen

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

- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .
- Sie kennen die"häufig verwendete Prometheus-Metriken" .
- Sie verstehen die "Syntax von Prometheus-Abfragen" .
- Optional haben Sie das Video angesehen: "Video: Benutzerdefinierte Benachrichtigungen" .



Informationen zu diesem Vorgang

StorageGRID validiert keine benutzerdefinierten Warnungen. Wenn Sie benutzerdefinierte Warnregeln erstellen möchten, befolgen Sie diese allgemeinen Richtlinien:

- Sehen Sie sich die Bedingungen für die Standardwarnregeln an und verwenden Sie sie als Beispiele für Ihre benutzerdefinierten Warnregeln.
- Wenn Sie mehr als eine Bedingung für eine Warnregel definieren, verwenden Sie für alle Bedingungen denselben Ausdruck. Ändern Sie dann den Schwellenwert für jede Bedingung.
- Überprüfen Sie jede Bedingung sorgfältig auf Tipp- und Logikfehler.
- Verwenden Sie nur die in der Grid Management API aufgeführten Metriken.
- Beachten Sie beim Testen eines Ausdrucks mithilfe der Grid Management API, dass eine „erfolgreiche“ Antwort ein leerer Antworttext sein kann (keine Warnung ausgelöst). Um zu sehen, ob der Alarm tatsächlich ausgelöst wird, können Sie vorübergehend einen Schwellenwert auf einen Wert festlegen, von dem Sie derzeit erwarten, dass er zutrifft.

  Um beispielsweise den Ausdruck zu testen `node_memory_MemTotal_bytes < 24000000000` , führen Sie zuerst `node_memory_MemTotal_bytes >= 0` und stellen Sie sicher, dass Sie die erwarteten Ergebnisse erhalten (alle Knoten geben einen Wert zurück). Ändern Sie dann den Operator und den Schwellenwert wieder auf die beabsichtigten Werte und führen Sie die Ausführung erneut aus. Keine Ergebnisse zeigen an, dass für diesen Ausdruck keine aktuellen Warnungen vorliegen.

- Gehen Sie nicht davon aus, dass eine benutzerdefinierte Warnung funktioniert, es sei denn, Sie haben überprüft, dass die Warnung zum erwarteten Zeitpunkt ausgelöst wird.

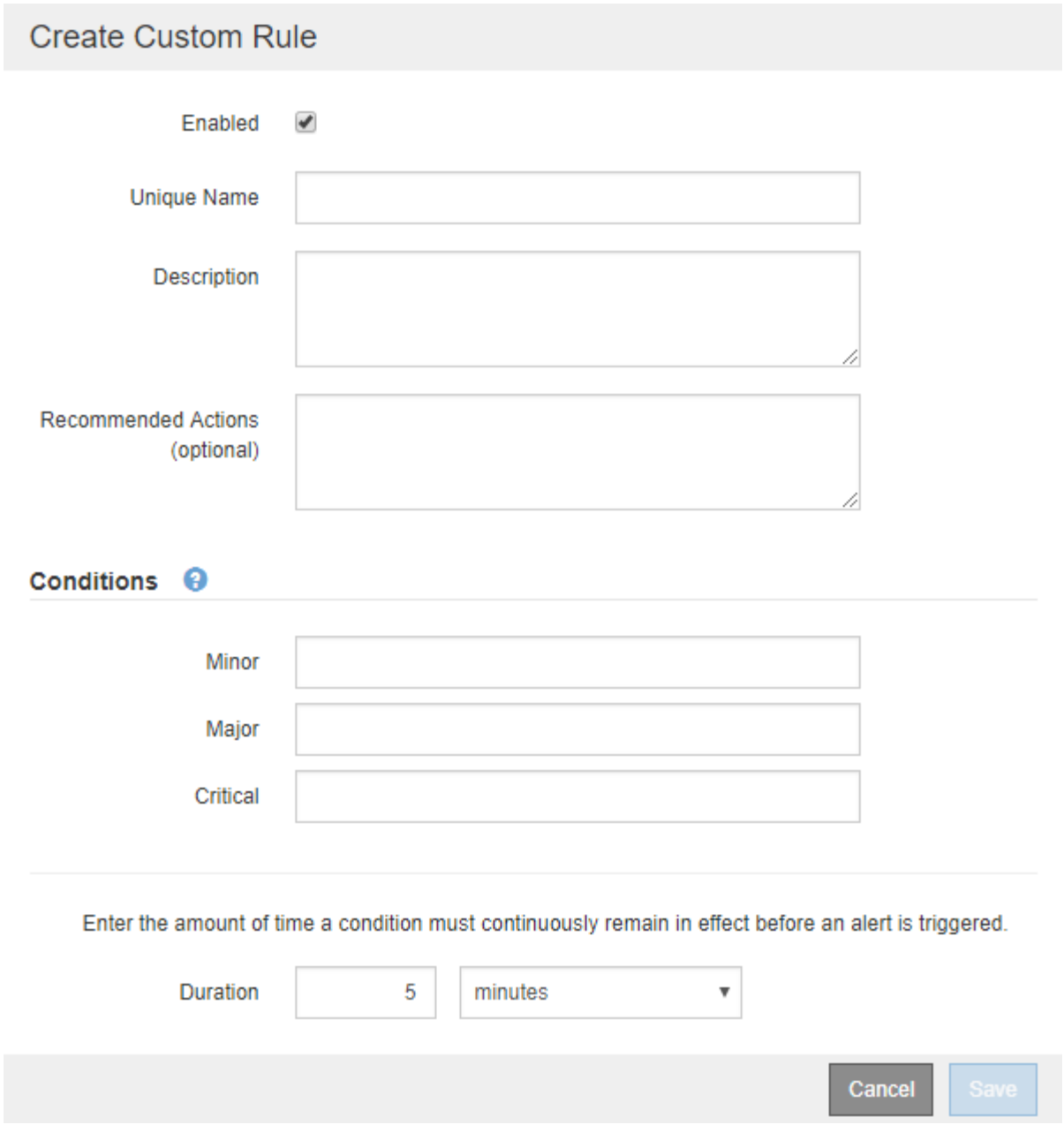
Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie **Benutzerdefinierte Regel erstellen**.

   Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.



3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktiviert**, um festzustellen, ob diese Warnregel derzeit aktiviert ist.

   Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

4. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Warnregel wird auf der Seite „Warnungen“ angezeigt und ist auch der Betreff für E-Mail-Benachrichtigungen. Namen für Warnregeln können zwischen 1 und 64 Zeichen lang sein.

Feld	Beschreibung
Beschreibung	Eine Beschreibung des auftretenden Problems. Die Beschreibung ist die Warnmeldung, die auf der Warnseite und in E-Mail-Benachrichtigungen angezeigt wird. Beschreibungen für Warnregeln können zwischen 1 und 128 Zeichen lang sein.
Empfohlene Maßnahmen	Optional die empfohlenen Maßnahmen, die ergriffen werden sollen, wenn diese Warnung ausgelöst wird. Geben Sie empfohlene Aktionen als einfachen Text ein (keine Formatierungscodes). Empfohlene Aktionen für Warnregeln können zwischen 0 und 1.024 Zeichen lang sein.

5. Geben Sie im Abschnitt „Bedingungen“ einen Prometheus-Ausdruck für einen oder mehrere Schweregrade der Warnung ein.

   Ein einfacher Ausdruck hat normalerweise die Form:

   ```
   [metric] [operator] [value]
   ```

   Ausdrücke können beliebig lang sein, werden in der Benutzeroberfläche jedoch in einer einzigen Zeile angezeigt. Mindestens ein Ausdruck ist erforderlich.

   Dieser Ausdruck bewirkt, dass eine Warnung ausgelöst wird, wenn die Menge des installierten RAM für einen Knoten weniger als 24.000.000.000 Byte (24 GB) beträgt.

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Um verfügbare Metriken anzuzeigen und Prometheus-Ausdrücke zu testen, wählen Sie das Hilfesymbol und folgen Sie dem Link zum Abschnitt „Metriken“ der Grid Management API.

6. Geben Sie im Feld **Dauer** die Zeitspanne ein, die eine Bedingung kontinuierlich wirksam bleiben muss, bevor der Alarm ausgelöst wird, und wählen Sie eine Zeiteinheit aus.

   Um sofort einen Alarm auszulösen, wenn eine Bedingung erfüllt wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass vorübergehende Bedingungen Warnungen auslösen.

   Der Standardwert beträgt 5 Minuten.

7. Wählen Sie **Speichern**.

   Das Dialogfeld wird geschlossen und die neue benutzerdefinierte Warnregel wird in der Tabelle „Warnregeln“ angezeigt.

Alarmregeln bearbeiten

Sie können eine Warnregel bearbeiten, um die Auslösebedingungen zu ändern. Bei einer benutzerdefinierten Warnregel können Sie auch den Regelnamen, die Beschreibung und die empfohlenen Aktionen aktualisieren.

Bevor Sie beginnen

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

- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Wenn Sie eine Standardwarnregel bearbeiten, können Sie die Bedingungen für geringfügige, schwerwiegende und kritische Warnungen sowie die Dauer ändern. Wenn Sie eine benutzerdefinierte Warnregel bearbeiten, können Sie auch den Namen, die Beschreibung und die empfohlenen Aktionen der Regel bearbeiten.

> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel zu bearbeiten. Wenn Sie Triggerwerte ändern, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

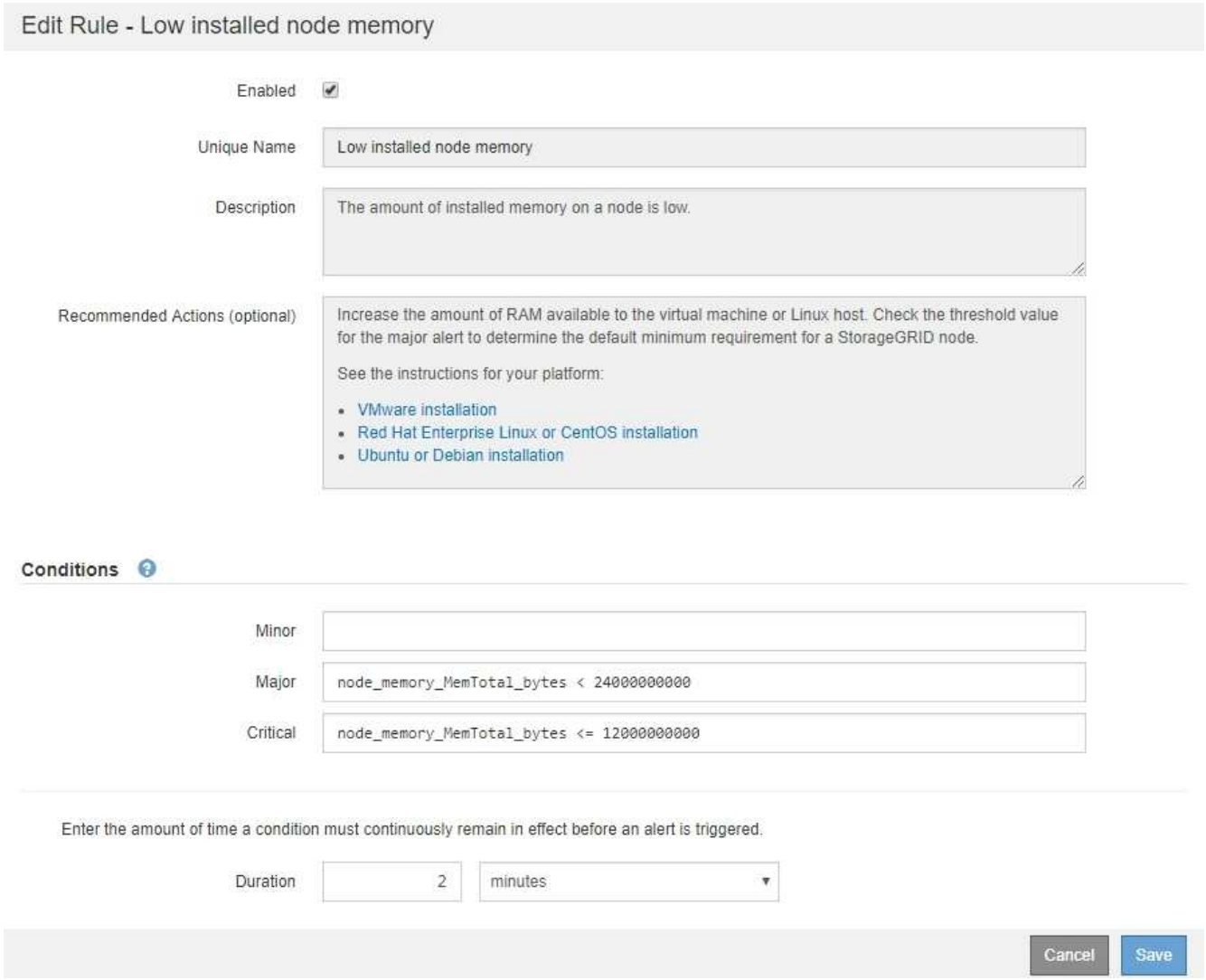
Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie das Optionsfeld für die Warnregel aus, die Sie bearbeiten möchten.
3. Wählen Sie **Regel bearbeiten**.

   Das Dialogfeld „Regel bearbeiten“ wird angezeigt. Dieses Beispiel zeigt eine Standardwarnregel – die Felder „Eindeutiger Name“, „Beschreibung“ und „Empfohlene Aktionen“ sind deaktiviert und können nicht bearbeitet werden.



4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktiviert**, um festzustellen, ob diese Warnregel derzeit aktiviert ist.

   Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

   Wenn Sie die Warnregel für eine aktuelle Warnmeldung deaktivieren, müssen Sie einige Minuten warten, bis die Warnmeldung nicht mehr als aktive Warnmeldung angezeigt wird.

   Im Allgemeinen wird das Deaktivieren einer Standardwarnregel nicht empfohlen. Wenn eine Warnregel deaktiviert ist, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

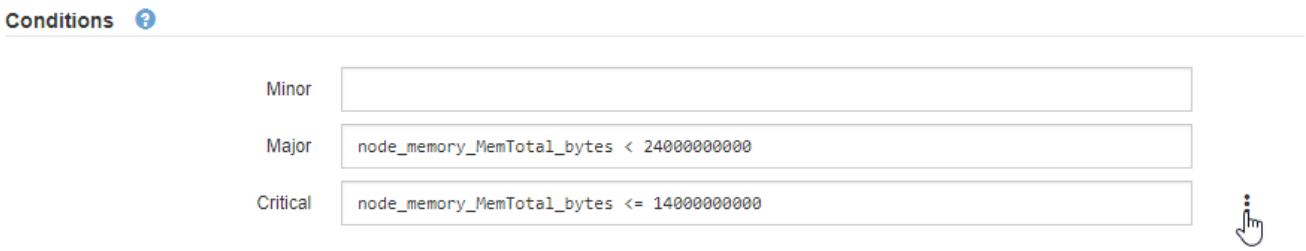
5. Aktualisieren Sie für benutzerdefinierte Warnregeln die folgenden Informationen nach Bedarf.

   Sie können diese Informationen für Standardwarnregeln nicht bearbeiten.

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Warnregel wird auf der Seite „Warnungen“ angezeigt und ist auch der Betreff für E-Mail-Benachrichtigungen. Namen für Warnregeln können zwischen 1 und 64 Zeichen lang sein.
Beschreibung	Eine Beschreibung des auftretenden Problems. Die Beschreibung ist die Warnmeldung, die auf der Warnseite und in E-Mail-Benachrichtigungen angezeigt wird. Beschreibungen für Warnregeln können zwischen 1 und 128 Zeichen lang sein.
Empfohlene Maßnahmen	Optional die empfohlenen Maßnahmen, die ergriffen werden sollen, wenn diese Warnung ausgelöst wird. Geben Sie empfohlene Aktionen als einfachen Text ein (keine Formatierungscodes). Empfohlene Aktionen für Warnregeln können zwischen 0 und 1.024 Zeichen lang sein.

6. Geben Sie im Abschnitt „Bedingungen“ den Prometheus-Ausdruck für einen oder mehrere Schweregrade der Warnung ein oder aktualisieren Sie ihn.

Wenn Sie eine Bedingung für eine bearbeitete Standardwarnregel auf ihren ursprünglichen Wert zurücksetzen möchten, wählen Sie die drei Punkte rechts neben der geänderten Bedingung aus.



Wenn Sie die Bedingungen für eine aktuelle Warnung aktualisieren, werden Ihre Änderungen möglicherweise erst implementiert, wenn die vorherige Bedingung behoben ist. Wenn das nächste Mal eine der Bedingungen für die Regel erfüllt ist, spiegelt die Warnung die aktualisierten Werte wider.

Ein einfacher Ausdruck hat normalerweise die Form:

```
[metric] [operator] [value]
```

Ausdrücke können beliebig lang sein, werden in der Benutzeroberfläche jedoch in einer einzigen Zeile angezeigt. Mindestens ein Ausdruck ist erforderlich.

Dieser Ausdruck bewirkt, dass eine Warnung ausgelöst wird, wenn die Menge des installierten RAM für einen Knoten weniger als 24.000.000.000 Byte (24 GB) beträgt.

```
node_memory_MemTotal_bytes < 24000000000
```

7. Geben Sie im Feld **Dauer** die Zeitspanne ein, die eine Bedingung kontinuierlich wirksam bleiben muss,

bevor der Alarm ausgelöst wird, und wählen Sie die Zeiteinheit aus.

Um sofort einen Alarm auszulösen, wenn eine Bedingung erfüllt wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass vorübergehende Bedingungen Warnungen auslösen.

Der Standardwert beträgt 5 Minuten.

8. Wählen Sie **Speichern**.

   Wenn Sie eine Standardwarnregel bearbeitet haben, wird **Standard*** in der Spalte Typ angezeigt. Wenn Sie eine standardmäßige oder benutzerdefinierte Warnregel deaktiviert haben, wird in der Spalte **Status Deaktiviert** angezeigt.

Warnregeln deaktivieren

Sie können den aktivierten/deaktivierten Status für eine Standard- oder benutzerdefinierte Warnregel ändern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

> Im Allgemeinen wird das Deaktivieren einer Standardwarnregel nicht empfohlen. Wenn eine Warnregel deaktiviert ist, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie das Optionsfeld für die Warnregel aus, die Sie deaktivieren oder aktivieren möchten.
3. Wählen Sie **Regel bearbeiten**.

   Das Dialogfeld „Regel bearbeiten“ wird angezeigt.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktiviert**, um festzustellen, ob diese Warnregel derzeit aktiviert ist.

   Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

   > Wenn Sie die Warnregel für eine aktuelle Warnmeldung deaktivieren, müssen Sie einige Minuten warten, bis die Warnmeldung nicht mehr als aktive Warnmeldung angezeigt wird.

5. Wählen Sie **Speichern**.

   Deaktiviert wird in der Spalte **Status** angezeigt.

Entfernen benutzerdefinierter Warnregeln

Sie können eine benutzerdefinierte Warnregel entfernen, wenn Sie sie nicht mehr verwenden möchten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie das Optionsfeld für die benutzerdefinierte Warnregel aus, die Sie entfernen möchten.

   Sie können eine Standardwarnregel nicht entfernen.

3. Wählen Sie **Benutzerdefinierte Regel entfernen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie **OK**, um die Warnregel zu entfernen.

   Alle aktiven Instanzen der Warnung werden innerhalb von 10 Minuten behoben.

Verwalten von Warnbenachrichtigungen

SNMP-Benachrichtigungen für Warnungen einrichten

Wenn StorageGRID beim Auftreten von Warnungen SNMP-Benachrichtigungen senden soll, müssen Sie den StorageGRID SNMP-Agenten aktivieren und ein oder mehrere Trap-Ziele konfigurieren.

Sie können die Option **KONFIGURATION** > **Überwachung** > **SNMP-Agent** im Grid Manager oder die SNMP-Endpunkte für die Grid Management-API verwenden, um den StorageGRID SNMP-Agenten zu aktivieren und zu konfigurieren. Der SNMP-Agent unterstützt alle drei Versionen des SNMP-Protokolls.

Informationen zur Konfiguration des SNMP-Agenten finden Sie unter"Verwenden Sie die SNMP-Überwachung" .

Nachdem Sie den StorageGRID SNMP-Agenten konfiguriert haben, können zwei Arten ereignisgesteuerter Benachrichtigungen gesendet werden:

- Traps sind vom SNMP-Agenten gesendete Benachrichtigungen, die keine Bestätigung durch das Verwaltungssystem erfordern. Traps dienen dazu, das Verwaltungssystem darüber zu informieren, dass in StorageGRID etwas passiert ist, beispielsweise dass ein Alarm ausgelöst wurde. Traps werden in allen drei Versionen von SNMP unterstützt.
- Informs ähneln Traps, erfordern jedoch eine Bestätigung durch das Managementsystem. Wenn der SNMP-Agent innerhalb einer bestimmten Zeitspanne keine Bestätigung erhält, sendet er die Information erneut, bis eine Bestätigung eingeht oder der maximale Wiederholungswert erreicht ist. Informs werden in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden gesendet, wenn ein Standard- oder benutzerdefinierter Alarm mit einem beliebigen Schweregrad ausgelöst wird. Um SNMP-Benachrichtigungen für einen Alarm zu unterdrücken, müssen Sie eine Stummschaltung für den Alarm konfigurieren. Sehen "Warnmeldungen stummschalten" .

Wenn Ihre StorageGRID -Bereitstellung mehrere Admin-Knoten umfasst, ist der primäre Admin-Knoten der bevorzugte Absender für Warnbenachrichtigungen, AutoSupport -Pakete sowie SNMP-Traps und -Informationen. Wenn der primäre Admin-Knoten nicht verfügbar ist, werden Benachrichtigungen vorübergehend von anderen Admin-Knoten gesendet. Sehen "Was ist ein Admin-Knoten?" .

E-Mail-Benachrichtigungen für Warnmeldungen einrichten

Wenn Sie beim Auftreten von Warnmeldungen E-Mail-Benachrichtigungen erhalten möchten, müssen Sie Informationen zu Ihrem SMTP-Server angeben. Sie müssen auch die E-Mail-Adressen der Empfänger von Warnbenachrichtigungen eingeben.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Das für Warnbenachrichtigungen verwendete E-Mail-Setup wird für AutoSupport Pakete nicht verwendet. Sie können jedoch für alle Benachrichtigungen denselben E-Mail-Server verwenden.

Wenn Ihre StorageGRID -Bereitstellung mehrere Admin-Knoten umfasst, ist der primäre Admin-Knoten der bevorzugte Absender für Warnbenachrichtigungen, AutoSupport -Pakete sowie SNMP-Traps und -Informationen. Wenn der primäre Admin-Knoten nicht verfügbar ist, werden Benachrichtigungen vorübergehend von anderen Admin-Knoten gesendet. Sehen "Was ist ein Admin-Knoten?" .

Schritte

1. Wählen Sie **WARNUNGEN** > **E-Mail-Setup**.

   Die Seite „E-Mail-Setup“ wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, um anzugeben, dass Benachrichtigungs-E-Mails gesendet werden sollen, wenn Warnungen konfigurierte Schwellenwerte erreichen.

   Die Abschnitte „E-Mail-Server (SMTP)“, „Transport Layer Security (TLS), E-Mail-Adressen“ und „Filter“ werden angezeigt.

3. Geben Sie im Abschnitt „E-Mail-Server (SMTP)“ die Informationen ein, die StorageGRID für den Zugriff auf Ihren SMTP-Server benötigt.

   Wenn Ihr SMTP-Server eine Authentifizierung erfordert, müssen Sie sowohl einen Benutzernamen als auch ein Kennwort angeben.

Feld	Eingeben
Mailserver	Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des SMTP-Servers.

Feld	Eingeben
Hafen	Der für den Zugriff auf den SMTP-Server verwendete Port. Muss zwischen 1 und 65535 liegen.
Benutzername (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen zur Authentifizierung ein.
Passwort (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie das Kennwort zur Authentifizierung ein.

4. Geben Sie im Abschnitt „E-Mail-Adressen“ die E-Mail-Adressen des Absenders und aller Empfänger ein.
   a. Geben Sie für die **E-Mail-Adresse des Absenders** eine gültige E-Mail-Adresse an, die als Absenderadresse für Warnbenachrichtigungen verwendet werden soll.

      Beispiel: `storagegrid-alerts@example.com`

   b. Geben Sie im Abschnitt „Empfänger“ für jede E-Mail-Liste oder Person eine E-Mail-Adresse ein, die bei Auftreten einer Warnung eine E-Mail erhalten soll.

      Wählen Sie das Plus-Symbol ➕ um Empfänger hinzuzufügen.

5. Wenn für die Kommunikation mit dem SMTP-Server Transport Layer Security (TLS) erforderlich ist, wählen Sie im Abschnitt Transport Layer Security (TLS) die Option **TLS erforderlich** aus.
   a. Geben Sie im Feld **CA-Zertifikat** das CA-Zertifikat ein, das zur Überprüfung der Identität des SMTP-Servers verwendet wird.

      Sie können den Inhalt kopieren und in dieses Feld einfügen oder **Durchsuchen** auswählen und die Datei auswählen.

      Sie müssen eine einzelne Datei bereitstellen, 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.

   b. Aktivieren Sie das Kontrollkästchen **Client-Zertifikat senden**, wenn Ihr SMTP-E-Mail-Server von E-Mail-Absendern die Bereitstellung von Client-Zertifikaten zur Authentifizierung erfordert.
   c. Geben Sie im Feld **Client-Zertifikat** das PEM-codierte Client-Zertifikat ein, das an den SMTP-Server gesendet werden soll.

      Sie können den Inhalt kopieren und in dieses Feld einfügen oder **Durchsuchen** auswählen und die Datei auswählen.

   d. Geben Sie im Feld **Privater Schlüssel** den privaten Schlüssel für das Client-Zertifikat in unverschlüsselter PEM-Kodierung ein.

      Sie können den Inhalt kopieren und in dieses Feld einfügen oder **Durchsuchen** auswählen und die Datei auswählen.

> ⓘ Wenn Sie die E-Mail-Einstellungen bearbeiten müssen, wählen Sie das Bleistiftsymbol um dieses Feld zu aktualisieren.

6. Wählen Sie im Abschnitt „Filter“ aus, welche Warnschweregrade zu E-Mail-Benachrichtigungen führen sollen, es sei denn, die Regel für eine bestimmte Warnmeldung wurde stummgeschaltet.

Schwere	Beschreibung
Geringfügig, schwerwiegend, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die geringfügige, schwerwiegende oder kritische Bedingung für eine Warnregel erfüllt ist.
Schwerwiegend, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die schwerwiegende oder kritische Bedingung für eine Warnregel erfüllt ist. Bei geringfügigen Warnungen werden keine Benachrichtigungen gesendet.
Nur kritisch	Eine E-Mail-Benachrichtigung wird nur gesendet, wenn die kritische Bedingung für eine Warnregel erfüllt ist. Für kleinere oder größere Warnungen werden keine Benachrichtigungen gesendet.

7. Wenn Sie bereit sind, Ihre E-Mail-Einstellungen zu testen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **Test-E-Mail senden**.

      Es wird eine Bestätigungsmeldung angezeigt, die darauf hinweist, dass eine Test-E-Mail gesendet wurde.

   b. Überprüfen Sie die Posteingänge aller E-Mail-Empfänger und bestätigen Sie, dass eine Test-E-Mail empfangen wurde.

      Wenn die E-Mail nicht innerhalb weniger Minuten eingeht oder die Warnung **Fehler bei E-Mail-Benachrichtigung** ausgelöst wird, überprüfen Sie Ihre Einstellungen und versuchen Sie es erneut.

   c. Sign in und senden Sie eine Test-E-Mail, um die Konnektivität von allen Sites zu überprüfen.

      Wenn Sie Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Konnektivität zu überprüfen. Dies steht im Gegensatz zum Testen von AutoSupport -Paketen, bei dem alle Admin-Knoten die Test-E-Mail senden.

8. Wählen Sie **Speichern**.

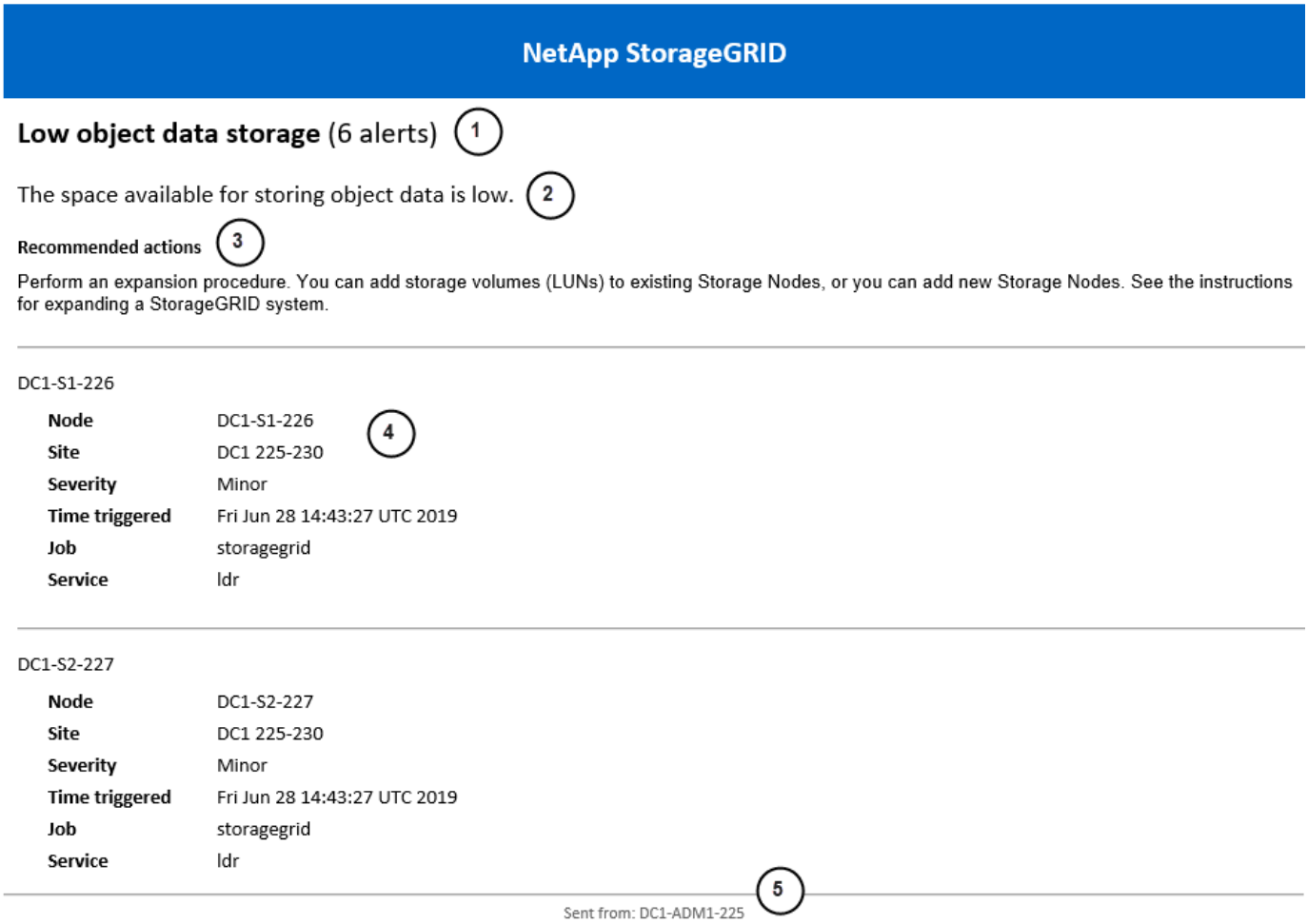
   Durch das Senden einer Test-E-Mail werden Ihre Einstellungen nicht gespeichert. Sie müssen **Speichern** auswählen.

   Die E-Mail-Einstellungen werden gespeichert.

In E-Mail-Benachrichtigungen enthaltene Informationen

Nachdem Sie den SMTP-E-Mail-Server konfiguriert haben, werden E-Mail-Benachrichtigungen an die angegebenen Empfänger gesendet, wenn eine Warnung ausgelöst wird, es sei denn, die Warnungsregel wird durch eine Stummschaltung unterdrückt. Sehen "Warnmeldungen stummschalten" .

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:



Aufbieten, ausrufen, zurufen	Beschreibung
1	Der Name der Warnung, gefolgt von der Anzahl der aktiven Instanzen dieser Warnung.
2	Die Beschreibung der Warnung.
3	Alle empfohlenen Maßnahmen für die Warnung.
4	Details zu jeder aktiven Instanz der Warnung, einschließlich des betroffenen Knotens und der betroffenen Site, des Schweregrads der Warnung, der UTC-Zeit, zu der die Warnungsregel ausgelöst wurde, und des Namens des betroffenen Auftrags und Dienstes.
5	Der Hostname des Admin-Knotens, der die Benachrichtigung gesendet hat.

So werden Warnungen gruppiert

Um zu verhindern, dass beim Auslösen von Warnungen eine übermäßige Anzahl von E-Mail-Benachrichtigungen gesendet wird, versucht StorageGRID , mehrere Warnungen in derselben Benachrichtigung zu gruppieren.

In der folgenden Tabelle finden Sie Beispiele dafür, wie StorageGRID mehrere Warnungen in E-Mail-

Benachrichtigungen gruppiert.

Verhalten	Beispiel
Jede Warnmeldung gilt nur für Warnmeldungen mit demselben Namen. Wenn zwei Warnungen mit unterschiedlichen Namen gleichzeitig ausgelöst werden, werden zwei E-Mail-Benachrichtigungen gesendet.	• Alarm A wird auf zwei Knoten gleichzeitig ausgelöst. Es wird nur eine Benachrichtigung gesendet. • Alarm A wird auf Knoten 1 ausgelöst und Alarm B wird gleichzeitig auf Knoten 2 ausgelöst. Es werden zwei Benachrichtigungen gesendet – eine für jeden Alarm.
Wenn bei einer bestimmten Warnung auf einem bestimmten Knoten die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird nur für die Warnung mit dem höchsten Schweregrad eine Benachrichtigung gesendet.	• Alarm A wird ausgelöst und die Schwellenwerte für geringfügige, schwerwiegende und kritische Alarme werden erreicht. Für den kritischen Alarm wird eine Benachrichtigung gesendet.
Wenn zum ersten Mal ein Alarm ausgelöst wird, wartet StorageGRID 2 Minuten, bevor eine Benachrichtigung gesendet wird. Wenn während dieser Zeit andere Warnungen mit demselben Namen ausgelöst werden, gruppiert StorageGRID alle Warnungen in der ersten Benachrichtigung.	1. Alarm A wird um 08:00 Uhr auf Knoten 1 ausgelöst. Es wird keine Benachrichtigung gesendet. 2. Alarm A wird um 08:01 Uhr auf Knoten 2 ausgelöst. Es wird keine Benachrichtigung gesendet. 3. Um 08:02 Uhr wird eine Benachrichtigung gesendet, um beide Instanzen des Alarms zu melden.
Wenn ein weiterer Alarm mit demselben Namen ausgelöst wird, wartet StorageGRID 10 Minuten, bevor eine neue Benachrichtigung gesendet wird. Die neue Benachrichtigung meldet alle aktiven Warnungen (aktuelle Warnungen, die nicht stummgeschaltet wurden), auch wenn sie zuvor gemeldet wurden.	1. Alarm A wird um 08:00 Uhr auf Knoten 1 ausgelöst. Um 08:02 Uhr wird eine Benachrichtigung gesendet. 2. Alarm A wird um 08:05 Uhr auf Knoten 2 ausgelöst. Eine zweite Benachrichtigung wird um 08:15 Uhr (10 Minuten später) gesendet. Beide Knoten werden gemeldet.
Wenn mehrere aktuelle Warnungen mit demselben Namen vorliegen und eine dieser Warnungen behoben wird, wird keine neue Benachrichtigung gesendet, wenn die Warnung auf dem Knoten erneut auftritt, für den die Warnung behoben wurde.	1. Alarm A wird für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Alarm A wird für Knoten 2 ausgelöst. Eine zweite Benachrichtigung wird gesendet. 3. Alarm A wird für Knoten 2 behoben, bleibt aber für Knoten 1 aktiv. 4. Alarm A wird für Knoten 2 erneut ausgelöst. Es wird keine neue Benachrichtigung gesendet, da der Alarm für Knoten 1 noch aktiv ist.

Verhalten	Beispiel
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen des Alarms behoben oder die Alarmregel stummgeschaltet sind.	1. Alarm A wird am 8. März für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Alarm A wird nicht behoben oder stummgeschaltet. Weitere Benachrichtigungen werden am 15. März, 22. März, 29. März usw. gesendet.

Fehlerbehebung bei E-Mail-Benachrichtigungen

Wenn die Warnung **Fehler bei E-Mail-Benachrichtigung** ausgelöst wird oder Sie die E-Mail-Benachrichtigung zum Testalarm nicht erhalten können, führen Sie die folgenden Schritte aus, um das Problem zu beheben.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Schritte

1. Überprüfen Sie Ihre Einstellungen.
   a. Wählen Sie **WARNUNGEN** > **E-Mail-Setup**.
   b. Überprüfen Sie, ob die Einstellungen des E-Mail-Servers (SMTP) korrekt sind.
   c. Stellen Sie sicher, dass Sie gültige E-Mail-Adressen für die Empfänger angegeben haben.
2. Überprüfen Sie Ihren Spamfilter und stellen Sie sicher, dass die E-Mail nicht in einen Junk-Ordner verschoben wurde.
3. Bitten Sie Ihren E-Mail-Administrator um Bestätigung, dass E-Mails von der Absenderadresse nicht blockiert werden.
4. Erstellen Sie eine Protokolldatei für den Admin-Knoten und wenden Sie sich dann an den technischen Support.

   Der technische Support kann die Informationen in den Protokollen verwenden, um festzustellen, was schiefgelaufen ist. Beispielsweise kann die Datei „prometheus.log“ beim Herstellen einer Verbindung mit dem von Ihnen angegebenen Server einen Fehler anzeigen.

   Sehen "Erfassen von Protokolldateien und Systemdaten" .

Warnmeldungen stummschalten

Optional können Sie Stummschaltungen konfigurieren, um Warnbenachrichtigungen vorübergehend zu unterdrücken.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Sie können Warnregeln für das gesamte Raster, eine einzelne Site oder einen einzelnen Knoten und für einen oder mehrere Schweregrade stummschalten. Jede Stille unterdrückt alle Benachrichtigungen für eine einzelne

Warnregel oder für alle Warnregeln.

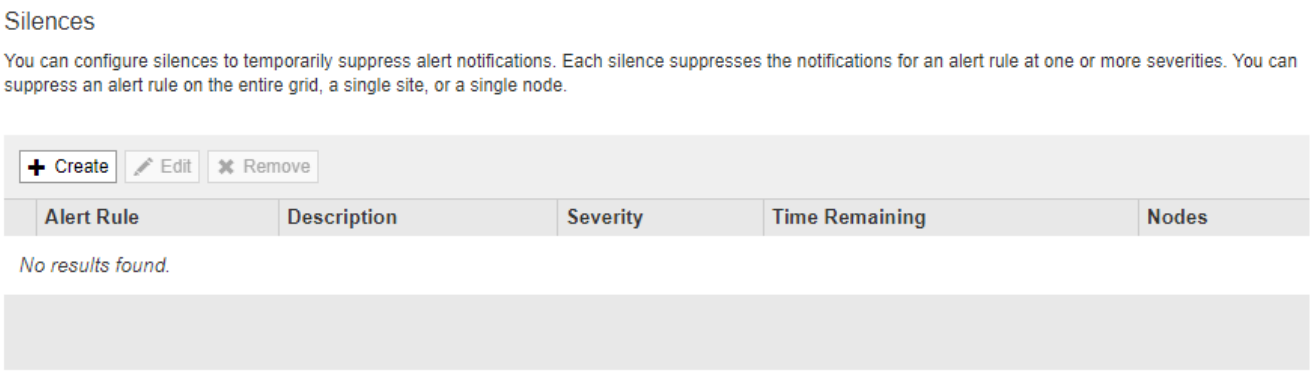
Wenn Sie den SNMP-Agenten aktiviert haben, werden durch Stummschalten auch SNMP-Traps und -Informationen unterdrückt.

> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel stummzuschalten. Wenn Sie eine Warnung stummschalten, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

Schritte

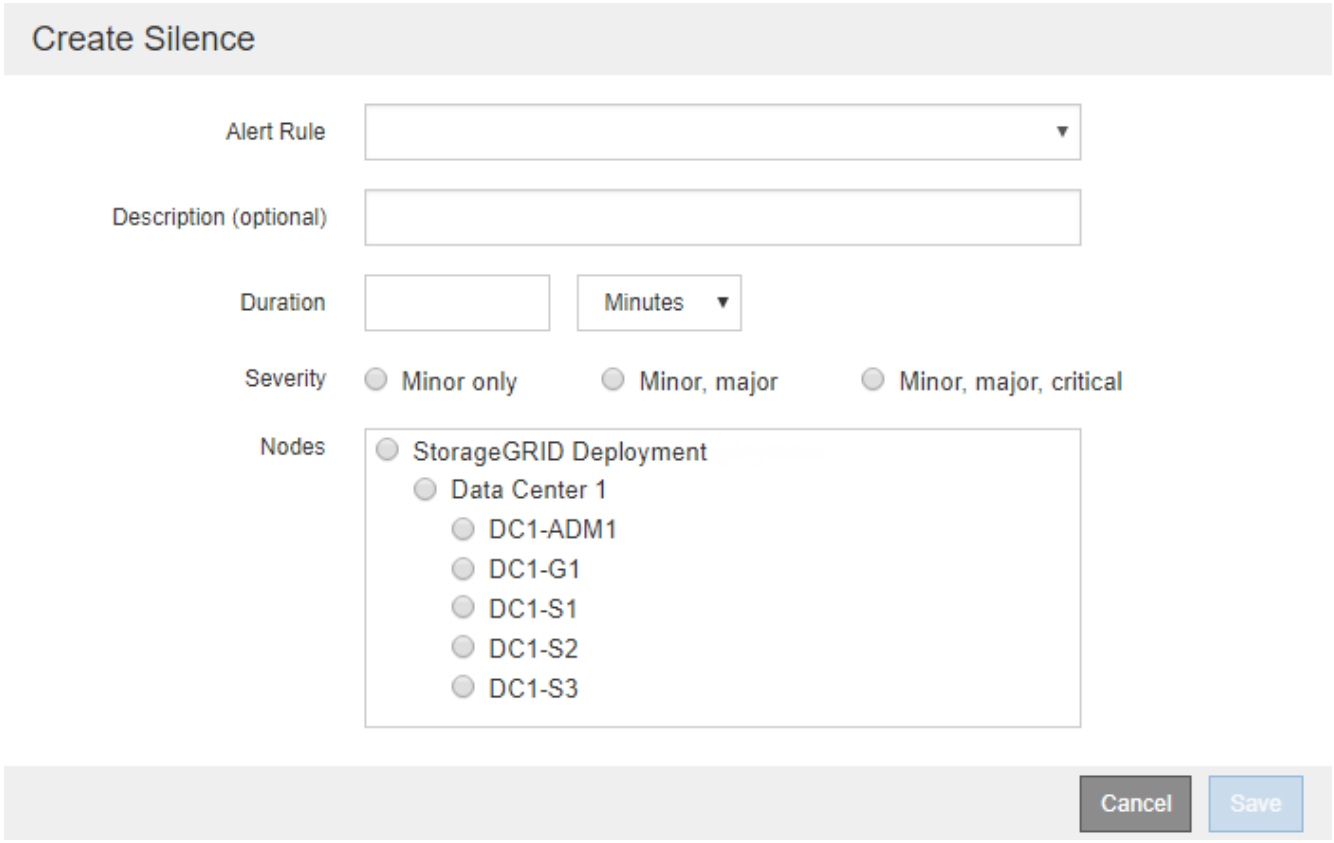
1. Wählen Sie **WARNUNGEN** > **Stummschaltungen**.

   Die Seite „Stille“ wird angezeigt.



2. Wählen Sie **Erstellen**.

   Das Dialogfeld „Stille erstellen“ wird angezeigt.



3. Wählen Sie die folgenden Informationen aus oder geben Sie sie ein:

Feld	Beschreibung
Warnregel	Der Name der Warnregel, die Sie stummschalten möchten. Sie können jede Standard- oder benutzerdefinierte Warnregel auswählen, auch wenn die Warnregel deaktiviert ist. **Hinweis:** Wählen Sie **Alle Regeln** aus, wenn Sie alle Warnregeln anhand der in diesem Dialogfeld angegebenen Kriterien stummschalten möchten.
Beschreibung	Optional eine Beschreibung der Stille. Beschreiben Sie beispielsweise den Zweck dieser Stille.
Dauer	Wie lange diese Stille in Kraft bleiben soll, in Minuten, Stunden oder Tagen. Eine Sperre kann zwischen 5 Minuten und 1.825 Tagen (5 Jahren) wirksam sein. **Hinweis:** Sie sollten eine Warnregel nicht für einen längeren Zeitraum stummschalten. Wenn eine Warnregel stummgeschaltet wird, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert. Möglicherweise müssen Sie jedoch eine längere Stille verwenden, wenn eine Warnung durch eine bestimmte, absichtliche Konfiguration ausgelöst wird, wie dies beispielsweise bei den Warnungen „Link zur Service-Appliance unterbrochen“ und „Link zur Speicher-Appliance unterbrochen“ der Fall sein kann.
Schwere	Welcher oder welche Schweregrade der Warnungen sollten stummgeschaltet werden? Wenn der Alarm bei einem der ausgewählten Schweregrade ausgelöst wird, werden keine Benachrichtigungen gesendet.
Nodes	Auf welchen Knoten oder welche Knoten soll diese Stille angewendet werden? Sie können eine Warnregel oder alle Regeln für das gesamte Raster, eine einzelne Site oder einen einzelnen Knoten unterdrücken. Wenn Sie das gesamte Raster auswählen, gilt die Stille für alle Sites und alle Knoten. Wenn Sie einen Standort auswählen, gilt die Stille nur für die Knoten an diesem Standort. **Hinweis:** Sie können für jede Stille nicht mehr als einen Knoten oder mehr als eine Site auswählen. Sie müssen zusätzliche Stummschaltungen erstellen, wenn Sie dieselbe Warnregel auf mehreren Knoten oder mehreren Sites gleichzeitig unterdrücken möchten.

4. Wählen Sie **Speichern**.
5. Wenn Sie eine Stille ändern oder beenden möchten, bevor sie abläuft, können Sie sie bearbeiten oder entfernen.

Option	Beschreibung
Bearbeiten einer Stille	a. Wählen Sie **WARNUNGEN** > **Stummschaltungen**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille aus, die Sie bearbeiten möchten. c. Wählen Sie **Bearbeiten**. d. Ändern Sie die Beschreibung, die verbleibende Zeit, die ausgewählten Schweregrade oder den betroffenen Knoten. e. Wählen Sie **Speichern**.
Eine Stille entfernen	a. Wählen Sie **WARNUNGEN** > **Stummschaltungen**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille aus, die Sie entfernen möchten. c. Wählen Sie **Entfernen**. d. Wählen Sie **OK**, um zu bestätigen, dass Sie diese Stille entfernen möchten. **Hinweis**: Wenn dieser Alarm ausgelöst wird, werden jetzt Benachrichtigungen gesendet (sofern sie nicht durch eine andere Stille unterdrückt werden). Wenn diese Warnung derzeit ausgelöst wird, kann es einige Minuten dauern, bis E-Mail- oder SNMP-Benachrichtigungen gesendet werden und die Seite „Warnungen“ aktualisiert wird.

Ähnliche Informationen

"Konfigurieren des SNMP-Agenten"

Warnungsreferenz

In dieser Referenz sind die Standardwarnungen aufgelistet, die im Grid Manager angezeigt werden. Empfohlene Maßnahmen finden Sie in der Warnmeldung, die Sie erhalten.

Bei Bedarf können Sie benutzerdefinierte Warnregeln erstellen, die zu Ihrem Systemverwaltungsansatz passen.

Einige der Standardwarnungen verwenden"Prometheus-Metriken" .

Gerätewarnungen

Name der Warnung	Beschreibung
Gerätebatterie leer	Die Batterie im Speichercontroller des Geräts ist leer.
Gerätebatterie defekt	Die Batterie im Speichercontroller des Geräts ist ausgefallen.

Name der Warnung	Beschreibung
Die Gerätebatterie hat nicht genügend gelernte Kapazität	Die Batterie im Speichercontroller des Geräts verfügt nicht über die erforderliche Kapazität.
Gerätebatterie fast leer	Die Batterie im Speichercontroller des Geräts ist fast leer.
Gerätebatterie entfernt	Die Batterie im Speichercontroller des Geräts fehlt.
Gerätebatterie zu heiß	Die Batterie im Speichercontroller des Geräts ist überhitzt.
Appliance- BMC Kommunikationsfehler	Die Kommunikation mit dem Baseboard Management Controller (BMC) ist verloren gegangen.
Fehler beim Boot-Gerät der Appliance erkannt	Es wurde ein Problem mit dem Startgerät in der Appliance erkannt.
Fehler beim Appliance-Cache-Sicherungsgerät	Ein persistentes Cache-Backup-Gerät ist ausgefallen.
Unzureichende Kapazität des Appliance-Cache-Sicherungsgeräts	Die Kapazität des Cache-Backup-Geräts ist nicht ausreichend.
Appliance-Cache-Sicherungsgerät schreibgeschützt	Ein Cache-Backup-Gerät ist schreibgeschützt.
Nicht übereinstimmende Größe des Appliance-Cache-Speichers	Die beiden Controller in der Appliance haben unterschiedliche Cachegrößen.
Fehler der CMOS-Batterie des Geräts	Es wurde ein Problem mit der CMOS-Batterie im Gerät festgestellt.
Gehäusetemperatur des Appliance-Compute-Controllers zu hoch	Die Temperatur des Compute-Controllers in einem StorageGRID Gerät hat einen nominalen Schwellenwert überschritten.
CPU-Temperatur des Appliance-Compute-Controllers zu hoch	Die Temperatur der CPU im Compute Controller in einem StorageGRID -Gerät hat einen nominalen Schwellenwert überschritten.
Der Appliance-Compute-Controller erfordert Aufmerksamkeit	Im Compute-Controller eines StorageGRID Geräts wurde ein Hardwarefehler erkannt.
Netzteil A des Appliance-Compute-Controllers hat ein Problem	Netzteil A im Compute-Controller hat ein Problem.
Das Netzteil B des Appliance-Compute-Controllers hat ein Problem	Netzteil B im Compute-Controller hat ein Problem.

Name der Warnung	Beschreibung
Der Dienst zur Überwachung der Appliance-Compute-Hardware ist angehalten	Der Dienst, der den Status der Speicherhardware überwacht, ist ins Stocken geraten.
Das Appliance-DAS-Laufwerk überschreitet das Limit für pro Tag geschriebene Daten	Jeden Tag werden übermäßig viele Daten auf ein Laufwerk geschrieben, was zum Erlöschen der Garantie führen kann.
Fehler im DAS-Laufwerk der Appliance erkannt	Es wurde ein Problem mit einem DAS-Laufwerk (Direct Attached Storage) in der Appliance erkannt.
Appliance DAS-Laufwerkssuchleuchte leuchtet	Die Laufwerkslokalisierungsleuchte für ein oder mehrere DAS-Laufwerke (Direct Attached Storage) in einem Appliance-Speicherknoten leuchtet.
Neuerstellung des Appliance-DAS-Laufwerks	Ein Direct-Attached-Storage-Laufwerk (DAS) wird neu erstellt. Dies ist zu erwarten, wenn es vor Kurzem ersetzt oder entfernt/wieder eingesetzt wurde.
Gerätelüfterfehler erkannt	Es wurde ein Problem mit einer Lüftereinheit im Gerät festgestellt.
Appliance-Fibre-Channel-Fehler erkannt	Zwischen dem Speichercontroller und dem Compute-Controller der Appliance wurde ein Fibre-Channel-Verbindungsproblem erkannt
Appliance-Fibre-Channel-HBA-Portfehler	Ein Fibre Channel-HBA-Port fällt aus oder ist ausgefallen.
Appliance-Flash-Cache-Laufwerke nicht optimal	Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal.
Geräteverbindung/Batteriebehälter entfernt	Der Verbindungs-/Batteriebehälter fehlt.
Appliance-LACP-Port fehlt	Ein Port auf einem StorageGRID -Gerät nimmt nicht an der LACP-Verbindung teil.
Fehler der Appliance-NIC erkannt	Es wurde ein Problem mit einer Netzwerkschnittstellenkarte (NIC) im Gerät erkannt.
Gesamtstromversorgung des Geräts beeinträchtigt	Die Leistung eines StorageGRID -Geräts weicht von der empfohlenen Betriebsspannung ab.
Kritische Warnung zur Appliance-SSD	Eine Appliance-SSD meldet eine kritische Warnung.

Name der Warnung	Beschreibung
Fehler beim Appliance-Speichercontroller A	Speichercontroller A in einem StorageGRID -Gerät ist ausgefallen.
Ausfall des Appliance-Speichercontrollers B	Speichercontroller B in einem StorageGRID Gerät ist ausgefallen.
Ausfall des Laufwerks des Appliance-Speichercontrollers	Ein oder mehrere Laufwerke in einem StorageGRID -Gerät sind ausgefallen oder nicht optimal.
Hardwareproblem mit dem Appliance-Speichercontroller	Die SANtricity -Software meldet „Benötigt Aufmerksamkeit“ für eine Komponente in einem StorageGRID Gerät.
Ausfall der Stromversorgung des Appliance-Speichercontrollers A	Netzteil A in einem StorageGRID -Gerät weicht von der empfohlenen Betriebsspannung ab.
Ausfall der Stromversorgung B des Appliance-Speichercontrollers	Netzteil B in einem StorageGRID -Gerät ist von der empfohlenen Betriebsspannung abgewichen.
Der Dienst zur Überwachung der Appliance-Speicherhardware ist angehalten	Der Dienst, der den Status der Speicherhardware überwacht, ist ins Stocken geraten.
Abgenutzte Regale für die Geräteablage	Der Status einer der Komponenten im Speicherregal für ein Speichergerät ist herabgestuft.
Gerätetemperatur überschritten	Die Nenn- oder Maximaltemperatur für den Speichercontroller der Appliance wurde überschritten.
Gerätetemperatursensor entfernt	Ein Temperatursensor wurde entfernt.
Appliance-UEFI-Sicherheitsstartfehler	Ein Gerät wurde nicht sicher gestartet.
Die Festplatten-E/A ist sehr langsam	Sehr langsame Festplatten-E/A können die Grid-Leistung beeinträchtigen.
Lüfterfehler des Speichergeräts erkannt	Es wurde ein Problem mit einer Lüftereinheit im Speichercontroller für eine Appliance erkannt.
Speicherkonnektivität des Speichergeräts beeinträchtigt	Es liegt ein Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller vor.
Auf das Speichergerät kann nicht zugegriffen werden	Auf ein Speichergerät kann nicht zugegriffen werden.

Audit- und Syslog-Warnmeldungen

Name der Warnung	Beschreibung
Audit-Protokolle werden der In-Memory-Warteschlange hinzugefügt	Der Knoten kann keine Protokolle an den lokalen Syslog-Server senden und die Warteschlange im Arbeitsspeicher füllt sich.
Fehler bei der Weiterleitung des externen Syslog-Servers	Der Knoten kann keine Protokolle an den externen Syslog-Server weiterleiten.
Große Prüfwarteschlange	Die Festplattenwarteschlange für Prüfmeldungen ist voll. Wenn dieser Zustand nicht behoben wird, können S3- oder Swift-Vorgänge fehlschlagen.
Protokolle werden der Warteschlange auf der Festplatte hinzugefügt	Der Knoten kann keine Protokolle an den externen Syslog-Server weiterleiten und die Warteschlange auf der Festplatte füllt sich.

Bucket-Benachrichtigungen

Name der Warnung	Beschreibung
FabricPool Bucket verfügt über eine nicht unterstützte Bucket-Konsistenzeinstellung	Ein FabricPool Bucket verwendet die Konsistenzebene „Verfügbar“ oder „Stark-Site“, die nicht unterstützt wird.
FabricPool Bucket verfügt über nicht unterstützte Versionseinstellungen	Für einen FabricPool Bucket sind Versionierung oder S3 Object Lock aktiviert, die nicht unterstützt werden.

Cassandra-Warnungen

Name der Warnung	Beschreibung
Cassandra-Autokompaktorfehler	Beim Cassandra-Autokompaktor ist ein Fehler aufgetreten.
Die Metriken des Cassandra-Autokompaktors sind veraltet	Die Metriken, die den Cassandra-Autokompaktor beschreiben, sind veraltet.
Cassandra-Kommunikationsfehler	Die Knoten, auf denen der Cassandra-Dienst ausgeführt wird, haben Probleme bei der Kommunikation untereinander.
Cassandra-Komprimierungen überlastet	Der Cassandra-Komprimierungsprozess ist überlastet.
Cassandra-Übergrößen-Schreibfehler	Ein interner StorageGRID -Prozess hat eine zu große Schreibanforderung an Cassandra gesendet.

Name der Warnung	Beschreibung
Cassandra-Reparaturmetriken veraltet	Die Metriken, die Cassandra-Reparaturjobs beschreiben, sind veraltet.
Cassandra-Reparaturfortschritt langsam	Die Reparatur der Cassandra-Datenbank schreitet nur langsam voran.
Cassandra-Reparaturdienst nicht verfügbar	Der Cassandra-Reparaturservice ist nicht verfügbar.
Cassandra-Tabellenbeschädigung	Cassandra hat eine Tabellenbeschädigung festgestellt. Cassandra wird automatisch neu gestartet, wenn eine Tabellenbeschädigung erkannt wird.

Cloud Storage Pool-Warnungen

Name der Warnung	Beschreibung
Verbindungsfehler beim Cloud-Speicherpool	Bei der Integritätsprüfung für Cloud Storage Pools wurden ein oder mehrere neue Fehler festgestellt.
Ablauf der IAM Roles Anywhere-Endentitätszertifizierung	Das Endentitätszertifikat von IAM Roles Anywhere läuft bald ab.

Warnungen zur Grid-übergreifenden Replikation

Name der Warnung	Beschreibung
Dauerhafter Fehler bei der Cross-Grid-Replikation	Bei der gitterübergreifenden Replikation ist ein Fehler aufgetreten, der zur Behebung einen Benutzereingriff erfordert.
Cross-Grid-Replikationsressourcen nicht verfügbar	Gridübergreifende Replikationsanforderungen stehen aus, weil eine Ressource nicht verfügbar ist.

DHCP-Warnmeldungen

Name der Warnung	Beschreibung
DHCP-Lease abgelaufen	Die DHCP-Lease einer Netzwerkschnittstelle ist abgelaufen.
DHCP-Lease läuft bald ab	Die DHCP-Lease einer Netzwerkschnittstelle läuft bald ab.
DHCP-Server nicht verfügbar	Der DHCP-Server ist nicht verfügbar.

Debug- und Trace-Warnungen

Name der Warnung	Beschreibung
Auswirkungen auf die Debugleistung	Wenn der Debug-Modus aktiviert ist, kann die Systemleistung negativ beeinflusst werden.
Trace-Konfiguration aktiviert	Wenn die Trace-Konfiguration aktiviert ist, kann die Systemleistung negativ beeinflusst werden.

E-Mail- und AutoSupport Benachrichtigungen

Name der Warnung	Beschreibung
AutoSupport -Nachricht konnte nicht gesendet werden	Das Senden der letzten AutoSupport -Nachricht ist fehlgeschlagen.
Fehler bei der Domänennamenauflösung	Der StorageGRID -Knoten konnte Domänennamen nicht auflösen.
Fehler bei der E-Mail-Benachrichtigung	Die E-Mail-Benachrichtigung für eine Warnung konnte nicht gesendet werden.
SNMP-Informationsfehler	Fehler beim Senden von SNMP-Informationsbenachrichtigungen an ein Trap-Ziel.
SSH- oder Konsolen-Login erkannt	In den letzten 24 Stunden hat sich ein Benutzer mit der Webkonsole oder SSH angemeldet.

Erasure Coding (EC)-Warnungen

Name der Warnung	Beschreibung
EC-Neuausgleichsfehler	Der EC-Neuausgleichsvorgang ist fehlgeschlagen oder wurde abgebrochen.
EC-Reparaturfehler	Ein Reparaturauftrag für EC-Daten ist fehlgeschlagen oder wurde abgebrochen.
EC-Reparatur ins Stocken geraten	Ein Reparaturauftrag für EC-Daten ist ins Stocken geraten.
Fehler bei der Überprüfung des Löschcodierungsfragments	Erasure-Coded-Fragmente können nicht mehr verifiziert werden. Beschädigte Fragmente können möglicherweise nicht repariert werden.

Warnungen zum Ablauf von Zertifikaten

Name der Warnung	Beschreibung
Ablauf des Admin Proxy CA-Zertifikats	Ein oder mehrere Zertifikate im CA-Paket des Admin-Proxyservers laufen bald ab.

Name der Warnung	Beschreibung
Ablauf des Client-Zertifikats	Ein oder mehrere Client-Zertifikate laufen bald ab.
Ablauf des globalen Serverzertifikats für S3 und Swift	Das globale Serverzertifikat für S3 und Swift läuft bald ab.
Ablauf des Load Balancer-Endpunktzertifikats	Ein oder mehrere Load Balancer-Endpunktzertifikate laufen bald ab.
Ablauf des Serverzertifikats für die Verwaltungsschnittstelle	Das für die Verwaltungsschnittstelle verwendete Serverzertifikat läuft bald ab.
Ablauf des externen Syslog-CA-Zertifikats	Das zum Signieren des externen Syslog-Serverzertifikats verwendete Zertifikat der Zertifizierungsstelle (CA) läuft bald ab.
Ablauf des externen Syslog-Client-Zertifikats	Das Client-Zertifikat für einen externen Syslog-Server läuft bald ab.
Ablauf des Zertifikats des externen Syslog-Servers	Das vom externen Syslog-Server vorgelegte Serverzertifikat läuft bald ab.

Grid-Netzwerkwarnungen

Name der Warnung	Beschreibung
MTU-Nichtübereinstimmung im Netz	Die MTU-Einstellung für die Grid-Netzwerkschnittstelle (eth0) unterscheidet sich erheblich zwischen den Knoten im Grid.

Grid-Föderationswarnungen

Name der Warnung	Beschreibung
Ablauf des Netzverbundzertifikats	Ein oder mehrere Grid-Föderation-Zertifikate laufen bald ab.
Grid-Föderation-Verbindungsfehler	Die Grid-Föderation-Verbindung zwischen dem lokalen und dem Remote-Grid funktioniert nicht.

Warnungen bei hoher Auslastung oder hoher Latenz

Name der Warnung	Beschreibung
Hohe Java-Heap-Nutzung	Ein hoher Prozentsatz des Java-Heap-Speichers wird verwendet.
Hohe Latenz bei Metadatenabfragen	Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang.

Identitätsföderationswarnungen

Name der Warnung	Beschreibung
Fehler bei der Synchronisierung der Identitätsföderation	Föderierte Gruppen und Benutzer können nicht aus der Identitätsquelle synchronisiert werden.
Fehler bei der Identitätsföderationssynchronisierung für einen Mandanten	Föderierte Gruppen und Benutzer können nicht aus der von einem Mandanten konfigurierten Identitätsquelle synchronisiert werden.

Warnungen zum Information Lifecycle Management (ILM)

Name der Warnung	Beschreibung
ILM-Platzierung nicht erreichbar	Für bestimmte Objekte ist eine Platzierungsanweisung in einer ILM-Regel nicht realisierbar.
Niedrige ILM-Scanrate	Die ILM-Scanrate ist auf weniger als 100 Objekte/Sekunde eingestellt.

Warnungen des Schlüsselverwaltungsservers (KMS)

Name der Warnung	Beschreibung
Ablauf des KMS-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des Zertifikats des Schlüsselverwaltungsservers (KMS) verwendet wurde, läuft bald ab.
Ablauf des KMS-Clientzertifikats	Das Client-Zertifikat für einen Schlüsselverwaltungsserver läuft bald ab
KMS-Konfiguration konnte nicht geladen werden	Die Konfiguration für den Schlüsselverwaltungsserver ist vorhanden, konnte aber nicht geladen werden.
KMS-Konnektivitätsfehler	Ein Appliance-Knoten konnte keine Verbindung zum Schlüsselverwaltungsserver für seine Site herstellen.
Name des KMS-Verschlüsselungsschlüssels nicht gefunden	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt.
Fehler bei der Rotation des KMS-Verschlüsselungsschlüssels	Alle Appliance-Volumes wurden erfolgreich entschlüsselt, aber ein oder mehrere Volumes konnten nicht auf den neuesten Schlüssel rotiert werden.
KMS ist nicht konfiguriert	Für diese Site ist kein Schlüsselverwaltungsserver vorhanden.

Name der Warnung	Beschreibung
KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln	Ein oder mehrere Volumes auf einer Appliance mit aktivierter Knotenverschlüsselung konnten mit dem aktuellen KMS-Schlüssel nicht entschlüsselt werden.
Ablauf des KMS-Serverzertifikats	Das vom Schlüsselverwaltungsserver (KMS) verwendete Serverzertifikat läuft bald ab.
KMS-Server-Konnektivitätsfehler	Ein Appliance-Knoten konnte keine Verbindung zu einem oder mehreren Servern im Schlüsselverwaltungsserver-Cluster für seine Site herstellen.

Load Balancer-Warnungen

Name der Warnung	Beschreibung
Erhöhte Zero-Request-Load-Balancer-Verbindungen	Ein erhöhter Prozentsatz der Verbindungen zu Load Balancer-Endpunkten wurde getrennt, ohne dass Anforderungen ausgeführt wurden.

Warnungen bei lokalem Zeitversatz

Name der Warnung	Beschreibung
Großer Zeitversatz der lokalen Uhr	Der Offset zwischen der lokalen Uhr und der Network Time Protocol (NTP)-Zeit ist zu groß.

Warnungen bei zu wenig Arbeitsspeicher oder Speicherplatz

Name der Warnung	Beschreibung
Geringe Festplattenkapazität für Überwachungsprotokolle	Der für Audit-Protokolle verfügbare Speicherplatz ist gering. Wenn dieser Zustand nicht behoben wird, können S3- oder Swift-Vorgänge fehlschlagen.
Wenig verfügbarer Knotenspeicher	Die auf einem Knoten verfügbare RAM-Menge ist gering.
Wenig freier Speicherplatz für Speicherpool	Der zum Speichern von Objektdaten im Speicherknoten verfügbare Speicherplatz ist gering.
Wenig installierter Knotenspeicher	Die Menge des auf einem Knoten installierten Speichers ist gering.
Geringe Speicherung von Metadaten	Der zum Speichern von Objektmetadaten verfügbare Speicherplatz ist gering.
Niedrige Metrik-Festplattenkapazität	Der für die Metrikdatenbank verfügbare Speicherplatz ist gering.

Name der Warnung	Beschreibung
Geringe Objektdatenspeicherung	Der zum Speichern von Objektdaten verfügbare Speicherplatz ist gering.
Niedrige schreibgeschützte Wasserzeichenüberschreibung	Die Soft-Read-Only-Wasserzeichenüberschreibung des Speichervolumes ist kleiner als das minimal optimierte Wasserzeichen für einen Speicherknoten.
Geringe Root-Disk-Kapazität	Der auf der Root-Festplatte verfügbare Speicherplatz ist gering.
Geringe Systemdatenkapazität	Der für /var/local verfügbare Speicherplatz ist gering. Wenn dieser Zustand nicht behoben wird, können S3- oder Swift-Vorgänge fehlschlagen.
Wenig freier Speicherplatz im temporären Verzeichnis	Im Verzeichnis /tmp ist nur noch wenig Speicherplatz verfügbar.

Knoten- oder Knotennetzwerkwarnungen

Name der Warnung	Beschreibung
Empfangsnutzung des Admin-Netzwerks	Die Empfangsnutzung im Admin-Netzwerk ist hoch.
Übertragungsnutzung des Admin-Netzwerks	Die Übertragungsnutzung im Admin-Netzwerk ist hoch.
Firewall-Konfigurationsfehler	Die Firewall-Konfiguration konnte nicht angewendet werden.
Management-Schnittstellenendpunkte im Fallback-Modus	Alle Endpunkte der Verwaltungsschnittstelle sind zu lange auf die Standardports zurückgefallen.
Knotennetzwerk-Konnektivitätsfehler	Beim Übertragen der Daten zwischen den Knoten sind Fehler aufgetreten.
Fehler beim Empfang des Knotennetzwerk-Frames	Ein hoher Prozentsatz der von einem Knoten empfangenen Netzwerk-Frames war fehlerhaft.
Knoten nicht mit NTP-Server synchronisiert	Der Knoten ist nicht mit dem Network Time Protocol (NTP)-Server synchronisiert.
Knoten nicht mit NTP-Server gesperrt	Der Knoten ist nicht an einen NTP-Server (Network Time Protocol) gebunden.
Nicht-Appliance-Knotennetzwerk ausgefallen	Ein oder mehrere Netzwerkgeräte sind ausgefallen oder getrennt.

Name der Warnung	Beschreibung
Verbindung zur Dienst-Appliance im Admin-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Verbindung der Services-Appliance auf Admin-Netzwerkport 1 unterbrochen	Der Admin-Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung zur Dienst-Appliance im Client-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 1 unterbrochen	Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 2 unterbrochen	Netzwerkport 2 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 3 unterbrochen	Netzwerkport 3 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 4 unterbrochen	Netzwerkport 4 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung zur Speicher-Appliance im Admin-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Verbindung zur Speicher-Appliance auf Admin-Netzwerk-Port 1 unterbrochen	Der Admin-Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung zur Speicher-Appliance im Client-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 1 unterbrochen	Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 2 unterbrochen	Netzwerkport 2 auf dem Gerät ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 3 unterbrochen	Netzwerkport 3 auf dem Gerät ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 4 unterbrochen	Netzwerkport 4 auf dem Gerät ist ausgefallen oder getrennt.

Name der Warnung	Beschreibung
Speicherknoten nicht im gewünschten Speicherzustand	Der LDR-Dienst auf einem Speicherknoten kann aufgrund eines internen Fehlers oder eines Volume-bezogenen Problems nicht in den gewünschten Zustand wechseln
TCP-Verbindungsnutzung	Die Anzahl der TCP-Verbindungen auf diesem Knoten nähert sich der maximalen Anzahl, die verfolgt werden kann.
Kommunikation mit Knoten nicht möglich	Ein oder mehrere Dienste reagieren nicht oder der Knoten kann nicht erreicht werden.
Unerwarteter Neustart des Knotens	Ein Knoten wurde innerhalb der letzten 24 Stunden unerwartet neu gestartet.

Objektwarnungen

Name der Warnung	Beschreibung
Objekt-Existenzprüfung fehlgeschlagen	Der Job zur Überprüfung der Objektexistenz ist fehlgeschlagen.
Objekt-Existenzprüfung angehalten	Der Job zur Überprüfung der Objektexistenz ist ins Stocken geraten.
Verlorene Gegenstände	Ein oder mehrere Objekte sind aus dem Raster verloren gegangen.
S3 PUT-Objektgröße zu groß	Ein Client versucht einen PUT-Objektvorgang, der die S3-Größenbeschränkungen überschreitet.
Unbekanntes beschädigtes Objekt erkannt	Im replizierten Objektspeicher wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte.

Warnungen zu Plattformdiensten

Name der Warnung	Beschreibung
Niedrige Kapazität für ausstehende Anfragen der Plattformdienste	Die Anzahl der ausstehenden Anfragen der Plattformdienste nähert sich der Kapazitätsgrenze.
Plattformdienste nicht verfügbar	An einem Standort sind zu wenige Speicherknoten mit dem RSM-Dienst aktiv oder verfügbar.

Speichervolumenwarnungen

Name der Warnung	Beschreibung
Speichervolumen erfordert Aufmerksamkeit	Ein Speichervolume ist offline und erfordert Aufmerksamkeit.

Name der Warnung	Beschreibung
Speichervolumen muss wiederhergestellt werden	Ein Speichervolume wurde wiederhergestellt und muss wiederhergestellt werden.
Speichervolume offline	Ein Speichervolume war länger als 5 Minuten offline.
Es wurde versucht, das Speichervolume erneut zu mounten.	Ein Speichervolume war offline und löste eine automatische Neubereitstellung aus. Dies könnte auf ein Laufwerksproblem oder Dateisystemfehler hinweisen.
Bei der Volume-Wiederherstellung konnte die Reparatur replizierter Daten nicht gestartet werden.	Die Reparatur replizierter Daten für ein repariertes Volume konnte nicht automatisch gestartet werden.

Warnungen zu StorageGRID -Diensten

Name der Warnung	Beschreibung
Nginx-Dienst mit Backup-Konfiguration	Die Konfiguration des Nginx-Dienstes ist ungültig. Es wird nun die vorherige Konfiguration verwendet.
nginx-gw-Dienst mit Backup-Konfiguration	Die Konfiguration des nginx-gw-Dienstes ist ungültig. Es wird nun die vorherige Konfiguration verwendet.
Zum Deaktivieren von FIPS ist ein Neustart erforderlich	Die Sicherheitsrichtlinie erfordert keinen FIPS-Modus, aber das NetApp Cryptographic Security Module ist aktiviert.
Neustart erforderlich, um FIPS zu aktivieren	Die Sicherheitsrichtlinie erfordert den FIPS-Modus, aber das NetApp Cryptographic Security Module ist deaktiviert.
SSH-Dienst mit Sicherungskonfiguration	Die Konfiguration des SSH-Dienstes ist ungültig. Es wird nun die vorherige Konfiguration verwendet.

Mieterwarnungen

Name der Warnung	Beschreibung
Hohe Auslastung des Mandantenkontingents	Ein hoher Prozentsatz des Kontingentplatzes wird genutzt. Diese Regel ist standardmäßig deaktiviert, da sie zu viele Benachrichtigungen verursachen könnte.

Häufig verwendete Prometheus-Metriken

Sehen Sie sich diese Liste häufig verwendeter Prometheus-Metriken an, um die Bedingungen in den Standardwarnregeln besser zu verstehen oder die Bedingungen für benutzerdefinierte Warnregeln zu erstellen.

Sie können auch Erhalten Sie eine vollständige Liste aller Metriken .

Einzelheiten zur Syntax von Prometheus-Abfragen finden Sie unter "Abfragen von Prometheus" .

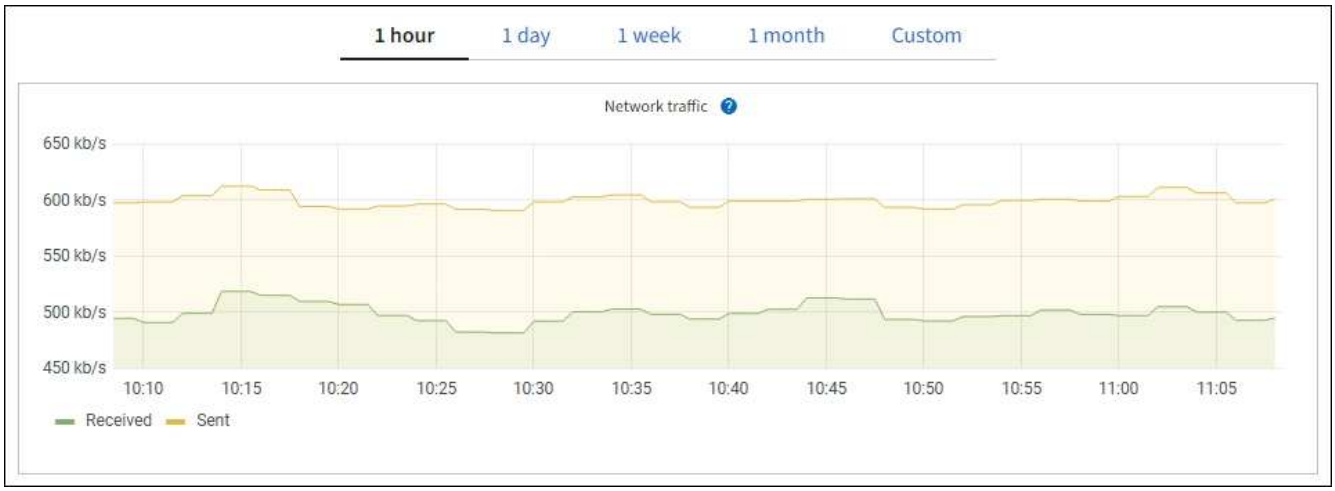
Was sind Prometheus-Metriken?

Prometheus-Metriken sind Zeitreihenmessungen. Der Prometheus-Dienst auf Admin-Knoten sammelt diese Metriken von den Diensten auf allen Knoten. Auf jedem Admin-Knoten werden Metriken gespeichert, bis der für Prometheus-Daten reservierte Speicherplatz voll ist. Wenn die `/var/local/mysql_ibdata/` Wenn das Volume die Kapazität erreicht, werden die ältesten Metriken zuerst gelöscht.

Wo werden Prometheus-Metriken verwendet?

Die von Prometheus gesammelten Metriken werden an mehreren Stellen im Grid Manager verwendet:

- **Knotenseite**: Die Grafiken und Diagramme auf den Registerkarten, die auf der Knotenseite verfügbar sind, verwenden das Grafana-Visualisierungstool, um die von Prometheus gesammelten Zeitreihenmetriken anzuzeigen. Grafana zeigt Zeitreihendaten in Diagramm- und Chartformaten an, während Prometheus als Backend-Datenquelle dient.



- **Warnungen**: Warnungen werden bei bestimmten Schweregraden ausgelöst, wenn Warnregelbedingungen, die Prometheus-Metriken verwenden, als wahr ausgewertet werden.
- **Grid Management API**: Sie können Prometheus-Metriken in benutzerdefinierten Warnregeln oder mit externen Automatisierungstools verwenden, um Ihr StorageGRID System zu überwachen. Eine vollständige Liste der Prometheus-Metriken ist über die Grid Management API verfügbar. (Wählen Sie oben im Grid Manager das Hilfesymbol und dann **API-Dokumentation** > **Metriken** aus.) Obwohl mehr als tausend Metriken verfügbar sind, wird nur eine relativ kleine Anzahl benötigt, um die kritischsten StorageGRID Vorgänge zu überwachen.

> Metriken, deren Namen „*private*“ enthalten, sind nur für den internen Gebrauch bestimmt und können zwischen StorageGRID Versionen ohne Vorankündigung geändert werden.

- Die Seite **SUPPORT** > **Tools** > **Diagnose** und die Seite **SUPPORT** > **Tools** > **Metriken**: Diese Seiten, die in erster Linie für den technischen Support vorgesehen sind, bieten mehrere Tools und Diagramme, die die Werte der Prometheus-Metriken verwenden.

> Einige Funktionen und Menüelemente auf der Seite „Metriken“ sind absichtlich nicht funktionsfähig und können sich ändern.

Liste der gängigsten Metriken

Die folgende Liste enthält die am häufigsten verwendeten Prometheus-Metriken.

> Metriken, deren Namen „*private*“ enthalten, sind nur für den internen Gebrauch bestimmt und können zwischen den StorageGRID Versionen ohne vorherige Ankündigung geändert werden.

alertmanager_notifications_failed_total
Die Gesamtzahl der fehlgeschlagenen Warnbenachrichtigungen.

node_filesystem_avail_bytes
Die Menge an Dateisystemspeicherplatz, die Nicht-Root-Benutzern in Bytes zur Verfügung steht.

node_memory_MemAvailable_bytes
Speicherinformationsfeld MemAvailable_bytes.

Knotennetzwerkträger
Trägerwert von `/sys/class/net/iface`.

node_network_receive_errs_total
Netzwerkgerätestatistik `receive_errs`.

node_network_transmit_errs_total
Netzwerkgerätestatistik `transmit_errs`.

storagegrid_administratively_down
Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert.

storagegrid_appliance_compute_controller_hardware_status
Der Status der Compute-Controller-Hardware in einem Gerät.

storagegrid_appliance_failed_disks
Für den Speichercontroller in einem Gerät die Anzahl der Laufwerke, die nicht optimal sind.

storagegrid_appliance_storage_controller_hardware_status
Der Gesamtstatus der Speichercontroller-Hardware in einer Appliance.

storagegrid_content_buckets_and_containers
Die Gesamtzahl der diesem Speicherknoten bekannten S3-Buckets und Swift-Container.

storagegrid_content_objects
Die Gesamtzahl der diesem Speicherknoten bekannten S3- und Swift-Datenobjekte. Die Anzahl ist nur für Datenobjekte gültig, die von Clientanwendungen erstellt wurden, die über S3 mit dem System kommunizieren.

storagegrid_content_objects_lost
Die Gesamtzahl der Objekte, die dieser Dienst als im StorageGRID -System fehlend erkennt. Es sollten Maßnahmen ergriffen werden, um die Ursache des Verlusts zu ermitteln und festzustellen, ob eine Wiederherstellung möglich ist.

"Fehlerbehebung bei verlorenen und fehlenden Objektdaten"

storagegrid_http_sessions_incoming_attempted

Die Gesamtzahl der HTTP-Sitzungen, die mit einem Speicherknoten versucht wurden.

storagegrid_http_sessions_incoming_currently_established

Die Anzahl der HTTP-Sitzungen, die derzeit auf dem Speicherknoten aktiv (offen) sind.

storagegrid_http_sessions_incoming_failed

Die Gesamtzahl der HTTP-Sitzungen, die nicht erfolgreich abgeschlossen werden konnten, entweder aufgrund einer fehlerhaften HTTP-Anforderung oder eines Fehlers bei der Verarbeitung eines Vorgangs.

storagegrid_http_sessions_incoming_successful

Die Gesamtzahl der HTTP-Sitzungen, die erfolgreich abgeschlossen wurden.

storagegrid_ilm_awaiting_background_objects

Die Gesamtzahl der Objekte auf diesem Knoten, die auf die ILM-Auswertung des Scans warten.

storagegrid_ilm_awaiting_client_evaluation_objects_per_second

Die aktuelle Rate, mit der Objekte anhand der ILM-Richtlinie auf diesem Knoten ausgewertet werden.

storagegrid_ilm_awaiting_client_objects

Die Gesamtzahl der Objekte auf diesem Knoten, die auf die ILM-Auswertung von Clientvorgängen (z. B. Aufnahme) warten.

storagegrid_ilm_awaiting_total_objects

Die Gesamtzahl der Objekte, die auf die ILM-Auswertung warten.

storagegrid_ilm_scan_objects_per_second

Die Rate, mit der Objekte, die diesem Knoten gehören, gescannt und für ILM in die Warteschlange gestellt werden.

storagegrid_ilm_scan_period_estimated_minutes

Die geschätzte Zeit zum Abschließen eines vollständigen ILM-Scans auf diesem Knoten.

Hinweis: Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde, die diesem Knoten gehören.

storagegrid_load_balancer_endpoint_cert_expiry_time

Die Ablaufzeit des Load Balancer-Endpunktzertifikats in Sekunden seit der Epoche.

storagegrid_metadata_queries_average_latency_milliseconds

Die durchschnittliche Zeit, die zum Ausführen einer Abfrage des Metadatenspeichers über diesen Dienst benötigt wird.

storagegrid_network_received_bytes

Die Gesamtmenge der seit der Installation empfangenen Daten.

storagegrid_network_transmitted_bytes

Die Gesamtmenge der seit der Installation gesendeten Daten.

storagegrid_node_cpu_utilization_percentage

Der Prozentsatz der verfügbaren CPU-Zeit, die derzeit von diesem Dienst verwendet wird. Gibt an, wie ausgelastet der Dienst ist. Die Menge der verfügbaren CPU-Zeit hängt von der Anzahl der CPUs des Servers ab.

storagegrid_ntp_chosen_time_source_offset_milliseconds

Systematischer Zeitversatz durch eine ausgewählte Zeitquelle. Ein Offset wird eingeführt, wenn die Verzögerung zum Erreichen einer Zeitquelle nicht der Zeit entspricht, die die Zeitquelle benötigt, um den NTP-Client zu erreichen.

storagegrid_ntp_locked

Der Knoten ist nicht an einen Network Time Protocol (NTP)-Server gebunden.

storagegrid_s3_data_transfers_bytes_ingested

Die Gesamtmenge der von S3-Clients in diesen Speicherknoten aufgenommenen Daten seit der letzten Zurücksetzung des Attributs.

storagegrid_s3_data_transfers_bytes_retrieved

Die Gesamtmenge der von S3-Clients von diesem Speicherknoten abgerufenen Daten seit der letzten Zurücksetzung des Attributs.

storagegrid_s3_operations_failed

Die Gesamtzahl der fehlgeschlagenen S3-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen derjenigen, die durch einen S3-Autorisierungsfehler verursacht wurden.

storagegrid_s3_operations_successful

Die Gesamtzahl der erfolgreichen S3-Operationen (HTTP-Statuscode 2xx).

storagegrid_s3_operations_unauthorized

Die Gesamtzahl der fehlgeschlagenen S3-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind.

storagegrid_servercertificate_management_interface_cert_expiry_days

Die Anzahl der Tage bis zum Ablauf des Management Interface-Zertifikats.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

Die Anzahl der Tage bis zum Ablauf des Object Storage API-Zertifikats.

storagegrid_service_cpu_seconds

Die kumulative Zeit, die die CPU seit der Installation von diesem Dienst verwendet wurde.

storagegrid_service_memory_usage_bytes

Die Menge an Arbeitsspeicher (RAM), die derzeit von diesem Dienst verwendet wird. Dieser Wert ist identisch mit dem Wert, der vom Linux-Dienstprogramm „top“ als RES angezeigt wird.

storagegrid_service_network_received_bytes

Die Gesamtmenge der von diesem Dienst seit der Installation empfangenen Daten.

storagegrid_service_network_transmitted_bytes

Die Gesamtmenge der von diesem Dienst gesendeten Daten.

storagegrid_service_restarts

Die Gesamtzahl der Neustarts des Dienstes.

storagegrid_service_runtime_seconds

Die Gesamtzeit, die der Dienst seit der Installation ausgeführt wurde.

storagegrid_service_uptime_seconds

Die Gesamtzeit, die der Dienst seit dem letzten Neustart ausgeführt wurde.

storagegrid_storage_state_current

Der aktuelle Status der Speicherdienste. Attributwerte sind:

- 10 = Offline
- 15 = Wartung
- 20 = Schreibgeschützt
- 30 = Online

storagegrid_storage_status

Der aktuelle Status der Speicherdienste. Attributwerte sind:

- 0 = Keine Fehler
- 10 = Im Übergang
- 20 = Nicht genügend freier Speicherplatz
- 30 = Datenträger nicht verfügbar
- 40 = Fehler

storagegrid_storage_utilization_data_bytes

Eine Schätzung der Gesamtgröße der replizierten und löschcodierten Objektdaten auf dem Speicherknoten.

storagegrid_storage_utilization_metadata_allowed_bytes

Der Gesamtspeicherplatz auf Volume 0 jedes Speicherknotens, der für Objektmetadaten zulässig ist. Dieser Wert ist immer kleiner als der tatsächliche Speicherplatz, der für Metadaten auf einem Knoten reserviert ist, da ein Teil des reservierten Speicherplatzes für wichtige Datenbankvorgänge (wie Komprimierung und Reparatur) und zukünftige Hardware- und Software-Upgrades benötigt wird. Der zulässige Speicherplatz für Objektmetadaten steuert die Gesamtobjektkapazität.

storagegrid_storage_utilization_metadata_bytes

Die Menge der Objektmetadaten auf Speichervolume 0 in Bytes.

storagegrid_storage_utilization_total_space_bytes

Die Gesamtmenge an Speicherplatz, die allen Objektspeichern zugewiesen ist.

storagegrid_storage_utilization_usable_space_bytes

Die Gesamtmenge des verbleibenden Objektspeicherplatzes. Berechnet durch Addition des verfügbaren Speicherplatzes für alle Objektspeicher auf dem Speicherknoten.

storagegrid_swift_data_transfers_bytes_ingested

Die Gesamtmenge der von Swift-Clients in diesen Speicherknoten aufgenommenen Daten seit der letzten

Zurücksetzung des Attributs.

storagegrid_swift_data_transfers_bytes_retrieved
Die Gesamtmenge der von Swift-Clients von diesem Speicherknoten abgerufenen Daten seit der letzten Zurücksetzung des Attributs.

storagegrid_swift_operations_failed
Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen derjenigen, die durch einen Swift-Autorisierungsfehler verursacht wurden.

storagegrid_swift_operations_successful
Die Gesamtzahl der erfolgreichen Swift-Operationen (HTTP-Statuscode 2xx).

storagegrid_swift_operations_unauthorized
Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind (HTTP-Statuscodes 401, 403, 405).

storagegrid_tenant_usage_data_bytes
Die logische Größe aller Objekte für den Mandanten.

storagegrid_tenant_usage_object_count
Die Anzahl der Objekte für den Mandanten.

storagegrid_tenant_usage_quota_bytes
Die maximale Menge an logischem Speicherplatz, der für die Objekte des Mandanten verfügbar ist. Wenn keine Kontingentmetrik angegeben ist, steht unbegrenzter Speicherplatz zur Verfügung.

Holen Sie sich eine Liste aller Metriken

Um die vollständige Liste der Metriken zu erhalten, verwenden Sie die Grid Management API.

1. Wählen Sie oben im Grid Manager das Hilfesymbol und dann **API-Dokumentation** aus.
2. Suchen Sie die **Metriken**-Operationen.
3. Führen Sie den `GET /grid/metric-names` Betrieb.
4. Laden Sie die Ergebnisse herunter.

Referenz zu Protokolldateien

Referenz zu Protokolldateien

StorageGRID bietet Protokolle, die zum Erfassen von Ereignissen, Diagnosemeldungen und Fehlerzuständen verwendet werden. Möglicherweise werden Sie gebeten, Protokolldateien zu sammeln und sie an den technischen Support weiterzuleiten, um bei der Fehlerbehebung zu helfen.

Die Protokolle sind wie folgt kategorisiert:

- "StorageGRID -Softwareprotokolle"
- "Bereitstellungs- und Wartungsprotokolle"
- "Über das bycast.log"

Die für jeden Protokolltyp bereitgestellten Details dienen nur als Referenz. Die Protokolle sind für die erweiterte Fehlerbehebung durch den technischen Support vorgesehen. Fortgeschrittene Techniken, bei denen der Problemverlauf mithilfe der Prüfprotokolle und der Anwendungsprotokolldateien rekonstruiert wird, gehen über den Rahmen dieser Anweisungen hinaus.

Zugriff auf die Protokolle

Um auf die Protokolle zuzugreifen, können Sie"Sammeln von Protokolldateien und Systemdaten" von einem oder mehreren Knoten als einzelnes Protokolldateiarchiv. Oder wenn der primäre Admin-Knoten nicht verfügbar ist oder einen bestimmten Knoten nicht erreichen kann, können Sie wie folgt auf einzelne Protokolldateien für jeden Grid-Knoten zugreifen:

1. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
2. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
3. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
4. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

Exportieren Sie Protokolle auf den Syslog-Server

Das Exportieren der Protokolle auf den Syslog-Server bietet folgende Möglichkeiten:

- Erhalten Sie eine Liste aller Grid Manager- und Tenant Manager-Anfragen sowie S3- und Swift-Anfragen.
- Bessere Transparenz bei S3-Anfragen, die Fehler zurückgeben, ohne die durch Audit-Protokollierungsmethoden verursachten Leistungseinbußen.
- Zugriff auf HTTP-Layer-Anfragen und Fehlercodes, die leicht zu analysieren sind.
- Bessere Transparenz bei Anfragen, die von Verkehrsklassifizierern beim Load Balancer blockiert wurden.

Informationen zum Exportieren der Protokolle finden Sie unter"Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Protokolldateikategorien

Das StorageGRID Protokolldateiarchiv enthält die für jede Kategorie beschriebenen Protokolle und zusätzliche Dateien, die Metriken und die Ausgabe von Debugbefehlen enthalten.

Archivspeicherort	Beschreibung
Prüfung	Während des normalen Systembetriebs generierte Prüfmeldungen.
Basis-Betriebssystem-Protokolle	Grundlegende Informationen zum Betriebssystem, einschließlich StorageGRID Image-Versionen.
Bündel	Globale Konfigurationsinformationen (Bundles).
Kassandra	Cassandra-Datenbankinformationen und Reaper-Reparaturprotokolle.

Archivspeicherort	Beschreibung
ec	VCS-Informationen zum aktuellen Knoten und EC-Gruppeninformationen nach Profil-ID.
Netz	Allgemeine Grid-Protokolle einschließlich Debug(`bycast.log`) Und `servermanager` Protokolle.
grid.json	Von allen Knoten gemeinsam genutzte Grid-Konfigurationsdatei. Zusätzlich, `node.json` ist spezifisch für den aktuellen Knoten.
hagroups	Metriken und Protokolle für Hochverfügbarkeitsgruppen.
installieren	`Gdu-server`und Protokolle installieren.
Lambda-Schiedsrichter	Protokolle im Zusammenhang mit der S3 Select-Proxy-Anforderung.
lumberjack.log	Debug-Meldungen im Zusammenhang mit der Protokollsammlung.
Metriken	Serviceprotokolle für Grafana, Jaeger, Node Exporter und Prometheus.
Sonstiges	Verschiedene Zugriffs- und Fehlerprotokolle.
MySQL	Die MariaDB-Datenbankkonfiguration und zugehörige Protokolle.
netto	Von netzwerkbezogenen Skripten und dem Dynip-Dienst generierte Protokolle.
nginx	Konfigurationsdateien und Protokolle für Load Balancer und Grid-Föderation. Enthält auch Grid Manager- und Tenant Manager-Verkehrsprotokolle.

Archivspeicherort	Beschreibung
nginx-gw	• `access.log`: Grid Manager und Tenant Manager fordern Protokollnachrichten an. ◦ Diesen Nachrichten vorangestellt ist `mgmt:` beim Exportieren mit Syslog. ◦ Das Format dieser Protokollnachrichten ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: Eingehende Cross-Grid-Replikationsanforderungen. ◦ Diesen Nachrichten vorangestellt ist `cgr:` beim Exportieren mit Syslog. ◦ Das Format dieser Protokollnachrichten ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: S3- und Swift-Anfragen an Load Balancer-Endpunkte. ◦ Diesen Nachrichten vorangestellt ist `endpoint:` beim Exportieren mit Syslog. ◦ Das Format dieser Protokollnachrichten ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Bezieht sich auf die neue DNS-Check-Warnung.
ntp	NTP-Konfigurationsdatei und -Protokolle.
Verwaiste Objekte	Protokolle zu verwaisten Objekten.
Betriebssystem	Knoten- und Netzzustandsdatei, einschließlich Dienste `pid` .
andere	Protokolldateien unter `/var/local/log` die nicht in anderen Ordnern gesammelt werden.
Leistung	Leistungsinformationen zu CPU, Netzwerk und Festplatten-E/A.
Prometheus-Daten	Aktuelle Prometheus-Metriken, wenn die Protokollsammlung Prometheus-Daten enthält.
Bereitstellung	Protokolle im Zusammenhang mit dem Grid-Bereitstellungsprozess.
Floß	Protokolle vom Raft-Cluster, die in Plattformdiensten verwendet werden.

Archivspeicherort	Beschreibung
ssh	Protokolle im Zusammenhang mit der SSH-Konfiguration und dem SSH-Dienst.
SNMP	SNMP-Agentenkonfiguration zum Senden von SNMP-Benachrichtigungen.
Sockets-Daten	Socket-Daten für die Netzwerkfehlerbehebung.
system-commands.txt	Ausgabe von StorageGRID Containerbefehlen. Enthält Systeminformationen, beispielsweise zur Netzwerk- und Festplattennutzung.
Synchronisierungs-Wiederherstellungspaket	Bezieht sich auf die Aufrechterhaltung der Konsistenz des neuesten Wiederherstellungspakets auf allen Admin-Knoten und Speicherknoten, die den ADC-Dienst hosten.

StorageGRID -Softwareprotokolle

Sie können StorageGRID Protokolle zur Fehlerbehebung verwenden.

Wenn Sie Ihre Protokolle an einen externen Syslog-Server senden oder das Ziel der Audit-Informationen ändern möchten, wie z. B. die `bycast.log` Und `nms.log` , sehen"Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Allgemeine StorageGRID Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/bycast.log	Die primäre StorageGRID Fehlerbehebungsdatei. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events**.	Alle Knoten
/var/local/log/bycast-err.log	Enthält eine Teilmenge von `bycast.log` (Meldungen mit Schweregrad ERROR und CRITICAL). Außerdem werden im System KRITISCHE Meldungen angezeigt. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events**.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/core/	Enthält alle Core-Dump-Dateien, die bei einer abnormalen Programmbeendigung erstellt werden. Mögliche Ursachen sind Assertionsfehler, Verstöße oder Thread-Timeouts. **Hinweis**: Die Datei `/var/local/core/kexec_cmd` ist normalerweise auf Appliance-Knoten vorhanden und weist nicht auf einen Fehler hin.	Alle Knoten

Verschlüsselungsbezogene Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/ssh-config-generation.log	Enthält Protokolle im Zusammenhang mit der Generierung von SSH-Konfigurationen und dem Neuladen von SSH-Diensten.	Alle Knoten
/var/local/log/nginx/config-generation.log	Enthält Protokolle im Zusammenhang mit der Generierung von Nginx-Konfigurationen und dem Neuladen von Nginx-Diensten.	Alle Knoten
/var/local/log/nginx-gw/config-generation.log	Enthält Protokolle im Zusammenhang mit der Generierung von nginx-gw-Konfigurationen (und dem Neuladen von nginx-gw-Diensten).	Admin- und Gateway-Knoten
/var/local/log/update-cipher-configurations.log	Enthält Protokolle im Zusammenhang mit der Konfiguration von TLS- und SSH-Richtlinien.	Alle Knoten

Grid-Föderationsprotokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/update_grid_federation_config.log	Enthält Protokolle im Zusammenhang mit der Generierung von Nginx- und Nginx-GW-Konfigurationen für Grid-Föderationsverbindungen.	Alle Knoten

NMS-Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/nms.log	• Erfasst Benachrichtigungen vom Grid Manager und Tenant Manager. • Erfasst Ereignisse im Zusammenhang mit dem Betrieb des NMS-Dienstes. Zum Beispiel E-Mail-Benachrichtigungen und Konfigurationsänderungen. • Enthält XML-Bundle-Updates, die sich aus im System vorgenommenen Konfigurationsänderungen ergeben. • Enthält Fehlermeldungen im Zusammenhang mit dem einmal täglich durchgeführten Downsampling der Attribute. • Enthält Fehlermeldungen des Java-Webservers, beispielsweise Fehler bei der Seitengenerierung und HTTP-Status 500-Fehler.	Admin-Knoten
/var/local/log/nms.errlog	Enthält Fehlermeldungen im Zusammenhang mit MySQL-Datenbank-Upgrades. Enthält den Standardfehler-Stream (stderr) der entsprechenden Dienste. Es gibt eine Protokolldatei pro Dienst. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Admin-Knoten
/var/local/log/nms.requestlog	Enthält Informationen zu ausgehenden Verbindungen von der Management-API zu internen StorageGRID Diensten.	Admin-Knoten

Server Manager-Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/servermanager.log	Protokolldatei für die auf dem Server ausgeführte Server Manager-Anwendung.	Alle Knoten
/var/local/log/GridstatBackend.errlog	Protokolldatei für die Server Manager-GUI-Backend-Anwendung.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/gridstat.errlog	Protokolldatei für die Server Manager-GUI.	Alle Knoten

StorageGRID -Dienstprotokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/acct.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/adc.errlog	Enthält den Standardfehler-Stream (stderr) der entsprechenden Dienste. Es gibt eine Protokolldatei pro Dienst. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/ams.errlog		Admin-Knoten
/var/local/log/cassandra/system.log	Informationen zum Metadatenspeicher (Cassandra-Datenbank), die verwendet werden können, wenn beim Hinzufügen neuer Speicherknoten Probleme auftreten oder die Nodetool-Reparaturaufgabe hängen bleibt.	Speicherknoten
/var/local/log/cassandra-reaper.log	Informationen zum Cassandra Reaper-Dienst, der Reparaturen der Daten in der Cassandra-Datenbank durchführt.	Speicherknoten
/var/local/log/cassandra-reaper.errlog	Fehlerinformationen für den Cassandra Reaper-Dienst.	Speicherknoten
/var/local/log/chunk.errlog		Speicherknoten
/var/local/log/cmn.errlog		Admin-Knoten
/var/local/log/cms.errlog	Diese Protokolldatei ist möglicherweise auf Systemen vorhanden, die von einer älteren Version von StorageGRID aktualisiert wurden. Es enthält Legacy-Informationen.	Speicherknoten
/var/local/log/dds.errlog		Speicherknoten
/var/local/log/dmv.errlog		Speicherknoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/dynip*	Enthält Protokolle im Zusammenhang mit dem Dynip-Dienst, der das Grid auf dynamische IP-Änderungen überwacht und die lokale Konfiguration aktualisiert.	Alle Knoten
/var/local/log/grafana.log	Das mit dem Grafana-Dienst verknüpfte Protokoll, das zur Visualisierung von Metriken im Grid Manager verwendet wird.	Admin-Knoten
/var/local/log/hagroups.log	Das mit Hochverfügbarkeitsgruppen verknüpfte Protokoll.	Admin-Knoten und Gateway-Knoten
/var/local/log/hagroups_events.log	Verfolgt Statusänderungen, wie etwa den Übergang von BACKUP zu MASTER oder FAULT.	Admin-Knoten und Gateway-Knoten
/var/local/log/idnt.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/jaeger.log	Das mit dem Jaeger-Dienst verknüpfte Protokoll, das zur Ablaufverfolgung verwendet wird.	Alle Knoten
/var/local/log/kstn.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/lambda*	Enthält Protokolle für den S3 Select-Dienst.	Admin- und Gateway-Knoten Nur bestimmte Admin- und Gateway-Knoten enthalten dieses Protokoll. Siehe die"S3 Select-Anforderungen und -Einschränkungen für Admin- und Gateway-Knoten" .
/var/local/log/ldr.errlog		Speicherknoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/miscd/*.log	Enthält Protokolle für den MISCd-Dienst (Information Service Control Daemon), der eine Schnittstelle zum Abfragen und Verwalten von Diensten auf anderen Knoten und zum Verwalten von Umgebungskonfigurationen auf dem Knoten bereitstellt, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Knoten
/var/local/log/nginx/*.log	Enthält Protokolle für den Nginx-Dienst, der als Authentifizierungs- und sicherer Kommunikationsmechanismus für verschiedene Grid-Dienste (wie Prometheus und Dynip) fungiert, um über HTTPS-APIs mit Diensten auf anderen Knoten kommunizieren zu können.	Alle Knoten
/var/local/log/nginx-gw/*.log	Enthält allgemeine Protokolle im Zusammenhang mit dem nginx-gw-Dienst, einschließlich Fehlerprotokollen und Protokollen für die eingeschränkten Admin-Ports auf Admin-Knoten.	Admin-Knoten und Gateway-Knoten
/var/local/log/nginx-gw/cgr-access.log.gz	Enthält Zugriffsprotokolle im Zusammenhang mit dem gitterübergreifenden Replikationsverkehr.	Admin-Knoten, Gateway-Knoten oder beides, basierend auf der Grid-Föderationskonfiguration. Wird nur im Zielraster für die rasterübergreifende Replikation gefunden.
/var/local/log/nginx-gw/endpoint-access.log.gz	Enthält Zugriffsprotokolle für den Load Balancer-Dienst, der den Lastenausgleich des S3-Verkehrs von Clients zu Speicherknoten bereitstellt.	Admin-Knoten und Gateway-Knoten
/var/local/log/persistenz*	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Stammfestplatte verwaltet, die über einen Neustart hinaus bestehen bleiben müssen.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/prometheus.log	Enthält für alle Knoten das Dienstprotokoll des Knotenexporters und das Dienstprotokoll des Ade-Exporter-Metriken. Enthält für Admin-Knoten auch Protokolle für die Dienste Prometheus und Alert Manager.	Alle Knoten
/var/local/log/raft.log	Enthält die Ausgabe der vom RSM-Dienst für das Raft-Protokoll verwendeten Bibliothek.	Speicherknoten mit RSM-Dienst
/var/local/log/rms.errlog	Enthält Protokolle für den Dienst Replicated State Machine Service (RSM), der für S3-Plattformdienste verwendet wird.	Speicherknoten mit RSM-Dienst
/var/local/log/ssm.errlog		Alle Knoten
/var/local/log/update-s3vs-domains.log	Enthält Protokolle im Zusammenhang mit der Verarbeitung von Updates für die Konfiguration der virtuell gehosteten S3-Domänennamen. Weitere Informationen finden Sie in den Anweisungen zum Implementieren von S3-Clientanwendungen.	Admin- und Gateway-Knoten
/var/local/log/update-snmp-firewall.*	Enthalten Protokolle zu den Firewall-Ports, die für SNMP verwaltet werden.	Alle Knoten
/var/local/log/update-sysl.log	Enthält Protokolle zu Änderungen an der Syslog-Konfiguration des Systems.	Alle Knoten
/var/local/log/update-traffic-classes.log	Enthält Protokolle im Zusammenhang mit Änderungen an der Konfiguration der Verkehrsklassifizierer.	Admin- und Gateway-Knoten
/var/local/log/update-utcn.log	Enthält Protokolle im Zusammenhang mit dem nicht vertrauenswürdigen Client-Netzwerkmodus auf diesem Knoten.	Alle Knoten

Ähnliche Informationen

- "Über das bycast.log"
- "Verwenden Sie die S3 REST-API"

Bereitstellungs- und Wartungsprotokolle

Sie können die Bereitstellungs- und Wartungsprotokolle zur Fehlerbehebung verwenden.

Dateiname	Hinweise	Gefunden auf
/var/local/log/install.log	Wird während der Softwareinstallation erstellt. Enthält eine Aufzeichnung der Installationsereignisse.	Alle Knoten
/var/local/log/expansion-progress.log	Im Zuge der Erweiterungsarbeiten entstanden. Enthält eine Aufzeichnung der Erweiterungsereignisse.	Speicherknoten
/var/local/log/pa-move.log	Erstellt während der Ausführung des `pa-move.sh` Skript.	Primärer Admin-Knoten
/var/local/log/pa-move-new_pa.log	Erstellt während der Ausführung des `pa-move.sh` Skript.	Primärer Admin-Knoten
/var/local/log/pa-move-old_pa.log	Erstellt während der Ausführung des `pa-move.sh` Skript.	Primärer Admin-Knoten
/var/local/log/gdu-server.log	Erstellt vom GDU-Dienst. Enthält Ereignisse im Zusammenhang mit Bereitstellungs- und Wartungsverfahren, die vom primären Admin-Knoten verwaltet werden.	Primärer Admin-Knoten
/var/local/log/send_admin_hw.log	Wird während der Installation erstellt. Enthält Debuginformationen zur Kommunikation eines Knotens mit dem primären Admin-Knoten.	Alle Knoten
/var/local/log/upgrade.log	Während des Software-Upgrades erstellt. Enthält eine Aufzeichnung der Software-Update-Ereignisse.	Alle Knoten

Über das bycast.log

Die Datei `/var/local/log/bycast.log` ist die primäre Fehlerbehebungsdatei für die StorageGRID -Software. Es gibt eine `bycast.log` Datei für jeden Rasterknoten. Die Datei enthält Nachrichten, die für diesen Grid-Knoten spezifisch sind.

Die Datei `/var/local/log/bycast-err.log` ist eine Teilmenge von `bycast.log` . Es enthält Meldungen mit den Schweregraden FEHLER und KRITISCH.

Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Dateirotation für bycast.log

Wenn die `bycast.log` Wenn die Datei 1 GB erreicht, wird die vorhandene Datei gespeichert und eine neue Protokolldatei gestartet.

Die gespeicherte Datei wird umbenannt `bycast.log.1` und die neue Datei heißt `bycast.log` . Wenn das neue `bycast.log` erreicht 1 GB, `bycast.log.1` wird umbenannt und komprimiert und wird `bycast.log.2.gz` , Und `bycast.log` wird umbenannt `bycast.log.1` .

Die Rotationsgrenze für `bycast.log` sind 21 Dateien. Als die 22. Version des `bycast.log` Datei erstellt wird, wird die älteste Datei gelöscht.

Die Rotationsgrenze für `bycast-err.log` sind sieben Dateien.

> Wenn eine Protokolldatei komprimiert wurde, dürfen Sie sie nicht an denselben Speicherort dekomprimieren, an dem sie geschrieben wurde. Das Dekomprimieren der Datei an denselben Speicherort kann die Protokollrotationsskripte beeinträchtigen.

Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Ähnliche Informationen

"Erfassen von Protokolldateien und Systemdaten"

Nachrichten im bycast.log

Nachrichten in `bycast.log` werden von der ADE (Asynchronous Distributed Environment) geschrieben. ADE ist die Laufzeitumgebung, die von den Diensten jedes Grid-Knotens verwendet wird.

Beispiel einer ADE-Nachricht:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE-Nachrichten enthalten die folgenden Informationen:

Nachrichtensegment	Wert im Beispiel
Knoten-ID	12455685
ADE-Prozess-ID	0357819531
Modulname	SVMR
Nachrichtenkennung	EVHR
UTC-Systemzeit	2019-05-05T27T17:10:29.784677 (JJJJ-MM-TTTHH:MM:SS.uuuuuu)
Schweregrad	FEHLER

Nachrichtensegment	Wert im Beispiel
Interne Trackingnummer	0906
Nachricht	SVMR: Integritätsprüfung auf Datenträger 3 ist mit der Begründung „TOUT“ fehlgeschlagen

Schweregrade der Nachrichten in bycast.log

Die Nachrichten in `bycast.log` werden Schweregrade zugewiesen.

Beispiel:

- **HINWEIS** – Ein Ereignis ist eingetreten, das aufgezeichnet werden sollte. Die meisten Protokollnachrichten befinden sich auf dieser Ebene.
- **WARNUNG** – Es ist ein unerwarteter Zustand aufgetreten.
- **FEHLER** – Es ist ein schwerwiegender Fehler aufgetreten, der den Betrieb beeinträchtigen wird.
- **KRITISCH** – Es ist ein anormaler Zustand aufgetreten, der den normalen Betrieb gestoppt hat. Sie sollten sich sofort um die zugrunde liegende Erkrankung kümmern.

Fehlercodes in `bycast.log`

Die meisten Fehlermeldungen in `bycast.log` enthalten Fehlercodes.

Die folgende Tabelle listet häufige nicht-numerische Codes in `bycast.log` Die genaue Bedeutung eines nicht numerischen Codes hängt vom Kontext ab, in dem er gemeldet wird.

Fehlercode	Bedeutung
SUCS	Kein Fehler
GERR	Unbekannt
CANC	Abgesagt
ABRT	Abgebrochen
TOUT	Time-out
INVL	Ungültig
NFND	Nicht gefunden
VERS	Version
KONF	Konfiguration

Fehlercode	Bedeutung
SCHEITERN	Fehlgeschlagen
ICPL	Unvollständig
ERLEDIGT	Erledigt
SUNV	Dienst nicht verfügbar

Die folgende Tabelle listet die numerischen Fehlercodes in `bycast.log` .

Fehlernummer	Fehlercode	Bedeutung
001	EPERM	Betrieb nicht zulässig
002	ENOENT	Keine solche Datei oder Verzeichnis
003	ESRCH	Kein solcher Prozess
004	EINTR	Unterbrochener Systemaufruf
005	EIO	E/A-Fehler
006	ENXIO	Kein solches Gerät oder keine solche Adresse
007	E2BIG	Argumentliste zu lang
008	ENOEXEC	Exec-Formatfehler
009	EBADF	Ungültige Dateinummer
010	ECHILD	Keine untergeordneten Prozesse
011	WIEDER	Versuchen Sie es erneut
012	ENOMEM	Nicht genügend Arbeitsspeicher
013	EACCES	Zugriff verweigert
014	EFAULT	Falsche Adresse
015	ENOTBLK	Blockgerät erforderlich
016	EBUSY	Gerät oder Ressource beschäftigt

Fehlernummer	Fehlercode	Bedeutung
017	EEXIST	Datei existiert
018	EXDEV	Geräteübergreifende Verknüpfung
019	ENODEV	Kein solches Gerät
020	ENOTDIR	Kein Verzeichnis
021	EISDIR	Ist ein Verzeichnis
022	EINVAL	Ungültiges Argument
023	ENFILE	Dateitabellenüberlauf
024	EMFILE	Zu viele geöffnete Dateien
025	ENOTTY	Keine Schreibmaschine
026	ETXTBSY	Textdatei belegt
027	EFBIG	Datei zu groß
028	ENOSPC	Kein Speicherplatz mehr auf dem Gerät
029	ESPEIPE	Unerlaubte Suche
030	EROFS	Schreibgeschütztes Dateisystem
031	EMLINK	Zu viele Links
032	EPIPE	Rohrbruch
033	EDOM	Mathematisches Argument außerhalb des Funktionsumfangs
034	ERANGE	Matheergebnis nicht darstellbar
035	EDEADLK	Es kommt zu einem Ressourcen-Deadlock
036	ENAMETOOLONG	Dateiname zu lang
037	ENOLCK	Keine Datensatzsperren verfügbar

Fehlernummer	Fehlercode	Bedeutung
038	ENOSYS	Funktion nicht implementiert
039	VERFÜHRUNG	Verzeichnis nicht leer
040	ELOOP	Zu viele symbolische Links gefunden
041		
042	ENOMSG	Keine Nachricht des gewünschten Typs
043	EIDRM	Kennung entfernt
044	EMHRNG	Kanalnummer außerhalb des gültigen Bereichs
045	EL2NSYNC	Ebene 2 nicht synchronisiert
046	EL3HLT	Level 3 gestoppt
047	EL3RST	Level 3 zurücksetzen
048	ELNRNG	Linknummer außerhalb des gültigen Bereichs
049	EUNATCH	Protokolltreiber nicht angeschlossen
050	ENOCSI	Keine CSI-Struktur verfügbar
051	EL2HLT	Level 2 gestoppt
052	EBADE	Ungültiger Umtausch
053	EBADR	Ungültiger Anforderungsdeskriptor
054	EXFULL	Austausch voll
055	ENOANO	Keine Anode
056	EBADRQC	Ungültiger Anforderungscode
057	EBADSLT	Ungültiger Steckplatz
058		
059	EBFONT	Ungültiges Schriftartdateiformat

Fehlernummer	Fehlercode	Bedeutung
060	ENOSTR	Gerät ist kein Stream
061	ENODATA	Keine Daten verfügbar
062	ETIME	Timer abgelaufen
063	ENOSR	Keine Stream-Ressourcen mehr vorhanden
064	ENONET	Maschine ist nicht im Netzwerk
065	ENOPKG	Paket nicht installiert
066	EREMOTE	Objekt ist remote
067	ENOLINK	Die Verbindung wurde getrennt
068	EADV	Fehler melden
069	ESRMNT	Srmount-Fehler
070	ECOMM	Kommunikationsfehler beim Senden
071	EPROTO	Protokollfehler
072	EMULTIHOP	Multihop versucht
073	EDOTDOT	RFS-spezifischer Fehler
074	EBADMSG	Keine Datennachricht
075	ÜBERLAUF	Wert zu groß für definierten Datentyp
076	ENOTUNIQ	Name im Netzwerk nicht eindeutig
077	EBADFD	Dateideskriptor in fehlerhaftem Zustand
078	EREMCHG	Remote-Adresse geändert
079	ELIBACC	Auf eine benötigte gemeinsam genutzte Bibliothek kann nicht zugegriffen werden
080	ELIBBAD	Zugriff auf eine beschädigte gemeinsam genutzte Bibliothek

Fehlernummer	Fehlercode	Bedeutung
081	ELIBSCN	
082	ELIBMAX	Versuch, zu viele gemeinsam genutzte Bibliotheken einzubinden
083	ELIBEXEC	Eine gemeinsam genutzte Bibliothek kann nicht direkt ausgeführt werden
084	EILSEQ	Unzulässige Bytefolge
085	ERESTART	Unterbrochener Systemaufruf sollte neu gestartet werden
086	ESTRPIPE	Streams-Pipe-Fehler
087	EUSERS	Zu viele Benutzer
088	ENOTSOCK	Socket-Operation auf Nicht-Socket
089	EDESTADDRREQ	Zieladresse erforderlich
090	EMSGSIZE	Nachricht zu lang
091	EPROTOTYP	Falscher Protokolltyp für Socket
092	ENOPROTOOPT	Protokoll nicht verfügbar
093	EPROTONOSUPPORT	Protokoll nicht unterstützt
094	ESOCKTNOSUPPORT	Socket-Typ wird nicht unterstützt
095	EOPNOTSUPP	Vorgang wird am Transportendpunkt nicht unterstützt
096	EPFNOSUPPORT	Protokollfamilie wird nicht unterstützt
097	EAFNOSUPPORT	Adressfamilie wird vom Protokoll nicht unterstützt
098	EADDRINUSE	Adresse bereits verwendet
099	EADDRNOTAVAIL	Die angeforderte Adresse kann nicht zugewiesen werden
100	ENETDOWN	Das Netzwerk ist ausgefallen

Fehlernummer	Fehlercode	Bedeutung
101	ENETUNREACH	Netzwerk ist nicht erreichbar
102	ENETRESET	Die Netzwerkverbindung wurde aufgrund eines Resets unterbrochen
103	ABGEBROCHEN	Software verursachte Verbindungsabbruch
104	ECONNRESET	Verbindung vom Peer zurückgesetzt
105	ENOBUFS	Kein Pufferspeicher verfügbar
106	EISCONN	Transportendpunkt ist bereits verbunden
107	ENOTCONN	Transportendpunkt ist nicht verbunden
108	ESHUTDOWN	Nach dem Herunterfahren des Transportendpunkts kann nicht gesendet werden
109	ETOOMANYREFS	Zu viele Referenzen: kann nicht zusammengefügt werden
110	ETIMEDOUT	Verbindungs-Timeout
111	ECONNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHOSTUNREACH	Keine Route zum Host
114	BEREITS	Vorgang läuft bereits
115	EINPROGRESS	Der Vorgang läuft derzeit
116		
117	EUCLEAN	Struktur muss gereinigt werden
118	ENOTNAM	Keine XENIX-Datei mit benanntem Typ
119	ENAVAIL	Keine XENIX-Semaphoren verfügbar
120	EISNAM	Ist eine benannte Typdatei

Fehlernummer	Fehlercode	Bedeutung
121	EREMOTEIO	Remote-E/A-Fehler
122	EDQUOT	Kontingent überschritten
123	ENOMEDIUM	Kein Medium gefunden
124	EMEDIUMTYPE	Falscher Medientyp
125	ABGESAGT	Vorgang abgebrochen
126	ENOKEY	Erforderlicher Schlüssel nicht verfügbar
127	EKEY ABGELAUFEN	Schlüssel ist abgelaufen
128	EKEY WIDERRUFEN	Schlüssel wurde widerrufen
129	EKEYABGELEHNT	Der Schlüssel wurde vom Dienst abgelehnt
130	EOWNERDEAD	Für robuste Mutexe: Besitzer gestorben
131	NICHT WIEDERHERSTELLBAR	Für robuste Mutexe: Zustand nicht wiederherstellbar

Konfigurieren von Überwachungsnachrichten und Protokollzielen

Überlegungen zur Verwendung eines externen Syslog-Servers

Ein externer Syslog-Server ist ein Server außerhalb von StorageGRID , den Sie zum Sammeln von Systemprüfungsinformationen an einem einzigen Ort verwenden können. Durch die Verwendung eines externen Syslog-Servers können Sie den Netzwerkverkehr auf Ihren Admin-Knoten reduzieren und die Informationen effizienter verwalten. Für StorageGRID ist das Paketformat für ausgehende Syslog-Nachrichten mit RFC 3164 kompatibel.

Zu den Arten von Prüfinformationen, die Sie an den externen Syslog-Server senden können, gehören:

- Audit-Protokolle mit den während des normalen Systembetriebs generierten Audit-Meldungen
- Sicherheitsrelevante Ereignisse wie Anmeldungen und Eskalationen zum Root
- Anwendungsprotokolle, die möglicherweise angefordert werden, wenn es notwendig ist, einen Supportfall zu eröffnen, um ein aufgetretenes Problem zu beheben

Wann Sie einen externen Syslog-Server verwenden sollten

Ein externer Syslog-Server ist besonders nützlich, wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Anwendungen verwenden oder alle Auditdaten behalten möchten. Durch das Senden von Auditinformationen an einen externen Syslog-Server können Sie:

- Erfassen und verwalten Sie Auditinformationen wie Auditmeldungen, Anwendungsprotokolle und Sicherheitsereignisse effizienter.
- Reduzieren Sie den Netzwerkverkehr auf Ihren Admin-Knoten, da Audit-Informationen direkt von den verschiedenen Speicherknoten an den externen Syslog-Server übertragen werden, ohne dass ein Admin-Knoten durchlaufen werden muss.

> Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle mit mehr als 8.192 Bytes am Ende der Nachricht abgeschnitten, um den allgemeinen Einschränkungen bei Implementierungen externer Syslog-Server zu entsprechen.

> Um die Möglichkeiten zur vollständigen Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers zu maximieren, können bis zu 20 GB lokale Protokolle mit Audit-Datensätzen gespeichert werden.(`localaudit.log`) werden auf jedem Knoten verwaltet.

So konfigurieren Sie einen externen Syslog-Server

Informationen zum Konfigurieren eines externen Syslog-Servers finden Sie unter"Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server" .

Wenn Sie die Verwendung des TLS- oder RELP/TLS-Protokolls konfigurieren möchten, benötigen Sie die folgenden Zertifikate:

- **Server-CA-Zertifikate**: Ein oder mehrere vertrauenswürdige CA-Zertifikate zur Überprüfung des externen Syslog-Servers in PEM-Kodierung. Wenn es weggelassen wird, wird das Standard-Grid-CA-Zertifikat verwendet.
- **Client-Zertifikat**: Das Client-Zertifikat zur Authentifizierung gegenüber dem externen Syslog-Server in PEM-Kodierung.
- **Privater Schlüssel des Clients**: Privater Schlüssel für das Client-Zertifikat in PEM-Kodierung.

> Wenn Sie ein Client-Zertifikat verwenden, müssen Sie auch einen privaten Client-Schlüssel verwenden. Wenn Sie einen verschlüsselten privaten Schlüssel angeben, müssen Sie auch die Passphrase angeben. Die Verwendung eines verschlüsselten privaten Schlüssels bietet keinen nennenswerten Sicherheitsvorteil, da Schlüssel und Passphrase gespeichert werden müssen. Aus Gründen der Einfachheit wird die Verwendung eines unverschlüsselten privaten Schlüssels empfohlen, sofern verfügbar.

So schätzen Sie die Größe des externen Syslog-Servers

Normalerweise ist Ihr Grid so dimensioniert, dass ein erforderlicher Durchsatz erreicht wird, der in S3-Operationen pro Sekunde oder Bytes pro Sekunde definiert ist. Beispielsweise besteht möglicherweise die Anforderung, dass Ihr Grid 1.000 S3-Operationen pro Sekunde oder 2.000 MB pro Sekunde an Objektaufnahmen und -abrufen verarbeiten muss. Sie sollten die Größe Ihres externen Syslog-Servers entsprechend den Datenanforderungen Ihres Grids anpassen.

Dieser Abschnitt enthält einige heuristische Formeln, mit deren Hilfe Sie die Rate und durchschnittliche Größe von Protokollnachrichten verschiedener Typen schätzen können, die Ihr externer Syslog-Server verarbeiten können muss, ausgedrückt in Bezug auf die bekannten oder gewünschten Leistungsmerkmale des Grids (S3-Operationen pro Sekunde).

Verwenden Sie S3-Operationen pro Sekunde in Schätzformeln

Wenn Ihr Grid für einen Durchsatz in Bytes pro Sekunde ausgelegt ist, müssen Sie diese Dimensionierung in S3-Operationen pro Sekunde umrechnen, um die Schätzformeln verwenden zu können. Um den Grid-Durchsatz zu konvertieren, müssen Sie zunächst Ihre durchschnittliche Objektgröße bestimmen. Dies können Sie mithilfe der Informationen in vorhandenen Prüfprotokollen und Metriken (sofern vorhanden) oder mithilfe Ihrer Kenntnisse über die Anwendungen tun, die StorageGRID verwenden. Wenn Ihr Grid beispielsweise so dimensioniert ist, dass ein Durchsatz von 2.000 MB/Sekunde erreicht wird und Ihre durchschnittliche Objektgröße 2 MB beträgt, dann ist Ihr Grid so dimensioniert, dass es 1.000 S3-Operationen pro Sekunde verarbeiten kann (2.000 MB / 2 MB).

> ⓘ Die Formeln zur Dimensionierung externer Syslog-Server in den folgenden Abschnitten stellen Schätzungen für den Normalfall dar (und nicht für den Worst-Case). Abhängig von Ihrer Konfiguration und Arbeitslast kann die Rate der Syslog-Nachrichten oder das Volumen der Syslog-Daten höher oder niedriger sein als in den Formeln vorhergesagt. Die Formeln dienen lediglich als Richtlinien.

Schätzformeln für Audit-Protokolle

Wenn Sie über keine anderen Informationen zu Ihrer S3-Arbeitslast verfügen als über die Anzahl der S3-Operationen pro Sekunde, die Ihr Grid voraussichtlich unterstützen wird, können Sie das Volumen der Prüfprotokolle, die Ihr externer Syslog-Server verarbeiten muss, mithilfe der folgenden Formeln schätzen, unter der Annahme, dass Sie die Prüfebenen auf den Standardwerten belassen (alle Kategorien auf „Normal“ eingestellt, außer „Speicher“, das auf „Fehler“ eingestellt ist):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 2.000 Syslog-Nachrichten pro Sekunde unterstützt und in der Lage sein, Prüfprotokolldaten mit einer Rate von 1,6 MB pro Sekunde zu empfangen (und normalerweise zu speichern).

Wenn Sie mehr über Ihre Arbeitsbelastung wissen, sind genauere Schätzungen möglich. Für Prüfprotokolle sind die wichtigsten zusätzlichen Variablen der Prozentsatz der S3-Operationen, die PUTs (vs. GETS) sind, und die durchschnittliche Größe in Bytes der folgenden S3-Felder (die in der Tabelle verwendeten 4-stelligen Abkürzungen sind Prüfprotokoll-Feldnamen):

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.

Code	Feld	Beschreibung
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Taste	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.

Verwenden wir P, um den Prozentsatz der S3-Operationen darzustellen, die PUTs sind, wobei 0 ≤ P ≤ 1 (also für eine 100 % PUT-Arbeitslast P = 1 und für eine 100 % GET-Arbeitslast P = 0).

Verwenden wir K, um die durchschnittliche Größe der Summe der S3-Kontonamen, des S3-Buckets und des S3-Schlüssels darzustellen. Angenommen, der S3-Kontoname lautet immer my-s3-account (13 Byte), Buckets haben Namen mit fester Länge wie /my/application/bucket-12345 (28 Byte) und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Byte). Dann beträgt der Wert von K 90 (13+13+28+36).

Wenn Sie Werte für P und K ermitteln können, können Sie das Volumen der Prüfprotokolle schätzen, die Ihr externer Syslog-Server verarbeiten muss. Verwenden Sie dazu die folgenden Formeln, vorausgesetzt, Sie belassen die Prüfebenen auf den Standardeinstellungen (alle Kategorien auf „Normal“ eingestellt, außer „Speicher“, das auf „Fehler“ eingestellt ist):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, Ihre Arbeitslast zu 50 % aus PUTs besteht und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte umfassen, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 1.500 Syslog-Nachrichten pro Sekunde unterstützt und in der Lage sein, Prüfprotokolldaten mit einer Rate von etwa 1 MB pro Sekunde zu empfangen (und normalerweise zu speichern).

Schätzformeln für nicht standardmäßige Prüfstufen

Die für Prüfprotokolle bereitgestellten Formeln gehen von der Verwendung der Standardeinstellungen für die Prüfebene aus (alle Kategorien sind auf „Normal“ eingestellt, mit Ausnahme von „Speicher“, das auf „Fehler“ eingestellt ist). Detaillierte Formeln zum Schätzen der Rate und der durchschnittlichen Größe von Überwachungsnachrichten für nicht standardmäßige Überwachungsebeneneinstellungen sind nicht verfügbar. Die folgende Tabelle kann jedoch für eine grobe Schätzung der Rate verwendet werden. Sie können die für Prüfprotokolle bereitgestellte Formel zur Berechnung der Durchschnittsgröße verwenden. Beachten Sie jedoch, dass dies wahrscheinlich zu einer Überschätzung führt, da die „zusätzlichen“ Prüfmeldungen im Durchschnitt kleiner sind als die Standardprüfmeldungen.

Zustand	Formel
Replikation: Audit-Levels alle auf Debug oder Normal eingestellt	Audit-Protokollrate = 8 x S3-Operationsrate
Erasure Coding: Audit-Levels alle auf Debug oder Normal eingestellt	Verwenden Sie dieselbe Formel wie für die Standardeinstellungen

Schätzformeln für Sicherheitsereignisse

Sicherheitsereignisse korrelieren nicht mit S3-Vorgängen und erzeugen normalerweise ein vernachlässigbares Volumen an Protokollen und Daten. Aus diesen Gründen werden keine Schätzformeln bereitgestellt.

Schätzformeln für Anwendungsprotokolle

Wenn Sie über keine anderen Informationen zu Ihrer S3-Arbeitslast verfügen als über die Anzahl der S3-Operationen pro Sekunde, die Ihr Grid voraussichtlich unterstützen wird, können Sie das Volumen der Anwendungsprotokolle, die Ihr externer Syslog-Server verarbeiten muss, mithilfe der folgenden Formeln schätzen:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 3.300 Anwendungsprotokolle pro Sekunde unterstützt und Anwendungsprotokolldaten mit einer Rate von etwa 1,2 MB pro Sekunde empfangen (und speichern) kann.

Wenn Sie mehr über Ihre Arbeitsbelastung wissen, sind genauere Schätzungen möglich. Bei Anwendungsprotokollen sind die wichtigsten zusätzlichen Variablen die Datensicherungsstrategie (Replikation vs. Erasure Coding), der Prozentsatz der S3-Operationen, die PUTs sind (vs. GETs/andere), und die durchschnittliche Größe der folgenden S3-Felder in Bytes (die in der Tabelle verwendeten 4-stelligen Abkürzungen sind die Namen der Prüfprotokollfelder):

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Taste	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.

Beispiele für Größenschätzungen

In diesem Abschnitt werden Beispielfälle erläutert, wie die Schätzformeln für Raster mit den folgenden Datenschutzmethoden verwendet werden können:

- Replikation

- Löschcodierung

Wenn Sie die Replikation zum Schutz Ihrer Daten verwenden

Lassen Sie P den Prozentsatz der S3-Operationen darstellen, die PUTs sind, wobei 0 ≤ P ≤ 1 (also für eine 100 % PUT-Arbeitslast P = 1 und für eine 100 % GET-Arbeitslast P = 0).

Lassen Sie K die durchschnittliche Größe der Summe der S3-Kontonamen, des S3-Buckets und des S3-Schlüssels darstellen. Angenommen, der S3-Kontoname lautet immer my-s3-account (13 Byte), Buckets haben Namen mit fester Länge wie /my/application/bucket-12345 (28 Byte) und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Byte). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie mithilfe der folgenden Formeln das Volumen der Anwendungsprotokolle schätzen, das Ihr externer Syslog-Server verarbeiten können muss.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, Ihre Arbeitslast zu 50 % aus PUTs besteht und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Bytes umfassen, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 1.800 Anwendungsprotokolle pro Sekunde unterstützt und Anwendungsdaten mit einer Rate von 0,5 MB pro Sekunde empfängt (und normalerweise speichert).

Wenn Sie Erasure Coding zum Datenschutz verwenden

Lassen Sie P den Prozentsatz der S3-Operationen darstellen, die PUTs sind, wobei 0 ≤ P ≤ 1 (also für eine 100 % PUT-Arbeitslast P = 1 und für eine 100 % GET-Arbeitslast P = 0).

Lassen Sie K die durchschnittliche Größe der Summe der S3-Kontonamen, des S3-Buckets und des S3-Schlüssels darstellen. Angenommen, der S3-Kontoname lautet immer my-s3-account (13 Byte), Buckets haben Namen mit fester Länge wie /my/application/bucket-12345 (28 Byte) und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Byte). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie mithilfe der folgenden Formeln das Volumen der Anwendungsprotokolle schätzen, das Ihr externer Syslog-Server verarbeiten können muss.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, Ihre Arbeitslast zu 50 % aus PUTs besteht und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte umfassen, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 2.250 Anwendungsprotokolle pro Sekunde unterstützt und in der Lage sein, Anwendungsdaten mit einer Rate von 0,6 MB pro Sekunde zu empfangen (und normalerweise zu speichern).

Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server

Sie können eine Reihe von Einstellungen im Zusammenhang mit Prüfmeldungen konfigurieren. Sie können die Anzahl der aufgezeichneten Prüfmeldungen anpassen, alle HTTP-Anforderungsheader definieren, die Sie in die Prüfmeldungen zum Lesen und Schreiben des Clients aufnehmen möchten, einen externen Syslog-Server konfigurieren und angeben, wohin Prüfprotokolle, Sicherheitsereignisprotokolle und StorageGRID Softwareprotokolle gesendet werden.

Prüfmeldungen und -protokolle zeichnen Systemaktivitäten und Sicherheitsereignisse auf und sind wichtige Tools zur Überwachung und Fehlerbehebung. Alle StorageGRID -Knoten generieren Prüfmeldungen und Protokolle, um Systemaktivitäten und Ereignisse zu verfolgen.

Optional können Sie einen externen Syslog-Server konfigurieren, um Audit-Informationen remote zu speichern. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Prüfnachrichten auf die Leistung minimiert, ohne die Vollständigkeit der Prüfdaten zu verringern. Ein externer Syslog-Server ist besonders nützlich, wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Anwendungen verwenden oder alle Auditdaten behalten möchten. Sehen"Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server" für Details.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Wenn Sie planen, einen externen Syslog-Server zu konfigurieren, haben Sie die"Überlegungen zur Verwendung eines externen Syslog-Servers" und sichergestellt, dass der Server über genügend Kapazität zum Empfangen und Speichern der Protokolldateien verfügt.
- Wenn Sie einen externen Syslog-Server mit dem TLS- oder RELP/TLS-Protokoll konfigurieren möchten, verfügen Sie über die erforderlichen Server-CA- und Client-Zertifikate sowie den privaten Client-Schlüssel.

Ändern der Überwachungsmeldungsebenen

Sie können für jede der folgenden Nachrichtenkategorien im Überwachungsprotokoll eine andere Überwachungsebene festlegen:

Prüfungskategorie	Standardeinstellung	Weitere Informationen
System	Normal	"System-Audit-Meldungen"
Storage	Fehler	"Objektspeicher-Auditmeldungen"
Management	Normal	"Management-Audit-Nachricht"
Client liest	Normal	"Client liest Audit-Nachrichten"
Kunde schreibt	Normal	"Client schreibt Prüfmeldungen"
ILM	Normal	"ILM-Audit-Meldungen"

Prüfungskategorie	Standardeinstellung	Weitere Informationen
Cross-Grid-Replikation	Fehler	"CGRR: Cross-Grid-Replikationsanforderung"

Diese Standardeinstellungen gelten, wenn Sie StorageGRID ursprünglich mit Version 10.3 oder höher installiert haben. Wenn Sie ursprünglich eine frühere Version von StorageGRID verwendet haben, ist die Standardeinstellung für alle Kategorien auf „Normal“ eingestellt.

Bei Upgrades werden Konfigurationen auf Audit-Ebene nicht sofort wirksam.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**.
2. Wählen Sie für jede Kategorie von Prüfmeldungen eine Prüfebene aus der Dropdown-Liste aus:

Prüfebene	Beschreibung
Aus	Es werden keine Auditmeldungen aus dieser Kategorie protokolliert.
Fehler	Es werden nur Fehlermeldungen protokolliert – Prüfmeldungen, deren Ergebniscode nicht „erfolgreich“ (SUCS) war.
Normal	Es werden standardmäßige Transaktionsnachrichten protokolliert – die Nachrichten, die in diesen Anweisungen für die Kategorie aufgeführt sind.
Debuggen	Veraltet. Diese Ebene verhält sich genauso wie die normale Überwachungsebene.

Zu den für eine bestimmte Ebene enthaltenen Nachrichten gehören auch diejenigen, die auf den höheren Ebenen protokolliert würden. Beispielsweise umfasst die Ebene „Normal“ alle Fehlermeldungen.

Wenn Sie keine detaillierte Aufzeichnung der Client-Lesevorgänge für Ihre S3-Anwendungen benötigen, ändern Sie optional die Einstellung **Client Reads** in **Error**, um die Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu verringern.

3. Wählen Sie **Speichern**.

   Ein grünes Banner zeigt an, dass Ihre Konfiguration gespeichert wurde.

Definieren von HTTP-Anforderungsheadern

Sie können optional alle HTTP-Anforderungsheader definieren, die Sie in die Prüfnachrichten zum Lesen und Schreiben des Clients aufnehmen möchten. Diese Protokollheader gelten nur für S3-Anfragen.

Schritte

1. Definieren Sie im Abschnitt **Audit-Protokollheader** die HTTP-Anforderungsheader, die Sie in die Lese- und Schreib-Auditnachrichten des Clients aufnehmen möchten.

   Verwenden Sie ein Sternchen (*) als Platzhalter, um null oder mehr Zeichen abzugleichen. Verwenden Sie

die Escape-Sequenz (*), um ein wörtliches Sternchen zu finden.

2. Wählen Sie **Weitere Kopfzeile hinzufügen**, um bei Bedarf zusätzliche Kopfzeilen zu erstellen.

   Wenn in einer Anfrage HTTP-Header gefunden werden, werden diese in die Prüfnachricht unter dem Feld HTRH aufgenommen.

   > Anforderungsheader des Prüfprotokolls werden nur protokolliert, wenn die Prüfstufe für **Client-Lesevorgänge** oder **Client-Schreibvorgänge** nicht **Aus** ist.

3. Wählen Sie **Speichern**

   Ein grünes Banner zeigt an, dass Ihre Konfiguration gespeichert wurde.

Verwenden Sie einen externen Syslog-Server

Sie können optional einen externen Syslog-Server konfigurieren, um Prüfprotokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Ort außerhalb Ihres Grids zu speichern.

> Wenn Sie keinen externen Syslog-Server verwenden möchten, überspringen Sie diesen Schritt und gehen Sie zuAuswählen von Zielen für Auditinformationen .

> Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihren Anforderungen gerecht zu werden, können zusätzliche Konfigurationsoptionen angewendet werden, indem Sie `audit-destinations` Endpunkte, die sich im privaten API-Bereich des"Grid-Management-API" . Sie können die API beispielsweise verwenden, wenn Sie für unterschiedliche Knotengruppen unterschiedliche Syslog-Server verwenden möchten.

Syslog-Informationen eingeben

Greifen Sie auf den Assistenten „Externen Syslog-Server konfigurieren“ zu und geben Sie die Informationen ein, die StorageGRID für den Zugriff auf den externen Syslog-Server benötigt.

Schritte

1. Wählen Sie auf der Seite „Audit- und Syslog-Server“ die Option „Externen Syslog-Server konfigurieren“ aus. Oder wählen Sie **Externen Syslog-Server bearbeiten**, wenn Sie zuvor einen externen Syslog-Server konfiguriert haben.

   Der Assistent „Externen Syslog-Server konfigurieren“ wird angezeigt.

2. Geben Sie im Schritt **Syslog-Informationen eingeben** des Assistenten im Feld **Host** einen gültigen vollqualifizierten Domänennamen oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server ein.
3. Geben Sie den Zielport auf dem externen Syslog-Server ein (muss eine Ganzzahl zwischen 1 und 65535 sein). Der Standardport ist 514.
4. Wählen Sie das Protokoll aus, das zum Senden von Audit-Informationen an den externen Syslog-Server verwendet wird.

   Die Verwendung von **TLS** oder **RELP/TLS** wird empfohlen. Sie müssen ein Serverzertifikat hochladen, um eine dieser Optionen zu verwenden. Durch die Verwendung von Zertifikaten können Sie die Verbindungen zwischen Ihrem Grid und dem externen Syslog-Server sichern. Weitere Informationen finden Sie unter "Sicherheitszertifikate verwalten" .

Alle Protokolloptionen erfordern die Unterstützung und Konfiguration des externen Syslog-Servers. Sie müssen eine Option wählen, die mit dem externen Syslog-Server kompatibel ist.

> Das Reliable Event Logging Protocol (RELP) erweitert die Funktionalität des Syslog-Protokolls, um eine zuverlässige Übermittlung von Ereignismeldungen zu ermöglichen. Durch die Verwendung von RELP können Sie den Verlust von Prüfinformationen verhindern, wenn Ihr externer Syslog-Server neu gestartet werden muss.

5. Wählen Sie **Weiter**.
6. Wenn Sie **TLS** oder **RELP/TLS** ausgewählt haben, laden Sie die Server-CA-Zertifikate, das Client-Zertifikat und den privaten Client-Schlüssel hoch.
   a. Wählen Sie **Durchsuchen** für das Zertifikat oder den Schlüssel, das/den Sie verwenden möchten.
   b. Wählen Sie das Zertifikat oder die Schlüsseldatei aus.
   c. Wählen Sie **Öffnen**, um die Datei hochzuladen.

      Neben dem Zertifikats- oder Schlüsseldateinamen wird ein grünes Häkchen angezeigt, das Sie darüber informiert, dass das Hochladen erfolgreich war.
7. Wählen Sie **Weiter**.

Syslog-Inhalte verwalten

Sie können auswählen, welche Informationen an den externen Syslog-Server gesendet werden sollen.

Schritte

1. Wählen Sie im Schritt **Syslog-Inhalt verwalten** des Assistenten alle Arten von Audit-Informationen aus, die Sie an den externen Syslog-Server senden möchten.
   - **Sende Audit-Protokolle**: Sendet StorageGRID -Ereignisse und Systemaktivitäten
   - **Sicherheitsereignisse senden**: Sendet Sicherheitsereignisse, beispielsweise wenn ein nicht autorisierter Benutzer versucht, sich anzumelden, oder wenn sich ein Benutzer als Root anmeldet
   - **Anwendungsprotokolle senden**: Sendet"Protokolldateien der StorageGRID -Software" nützlich für die Fehlerbehebung, einschließlich:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`(Nur Admin-Knoten)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - **Zugriffsprotokolle senden**: Sendet HTTP-Zugriffsprotokolle für externe Anfragen an Grid Manager, Tenant Manager, konfigurierte Load Balancer-Endpunkte und Grid-Föderationsanfragen von Remote-Systemen.
2. Wählen Sie mithilfe der Dropdown-Menüs den Schweregrad und die Einrichtung (Nachrichtentyp) für jede Kategorie von Prüfinformationen aus, die Sie senden möchten.

   Durch Festlegen von Schweregrad- und Einrichtungswerten können Sie die Protokolle auf anpassbare

Weise aggregieren, um die Analyse zu vereinfachen.

a. Wählen Sie für **Schweregrad Passthrough** oder einen Schweregradwert zwischen 0 und 7 aus.

   Wenn Sie einen Wert auswählen, wird der ausgewählte Wert auf alle Nachrichten dieses Typs angewendet. Informationen zu unterschiedlichen Schweregraden gehen verloren, wenn Sie den Schweregrad mit einem festen Wert überschreiben.

Schwere	Beschreibung
Durchreichen	Jede an das externe Syslog gesendete Nachricht muss denselben Schweregrad haben wie bei der lokalen Protokollierung auf dem Knoten: • Bei Prüfprotokollen ist der Schweregrad „Info“. • Bei Sicherheitsereignissen werden die Schweregrade von der Linux-Distribution auf den Knoten generiert. • Bei Anwendungsprotokollen variieren die Schweregrade je nach Problem zwischen „Info“ und „Hinweis“. Beispielsweise ergibt das Hinzufügen eines NTP-Servers und das Konfigurieren einer HA-Gruppe den Wert „Info“, während das absichtliche Stoppen des SSM- oder RSM-Dienstes den Wert „Notice“ ergibt. • Bei Zugriffsprotokollen ist der Schweregrad „Info“.
0	Notfall: System ist nicht nutzbar
1	Warnung: Sofortige Maßnahmen erforderlich
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber signifikanter Zustand
6	Informativ: Informationsnachrichten
7	Debug: Meldungen auf Debug-Ebene

b. Wählen Sie für **Einrichtung Passthrough** oder einen Einrichtungswert zwischen 0 und 23.

   Wenn Sie einen Wert auswählen, wird dieser auf alle Nachrichten dieses Typs angewendet. Informationen zu verschiedenen Einrichtungen gehen verloren, wenn Sie die Einrichtung mit einem festen Wert überschreiben.

Einrichtung	Beschreibung
Durchreichen	Jede an das externe Syslog gesendete Nachricht muss denselben Einrichtungswert haben wie bei der lokalen Protokollierung auf dem Knoten: • Bei Prüfprotokollen lautet die an den externen Syslog-Server gesendete Einrichtung „local7“. • Bei Sicherheitsereignissen werden die Einrichtungswerte von der Linux-Distribution auf den Knoten generiert. • Bei Anwendungsprotokollen weisen die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Einrichtungswerte auf: ◦ `bycast.log`: Benutzer oder Daemon ◦ `bycast-err.log`: Benutzer, Daemon, local3 oder local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Bei Zugriffsprotokollen lautet die an den externen Syslog-Server gesendete Einrichtung „local0“.
0	kern (Kernel-Nachrichten)
1	Benutzer (Nachrichten auf Benutzerebene)
2	mail
3	Daemon (Systemdaemons)
4	Auth (Sicherheits-/Autorisierungsnachrichten)
5	Syslog (intern von syslogd generierte Nachrichten)
6	lpr (Zeilendrucker-Subsystem)
7	Nachrichten (Netzwerk-Nachrichten-Subsystem)
8	UUCP
9	Cron (Uhr-Daemon)
10	Sicherheit (Sicherheits-/Autorisierungsnachrichten)

Einrichtung	Beschreibung
11	FTP
12	NTP
13	logaudit (Protokollprüfung)
14	logalert (Protokollalarm)
15	Uhr (Uhr-Daemon)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Wählen Sie **Weiter**.

Testnachrichten senden

Bevor Sie mit der Verwendung eines externen Syslog-Servers beginnen, sollten Sie alle Knoten in Ihrem Grid auffordern, Testnachrichten an den externen Syslog-Server zu senden. Sie sollten diese Testnachrichten verwenden, um Ihre gesamte Infrastruktur zur Protokollsammlung zu validieren, bevor Sie Daten an den externen Syslog-Server senden.

> Verwenden Sie die Konfiguration des externen Syslog-Servers erst, wenn Sie bestätigt haben, dass der externe Syslog-Server von jedem Knoten in Ihrem Grid eine Testnachricht empfangen hat und die Nachricht wie erwartet verarbeitet wurde.

Schritte

1. Wenn Sie keine Testnachrichten senden möchten, weil Sie sicher sind, dass Ihr externer Syslog-Server richtig konfiguriert ist und Prüfinformationen von allen Knoten in Ihrem Grid empfangen kann, wählen Sie **Überspringen und beenden**.

   Ein grünes Banner zeigt an, dass die Konfiguration gespeichert wurde.

2. Andernfalls wählen Sie **Testnachrichten senden** (empfohlen).

   Die Testergebnisse werden kontinuierlich auf der Seite angezeigt, bis Sie den Test beenden. Während der Test läuft, werden Ihre Prüfnachrichten weiterhin an Ihre zuvor konfigurierten Ziele gesendet.

3. Wenn Sie während der Syslog-Serverkonfiguration oder zur Laufzeit Fehler erhalten, korrigieren Sie diese und wählen Sie erneut **Testnachrichten senden**.

   Sehen"Fehlerbehebung bei einem externen Syslog-Server" um Ihnen bei der Behebung etwaiger Fehler zu helfen.

4. Warten Sie, bis ein grünes Banner angezeigt wird, das anzeigt, dass alle Knoten den Test bestanden haben.
5. Überprüfen Sie Ihren Syslog-Server, um festzustellen, ob Testnachrichten wie erwartet empfangen und verarbeitet werden.

   Wenn Sie UDP verwenden, überprüfen Sie Ihre gesamte Infrastruktur zur Protokollsammlung. Das UDP-Protokoll ermöglicht keine so strenge Fehlererkennung wie die anderen Protokolle.

6. Wählen Sie **Stoppen und beenden**.

   Sie werden zur Seite **Audit- und Syslog-Server** zurückgeleitet. Ein grünes Banner zeigt an, dass die Syslog-Serverkonfiguration gespeichert wurde.

   StorageGRID Auditinformationen werden erst an den externen Syslog-Server gesendet, wenn Sie ein Ziel auswählen, das den externen Syslog-Server enthält.

Auswählen von Zielen für Auditinformationen

Sie können angeben, wo Überwachungsprotokolle, Sicherheitsereignisprotokolle und"StorageGRID -Softwareprotokolle" gesendet werden.

StorageGRID verwendet standardmäßig lokale Knoten-Audit-Ziele und speichert die Audit-Informationen in `/var/local/log/localaudit.log` .

Bei der Verwendung `/var/local/log/localaudit.log` , die Audit-Protokolleinträge des Grid Managers und des Tenant Managers können an einen Speicherknoten gesendet werden. Welcher Knoten die aktuellsten Einträge hat, können Sie mithilfe der `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` Befehl.

Einige Ziele sind nur verfügbar, wenn Sie einen externen Syslog-Server konfiguriert haben.

Schritte

1. Wählen Sie auf der Seite „Audit- und Syslog-Server“ das Ziel für die Audit-Informationen aus.

   Nur lokale Knoten und **Externer Syslog-Server** bieten normalerweise eine bessere Leistung.

Option	Beschreibung
Nur lokale Knoten (Standard)	Prüfmeldungen, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden nicht an Admin-Knoten gesendet. Stattdessen werden sie nur auf den Knoten gespeichert, die sie generiert haben („der lokale Knoten“). Die auf jedem lokalen Knoten generierten Prüfinformationen werden gespeichert in `/var/local/log/localaudit.log` . **Hinweis**: StorageGRID entfernt regelmäßig lokale Protokolle in einer Rotation, um Speicherplatz freizugeben. Wenn die Protokolldatei für einen Knoten 1 GB erreicht, wird die vorhandene Datei gespeichert und eine neue Protokolldatei gestartet. Die Rotationsgrenze für das Protokoll liegt bei 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Durchschnittlich werden auf jedem Knoten etwa 20 GB Protokolldaten gespeichert.
Admin-Knoten/lokale Knoten	Audit-Meldungen werden an das Audit-Protokoll auf den Admin-Knoten gesendet und Sicherheitsereignisprotokolle sowie Anwendungsprotokolle werden auf den Knoten gespeichert, die sie generiert haben. Die Auditinformationen werden in den folgenden Dateien gespeichert: • Admin-Knoten (primär und nicht primär): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Die Datei ist normalerweise leer oder fehlt. Es kann sekundäre Informationen enthalten, beispielsweise eine zusätzliche Kopie einiger Nachrichten.
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf den lokalen Knoten gespeichert(`/var/local/log/localaudit.log`). Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option wird erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Knoten und externer Syslog-Server	Audit-Meldungen werden an das Audit-Protokoll gesendet(`/var/local/audit/export/audit.log`) auf Admin-Knoten, und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert(`/var/local/log/localaudit.log`). Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option wird erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.

2. Wählen Sie **Speichern**.

   Es wird eine Warnmeldung angezeigt.

3. Wählen Sie **OK**, um zu bestätigen, dass Sie das Ziel für Auditinformationen ändern möchten.

Ein grünes Banner zeigt an, dass die Audit-Konfiguration gespeichert wurde.

Neue Protokolle werden an die von Ihnen ausgewählten Ziele gesendet. Vorhandene Protokolle verbleiben an ihrem aktuellen Speicherort.

Verwenden Sie die SNMP-Überwachung

Verwenden Sie die SNMP-Überwachung

Wenn Sie StorageGRID mithilfe des Simple Network Management Protocol (SNMP) überwachen möchten, müssen Sie den in StorageGRID enthaltenen SNMP-Agenten konfigurieren.

- "Konfigurieren des SNMP-Agenten"
- "Aktualisieren Sie den SNMP-Agenten"

Funktionen

Auf jedem StorageGRID Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine MIB bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Warnungen. Die MIB enthält außerdem Systembeschreibungsinformationen wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID Knoten unterstützt auch eine Teilmenge von MIB-II-Objekten.

Sehen"Zugriff auf MIB-Dateien" wenn Sie die MIB-Dateien auf Ihre Grid-Knoten herunterladen möchten.

Zunächst ist SNMP auf allen Knoten deaktiviert. Wenn Sie den SNMP-Agenten konfigurieren, erhalten alle StorageGRID Knoten dieselbe Konfiguration.

Der StorageGRID SNMP-Agent unterstützt alle drei Versionen des SNMP-Protokolls. Es bietet schreibgeschützten MIB-Zugriff für Abfragen und kann zwei Arten ereignisgesteuerter Benachrichtigungen an ein Verwaltungssystem senden:

Fallen

Traps sind vom SNMP-Agenten gesendete Benachrichtigungen, die keine Bestätigung durch das Verwaltungssystem erfordern. Traps dienen dazu, das Verwaltungssystem darüber zu informieren, dass in StorageGRID etwas passiert ist, beispielsweise dass ein Alarm ausgelöst wurde.

Traps werden in allen drei Versionen von SNMP unterstützt.

Informiert

Informs ähneln Traps, erfordern jedoch eine Bestätigung durch das Managementsystem. Wenn der SNMP-Agent innerhalb einer bestimmten Zeitspanne keine Bestätigung erhält, sendet er die Information erneut, bis eine Bestätigung eingeht oder der maximale Wiederholungswert erreicht ist.

Informs werden in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden in den folgenden Fällen gesendet:

- Bei jedem Schweregrad wird eine Standard- oder benutzerdefinierte Warnung ausgelöst. Um SNMP-Benachrichtigungen für einen Alarm zu unterdrücken, müssen Sie"Konfigurieren Sie eine Stille" für die Warnung. Warnmeldungen werden gesendet von"bevorzugter Absender-Admin-Knoten" .

Jeder Alarm wird basierend auf seinem Schweregrad einem von drei Trap-Typen zugeordnet: activeMinorAlert, activeMajorAlert und activeCriticalAlert. Eine Liste der Warnungen, die diese Traps auslösen können, finden Sie im"Warnungsreferenz" .

SNMP-Versionsunterstützung

Die Tabelle bietet eine allgemeine Zusammenfassung der Unterstützung für jede SNMP-Version.

	SNMPv1	SNMPv2c	SNMPv3
Abfragen (GET und GETNEXT)	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-Zeichenfolge	Community-Zeichenfolge	Benutzer des benutzerbasierten Sicherheitsmodells (USM)
Benachrichtigungen (Falle und Inform)	Nur Fallen	Fallen und Informationen	Fallen und Informationen
Benachrichtigungsauthentifizierung	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	USM-Benutzer für jedes Trap-Ziel

Einschränkungen

- StorageGRID unterstützt schreibgeschützten MIB-Zugriff. Lese-/Schreibzugriff wird nicht unterstützt.
- Alle Knoten im Grid erhalten die gleiche Konfiguration.
- SNMPv3: StorageGRID unterstützt den Transport Support Mode (TSM) nicht.
- SNMPv3: Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).
- SNMPv3: Das einzige unterstützte Datenschutzprotokoll ist AES.

Konfigurieren des SNMP-Agenten

Sie können den StorageGRID SNMP-Agenten so konfigurieren, dass er ein SNMP-Verwaltungssystem eines Drittanbieters für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwendet.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Der StorageGRID SNMP-Agent unterstützt SNMPv1, SNMPv2c und SNMPv3. Sie können den Agenten für eine oder mehrere Versionen konfigurieren. Für SNMPv3 wird nur die User Security Model (USM)-Authentifizierung unterstützt.

Alle Knoten im Grid verwenden dieselbe SNMP-Konfiguration.

Grundlegende Konfiguration festlegen

Aktivieren Sie als ersten Schritt den StorageGRID SMNP-Agenten und geben Sie grundlegende Informationen ein.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.

   Die SNMP-Agent-Seite wird angezeigt.

2. Um den SNMP-Agenten auf allen Grid-Knoten zu aktivieren, aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.
3. Geben Sie im Abschnitt „Grundkonfiguration“ die folgenden Informationen ein.

Feld	Beschreibung
Systemkontakt	Optional. Der primäre Kontakt für das StorageGRID -System, der in SNMP-Nachrichten als sysContact zurückgegeben wird. Der Systemkontakt ist normalerweise eine E-Mail-Adresse. Dieser Wert gilt für alle Knoten im StorageGRID -System. **Systemkontakt** darf maximal 255 Zeichen lang sein.
Systemstandort	Optional. Der Standort des StorageGRID -Systems, der in SNMP-Nachrichten als sysLocation zurückgegeben wird. Der Systemstandort kann jede Information sein, die zur Identifizierung des Standorts Ihres StorageGRID Systems nützlich ist. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Dieser Wert gilt für alle Knoten im StorageGRID -System. **Systemstandort** darf maximal 255 Zeichen lang sein.
Aktivieren Sie SNMP-Agent-Benachrichtigungen	• Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Trap- und Inform-Benachrichtigungen. • Wenn diese Option nicht ausgewählt ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.
Authentifizierungs-Traps aktivieren	Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Authentifizierungs-Traps, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.

Community-Strings eingeben

Wenn Sie SNMPv1 oder SNMPv2c verwenden, füllen Sie den Abschnitt „Community-Strings“ aus.

Wenn das Verwaltungssystem die StorageGRID MIB abfragt, sendet es eine Community-Zeichenfolge. Wenn der Community-String mit einem der hier angegebenen Werte übereinstimmt, sendet der SNMP-Agent eine Antwort an das Verwaltungssystem.

Schritte

1. Geben Sie für **Nur-Lese-Community** optional eine Community-Zeichenfolge ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agentadressen zuzulassen.

   Um die Sicherheit Ihres StorageGRID -Systems zu gewährleisten, verwenden Sie nicht „public“ als Community-String. Wenn Sie dieses Feld leer lassen, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID Systems als Community-String.

   Jeder Community-String darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

2. Wählen Sie **Weitere Community-Zeichenfolge hinzufügen**, um zusätzliche Zeichenfolgen hinzuzufügen.

   Es sind bis zu fünf Zeichenfolgen zulässig.

Trap-Ziele erstellen

Verwenden Sie die Registerkarte „Trap-Ziele“ im Abschnitt „Weitere Konfigurationen“, um ein oder mehrere Ziele für StorageGRID -Trap- oder Inform-Benachrichtigungen zu definieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, wenn Warnungen ausgelöst werden. Für die unterstützten MIB-II-Entitäten werden auch Standardbenachrichtigungen gesendet (z. B. ifDown und coldStart).

Schritte

1. Geben Sie im Feld **Standard-Trap-Community** optional die Standard-Community-Zeichenfolge ein, die Sie für SNMPv1- oder SNMPv2-Trap-Ziele verwenden möchten.

   Bei Bedarf können Sie bei der Definition eines bestimmten Trap-Ziels einen anderen („benutzerdefinierten“) Community-String angeben.

   Standard-Trap-Community darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

2. Um ein Trap-Ziel hinzuzufügen, wählen Sie **Erstellen**.
3. Wählen Sie aus, welche SNMP-Version für dieses Trap-Ziel verwendet werden soll.
4. Füllen Sie das Formular „Trap-Ziel erstellen“ für die von Ihnen ausgewählte Version aus.

SNMPv1

Wenn Sie SNMPv1 als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Muss Trap für SNMPv1 sein.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein vollqualifizierter Domänenname (FQDN) zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, sofern eine angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

SNMPv2c

Wenn Sie SNMPv2c als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Ob das Ziel für Fallen oder Informationen verwendet wird.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, sofern Sie nicht einen anderen Wert verwenden müssen.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, sofern eine angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

SNMPv3

Wenn Sie SNMPv3 als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Ob das Ziel für Fallen oder Informationen verwendet wird.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, sofern Sie nicht einen anderen Wert verwenden müssen.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
USM-Benutzer	Der USM-Benutzer, der für die Authentifizierung verwendet wird. • Wenn Sie **Trap** ausgewählt haben, werden nur USM-Benutzer ohne autoritative Engine-IDs angezeigt. • Wenn Sie **Informieren** ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt. • Wenn keine Benutzer angezeigt werden: i. Erstellen und speichern Sie das Trap-Ziel. ii. Gehe zuErstellen von USM-Benutzern und erstellen Sie den Benutzer. iii. Kehren Sie zur Registerkarte „Trap-Ziele“ zurück, wählen Sie das gespeicherte Ziel aus der Tabelle aus und wählen Sie **Bearbeiten**. iv. Wählen Sie den Benutzer aus.

5. Wählen Sie **Erstellen**.

   Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

Agentenadressen erstellen

Optional können Sie auf der Registerkarte „Agentenadressen“ im Abschnitt „Weitere Konfigurationen“ eine oder mehrere „Abhöradressen“ angeben. Dies sind die StorageGRID -Adressen, unter denen der SNMP-Agent Abfragen empfangen kann.

Wenn Sie keine Agentenadresse konfigurieren, ist die Standard-Abhöradresse der UDP-Port 161 in allen StorageGRID Netzwerken.

Schritte

1. Wählen Sie **Erstellen**.
2. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Internetprotokoll	Ob diese Adresse IPv4 oder IPv6 verwendet. Standardmäßig verwendet SNMP IPv4.
Transportprotokoll	Ob diese Adresse UDP oder TCP verwendet. Standardmäßig verwendet SNMP UDP.
StorageGRID Netzwerk	Auf welches StorageGRID -Netzwerk der Agent lauscht. • Grid-, Admin- und Client-Netzwerke: Der SNMP-Agent überwacht alle drei Netzwerke auf Abfragen. • Netznetzwerk • Admin-Netzwerk • Kundennetzwerk **Hinweis**: Wenn Sie das Client-Netzwerk für unsichere Daten verwenden und eine Agentenadresse für das Client-Netzwerk erstellen, beachten Sie, dass auch der SNMP-Verkehr unsicher ist.
Hafen	Optional die Portnummer, auf der der SNMP-Agent lauschen soll. Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch jede beliebige nicht verwendete Portnummer eingeben. **Hinweis**: Wenn Sie den SNMP-Agenten speichern, öffnet StorageGRID automatisch die Agenten-Adressports auf der internen Firewall. Sie müssen sicherstellen, dass alle externen Firewalls den Zugriff auf diese Ports zulassen.

3. Wählen Sie **Erstellen**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

USM-Benutzer erstellen

Wenn Sie SNMPv3 verwenden, verwenden Sie die Registerkarte „USM-Benutzer“ im Abschnitt „Weitere Konfigurationen“, um die USM-Benutzer zu definieren, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

SNMPv3-*Inform*-Ziele müssen Benutzer mit Engine-IDs haben. Das SNMPv3-Trap-Ziel kann keine Benutzer mit Engine-IDs haben.

Diese Schritte gelten nicht, wenn Sie nur SNMPv1 oder SNMPv2c verwenden.

Schritte

1. Wählen Sie **Erstellen**.

2. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Benutzername	Ein eindeutiger Name für diesen USM-Benutzer. Benutzernamen dürfen maximal 32 Zeichen lang sein und keine Leerzeichen enthalten. Der Benutzername kann nach der Erstellung des Benutzers nicht mehr geändert werden.
Nur-Lese-MIB-Zugriff	Wenn diese Option ausgewählt ist, sollte dieser Benutzer nur Lesezugriff auf die MIB haben.
Autoritative Engine-ID	Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, die maßgebliche Engine-ID für diesen Benutzer. Geben Sie 10 bis 64 Hex-Zeichen (5 bis 32 Bytes) ohne Leerzeichen ein. Dieser Wert ist für USM-Benutzer erforderlich, die in Trap-Zielen für Informs ausgewählt werden. Dieser Wert ist für USM-Benutzer, die in Trap-Zielen für Traps ausgewählt werden, nicht zulässig. **Hinweis**: Dieses Feld wird nicht angezeigt, wenn Sie **Schreibgeschützter MIB-Zugriff** ausgewählt haben, da USM-Benutzer mit schreibgeschütztem MIB-Zugriff keine Engine-IDs haben können.
Sicherheitsstufe	Die Sicherheitsstufe für den USM-Benutzer: • **authPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Kennwort sowie ein Datenschutzprotokoll und ein Kennwort angeben. • **authNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Privatsphäre (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Kennwort angeben.
Authentifizierungsprotokoll	Immer auf SHA eingestellt, das einzige unterstützte Protokoll (HMAC-SHA-96).
Passwort	Das Kennwort, das dieser Benutzer zur Authentifizierung verwendet.
Datenschutzprotokoll	Wird nur angezeigt, wenn Sie **authPriv** ausgewählt und immer auf AES eingestellt haben, das einzige unterstützte Datenschutzprotokoll.
Passwort	Wird nur angezeigt, wenn Sie **authPriv** ausgewählt haben. Das Passwort, das dieser Benutzer aus Datenschutzgründen verwenden wird.

3. Wählen Sie **Erstellen**.

   Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

4. Wenn Sie die SNMP-Agent-Konfiguration abgeschlossen haben, wählen Sie **Speichern**.

   Die neue SNMP-Agent-Konfiguration wird aktiv.

Aktualisieren Sie den SNMP-Agenten

Sie können SNMP-Benachrichtigungen deaktivieren, Community-Strings aktualisieren oder Agentenadressen, USM-Benutzer und Trap-Ziele hinzufügen oder entfernen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Sehen"Konfigurieren des SNMP-Agenten" für Details zu jedem Feld auf der SNMP-Agent-Seite. Sie müssen unten auf der Seite **Speichern** auswählen, um alle auf den einzelnen Registerkarten vorgenommenen Änderungen zu übernehmen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.

   Die SNMP-Agent-Seite wird angezeigt.

2. Um den SNMP-Agenten auf allen Grid-Knoten zu deaktivieren, deaktivieren Sie das Kontrollkästchen **SNMP aktivieren** und wählen Sie **Speichern**.

   Wenn Sie den SNMP-Agenten erneut aktivieren, bleiben alle vorherigen SNMP-Konfigurationseinstellungen erhalten.

3. Aktualisieren Sie optional die Informationen im Abschnitt „Grundkonfiguration“:
   a. Aktualisieren Sie bei Bedarf den **Systemkontakt** und den **Systemstandort**.
   b. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, um zu steuern, ob der StorageGRID -SNMP-Agent Trap- und Inform-Benachrichtigungen sendet.

      Wenn dieses Kontrollkästchen deaktiviert ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.

   c. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Authentifizierungs-Traps aktivieren**, um zu steuern, ob der StorageGRID SNMP-Agent Authentifizierungs-Traps sendet, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.
4. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren oder fügen Sie optional eine **Nur-Lese-Community** im Abschnitt „Community-Strings“ hinzu.
5. Um Trap-Ziele zu aktualisieren, wählen Sie die Registerkarte Trap-Ziele im Abschnitt „Andere Konfigurationen“ aus.

   Verwenden Sie diese Registerkarte, um ein oder mehrere Ziele für StorageGRID Trap- oder Inform-Benachrichtigungen zu definieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, wenn Warnungen ausgelöst werden. Für die unterstützten MIB-II-Entitäten werden auch Standardbenachrichtigungen gesendet (z. B. ifDown und coldStart).

Einzelheiten zu den einzugebenden Informationen finden Sie unter"Erstellen von Trap-Zielen" .

- Aktualisieren oder entfernen Sie optional die Standard-Trap-Community.

  Wenn Sie die Standard-Trap-Community entfernen, müssen Sie zunächst sicherstellen, dass alle vorhandenen Trap-Ziele eine benutzerdefinierte Community-Zeichenfolge verwenden.

- Um ein Trap-Ziel hinzuzufügen, wählen Sie **Erstellen**.
- Um ein Trap-Ziel zu bearbeiten, wählen Sie das Optionsfeld und dann **Bearbeiten**.
- Um ein Trap-Ziel zu entfernen, wählen Sie das Optionsfeld und dann **Entfernen**.
- Um Ihre Änderungen zu übernehmen, wählen Sie unten auf der Seite **Speichern** aus.

6. Um Agentenadressen zu aktualisieren, wählen Sie die Registerkarte Agentenadressen im Abschnitt „Weitere Konfigurationen“ aus.

   Verwenden Sie diese Registerkarte, um eine oder mehrere „Abhöradressen“ anzugeben. Dies sind die StorageGRID -Adressen, unter denen der SNMP-Agent Abfragen empfangen kann.

   Einzelheiten zu den einzugebenden Informationen finden Sie unter"Agentenadressen erstellen" .

   - Um eine Agentenadresse hinzuzufügen, wählen Sie **Erstellen**.
   - Um eine Agentenadresse zu bearbeiten, wählen Sie das Optionsfeld und dann **Bearbeiten**.
   - Um eine Agentenadresse zu entfernen, wählen Sie das Optionsfeld und dann **Entfernen**.
   - Um Ihre Änderungen zu übernehmen, wählen Sie unten auf der Seite **Speichern** aus.

7. Um USM-Benutzer zu aktualisieren, wählen Sie im Abschnitt „Andere Konfigurationen“ die Registerkarte „USM-Benutzer“ aus.

   Verwenden Sie diese Registerkarte, um die USM-Benutzer zu definieren, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

   Einzelheiten zu den einzugebenden Informationen finden Sie unter"Erstellen von USM-Benutzern" .

   - Um einen USM-Benutzer hinzuzufügen, wählen Sie **Erstellen**.
   - Um einen USM-Benutzer zu bearbeiten, aktivieren Sie das Optionsfeld und wählen Sie **Bearbeiten**.

     Der Benutzername eines vorhandenen USM-Benutzers kann nicht geändert werden. Wenn Sie einen Benutzernamen ändern müssen, müssen Sie den Benutzer entfernen und einen neuen erstellen.

     > Wenn Sie die autoritative Engine-ID eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt beim Speichern der SNMP-Agent-Konfiguration ein Validierungsfehler auf.

   - Um einen USM-Benutzer zu entfernen, aktivieren Sie das Optionsfeld und wählen Sie **Entfernen**.

     > Wenn der von Ihnen entfernte Benutzer derzeit für ein Trap-Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt beim Speichern der SNMP-Agent-Konfiguration ein Validierungsfehler auf.

   - Um Ihre Änderungen zu übernehmen, wählen Sie unten auf der Seite **Speichern** aus.

8. Wenn Sie die SNMP-Agentenkonfiguration aktualisiert haben, wählen Sie **Speichern**.

Zugriff auf MIB-Dateien

MIB-Dateien enthalten Definitionen und Informationen zu den Eigenschaften verwalteter Ressourcen und Dienste für die Knoten in Ihrem Grid. Sie können auf MIB-Dateien zugreifen, die die Objekte und Benachrichtigungen für StorageGRID definieren. Diese Dateien können für die Überwachung Ihres Netzes nützlich sein.

Sehen"Verwenden Sie die SNMP-Überwachung" Weitere Informationen zu SNMP- und MIB-Dateien.

Zugriff auf MIB-Dateien

Befolgen Sie diese Schritte, um auf die MIB-Dateien zuzugreifen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.
2. Wählen Sie auf der SNMP-Agent-Seite die Datei aus, die Sie herunterladen möchten:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definiert die Warntabelle und Benachrichtigungen (Traps), auf die auf allen Admin-Knoten zugegriffen werden kann.
   - **ES-NETAPP-06-MIB.mib**: Definiert Objekte und Benachrichtigungen für Geräte auf Basis der E-Serie.
   - **MIB_1_10.zip**: Definiert Objekte und Benachrichtigungen für Appliances mit einer BMC Schnittstelle.

   Sie können auf jedem StorageGRID -Knoten auch am folgenden Speicherort auf MIB-Dateien zugreifen: `/usr/share/snmp/mibs`

3. So extrahieren Sie die StorageGRID OIDs aus der MIB-Datei:

   a. Holen Sie sich die OID des Stammverzeichnisses der StorageGRID -MIB:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Ergebnis: `.1.3.6.1.4.1.789.28669` (`28669` ist immer die OID für StorageGRID)

   a. Suchen Sie im gesamten Baum nach der StorageGRID -OID (mithilfe `paste` zum Verbinden von Zeilen):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

Der `snmptranslate` Der Befehl verfügt über viele Optionen, die zum Erkunden der MIB nützlich sind. Dieser Befehl ist auf jedem StorageGRID -Knoten verfügbar.

Inhalt der MIB-Datei

Alle Objekte befinden sich unter der StorageGRID -OID.

Objektname	Objekt-ID (OID)	Beschreibung
		Das MIB-Modul für NetApp StorageGRID Einheiten.

MIB-Objekte

Objektname	Objekt-ID (OID)	Beschreibung
activeAlertCount		Die Anzahl der aktiven Warnungen in der activeAlertTable.
aktiveAlarmtabelle		Eine Tabelle mit aktiven Warnungen in StorageGRID.
aktiveAlertId		Die ID der Warnung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
activeAlertName		Der Name der Warnung.
activeAlertInstance		Der Name der Entität, die die Warnung generiert hat, normalerweise der Knotenname.
activeAlertSeverity		Der Schweregrad der Warnung.
activeAlertStartTime		Datum und Uhrzeit der Auslösung des Alarms.

Benachrichtigungstypen (Traps)

Alle Benachrichtigungen enthalten die folgenden Variablen als Varbinds:

- aktiveAlertId
- activeAlertName
- activeAlertInstance
- activeAlertSeverity
- activeAlertStartTime

Benachrichtigungstyp	Objekt-ID (OID)	Beschreibung
aktiver MinorAlarm		Eine Warnung mit geringem Schweregrad
aktiver MajorAlert		Eine Warnung mit hohem Schweregrad
aktivKritischerAlarm		Eine Warnung mit kritischem Schweregrad

Sammeln Sie zusätzliche StorageGRID Daten

Verwenden Sie Diagramme und Grafiken

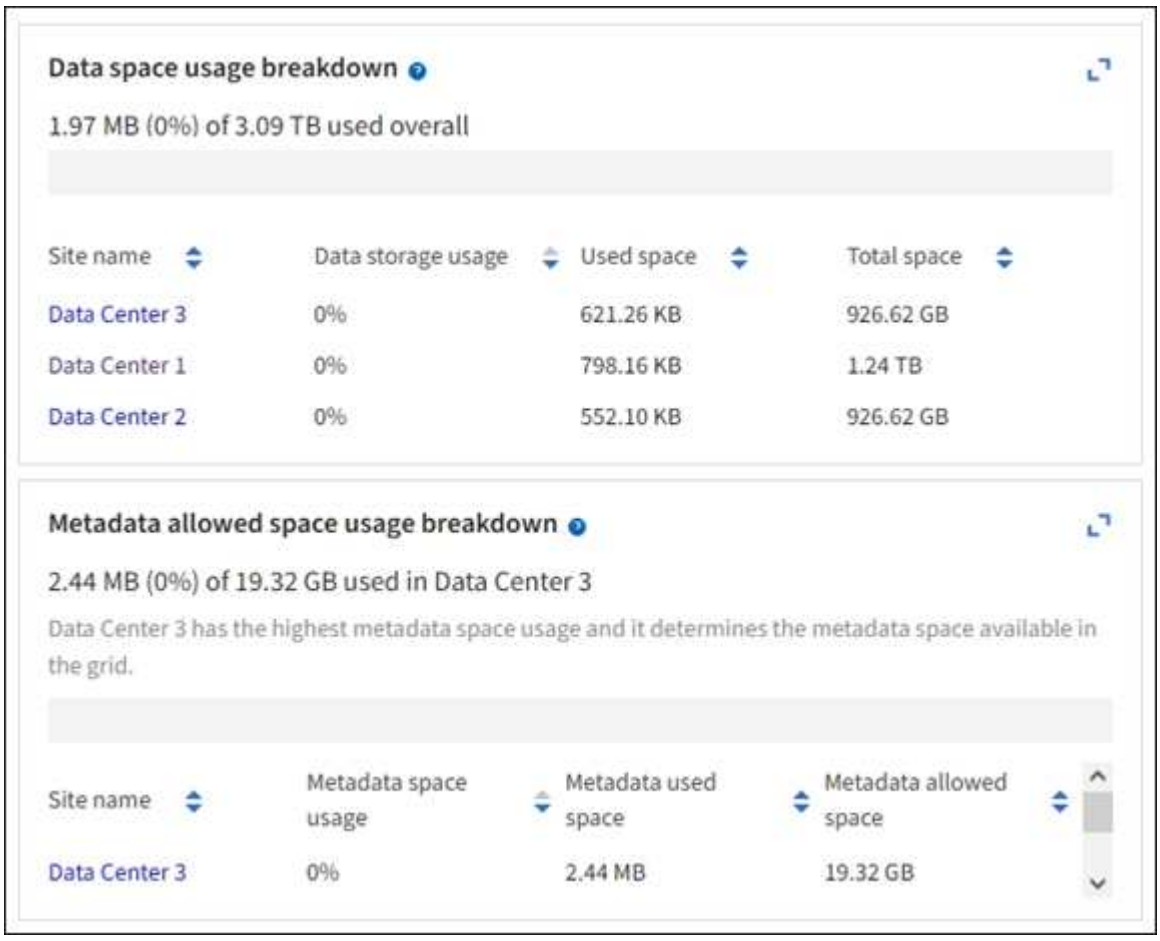
Mithilfe von Diagrammen und Berichten können Sie den Zustand des StorageGRID -Systems überwachen und Probleme beheben.

Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispiel-Screenshots auf dieser Seite überein.

Diagrammtypen

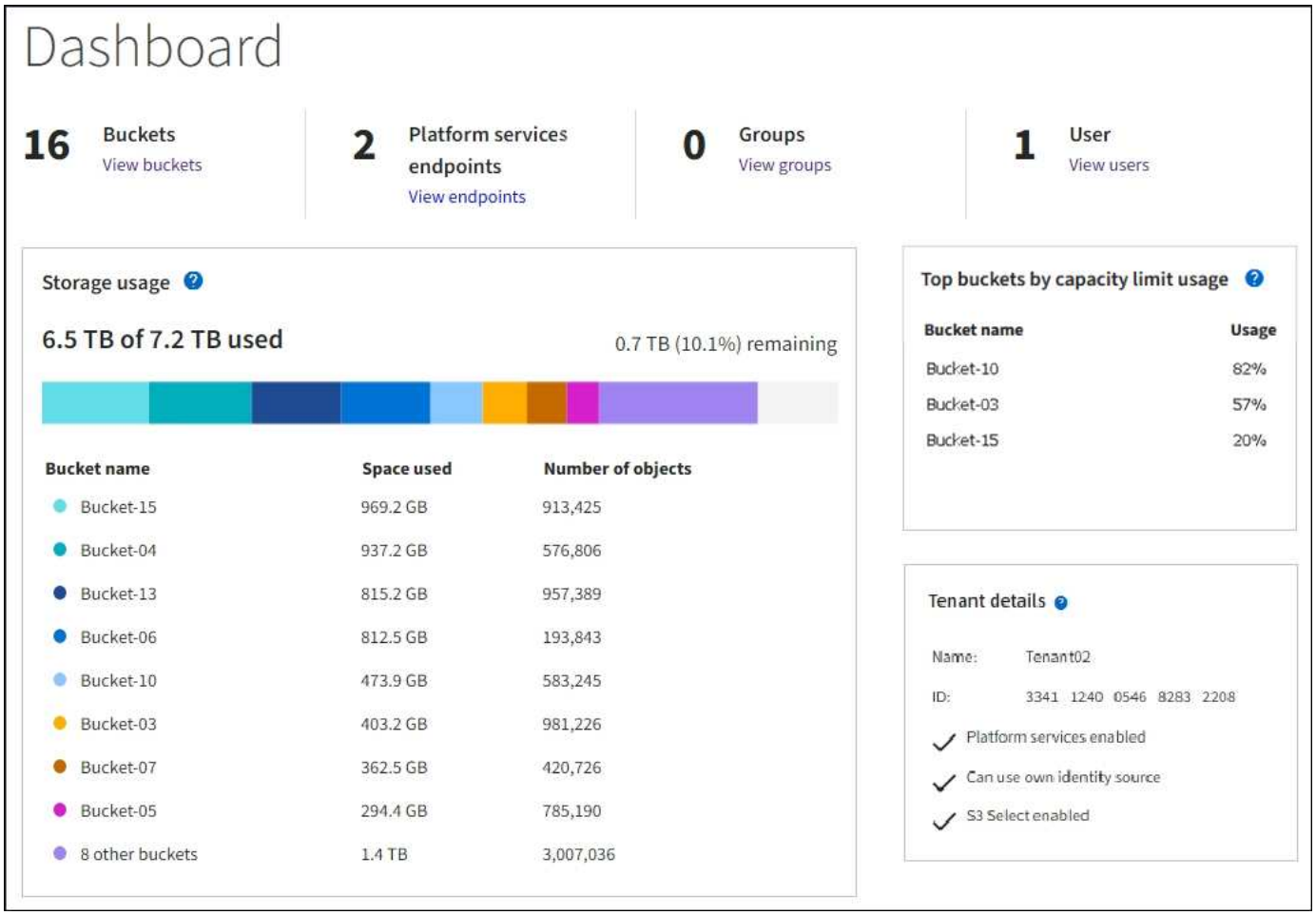
Diagramme und Grafiken fassen die Werte bestimmter StorageGRID -Metriken und -Attribute zusammen.

Das Grid Manager-Dashboard enthält Karten, die den verfügbaren Speicher für das Grid und jede Site zusammenfassen.



Das Speichernutzungsfenster im Tenant Manager-Dashboard zeigt Folgendes an:

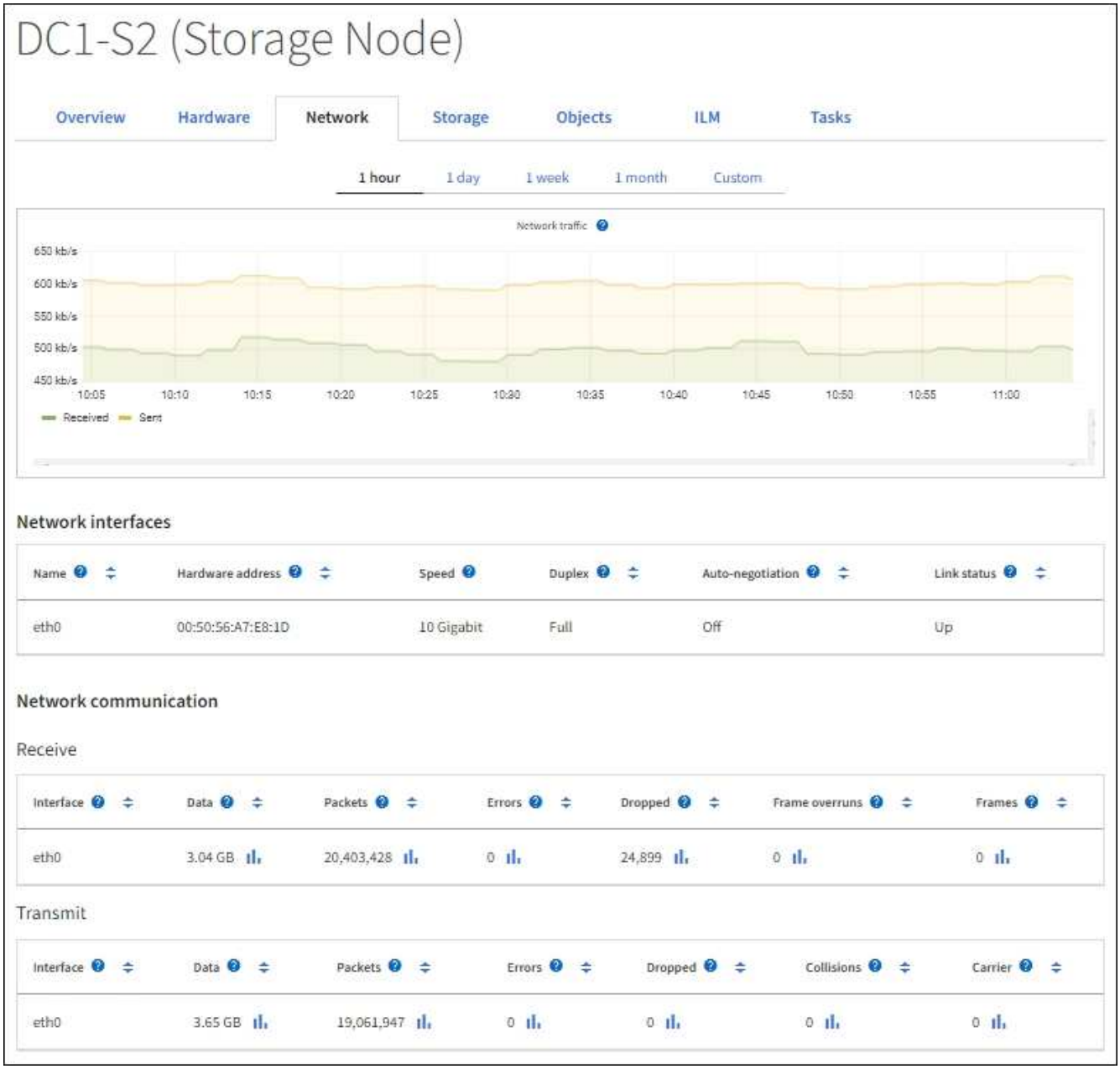
- Eine Liste der größten Buckets (S3) oder Container (Swift) für den Mandanten
- Ein Balkendiagramm, das die relativen Größen der größten Eimer oder Behälter darstellt
- Die insgesamt verwendete Speicherplatzmenge und, falls ein Kontingent festgelegt ist, die Menge und der Prozentsatz des verbleibenden Speicherplatzes



Darüber hinaus sind auf der Seite „Knoten“ und auf der Seite **SUPPORT** > **Tools** > **Grid-Topologie** Diagramme verfügbar, die zeigen, wie sich die Metriken und Attribute von StorageGRID im Laufe der Zeit ändern.

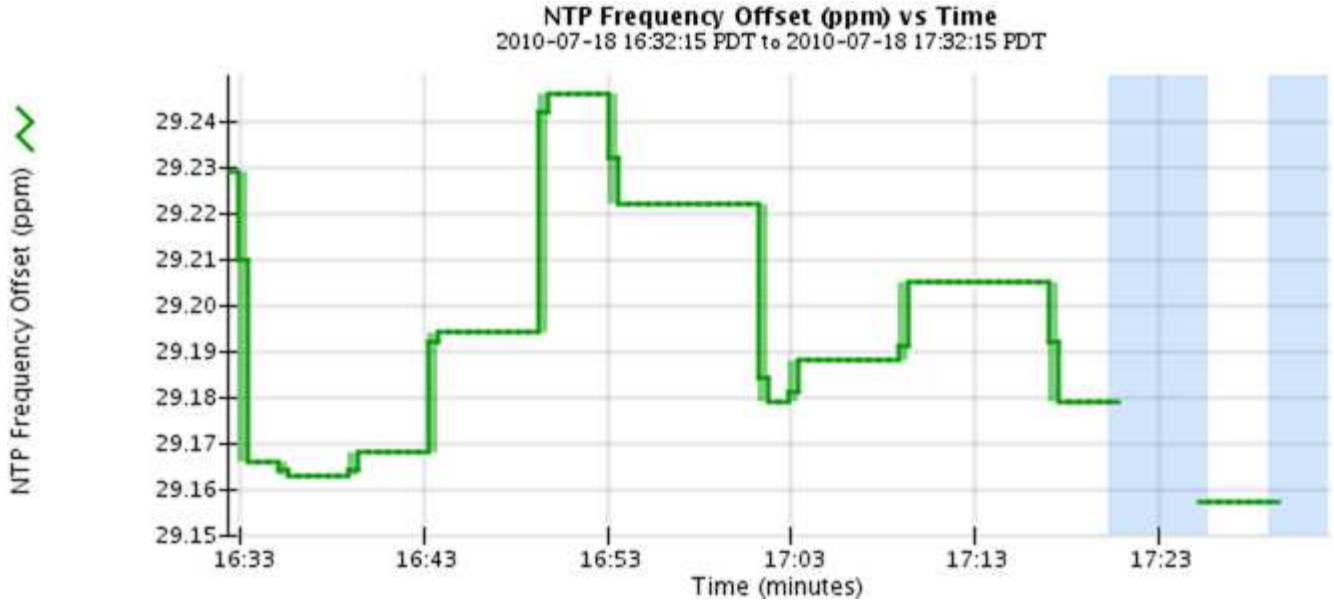
Es gibt vier Arten von Diagrammen:

- **Grafana-Diagramme**: Die auf der Knotenseite angezeigten Grafana-Diagramme werden verwendet, um die Werte der Prometheus-Metriken im Zeitverlauf darzustellen. Beispielsweise enthält die Registerkarte **NODES** > **Network** für einen Storage Node ein Grafana-Diagramm für den Netzwerkverkehr.

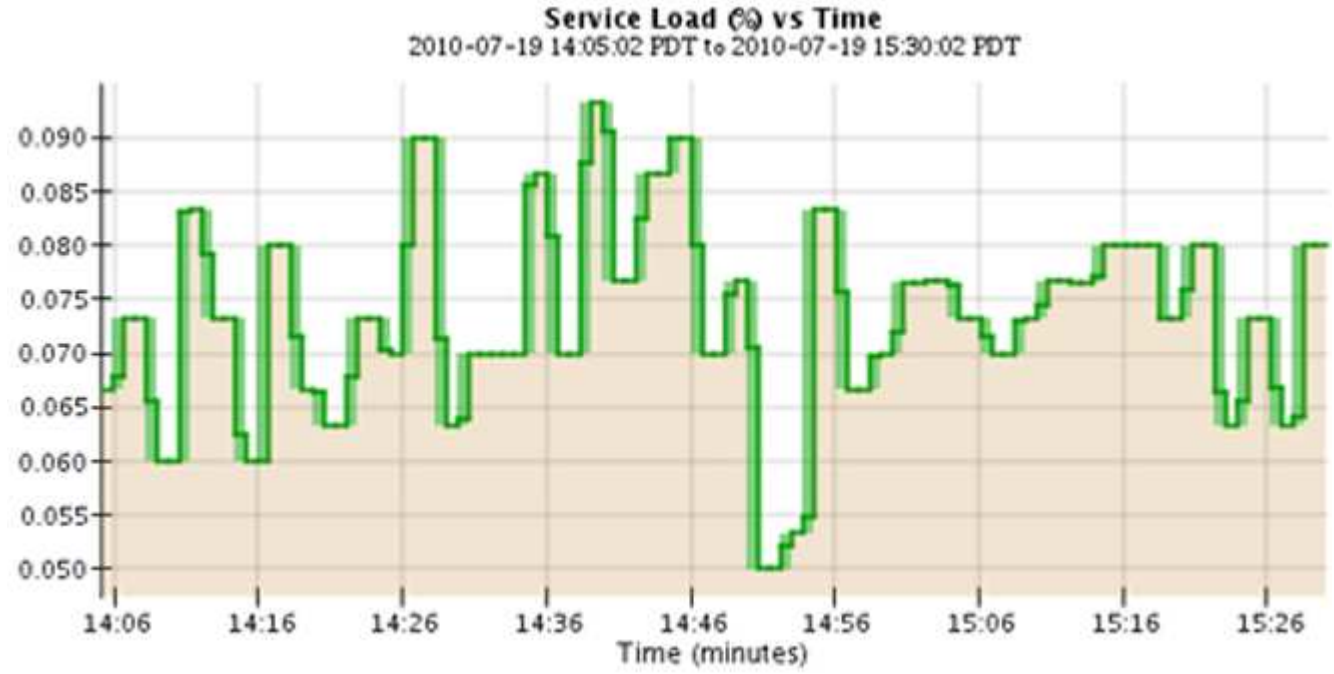


Grafana-Diagramme sind auch in den vorgefertigten Dashboards enthalten, die auf der Seite **SUPPORT** > **Tools** > **Metriken** verfügbar sind.

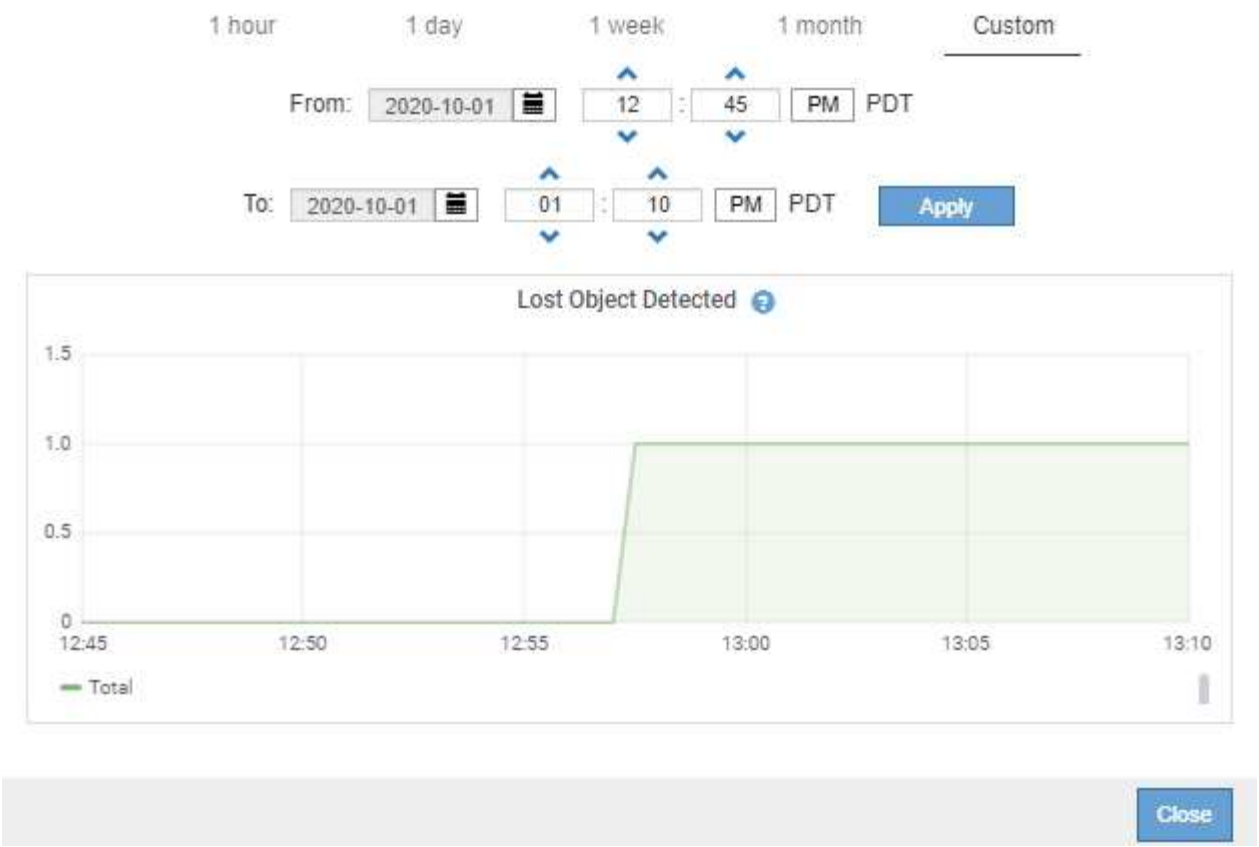
- **Liniendiagramme**: Verfügbar auf der Knotenseite und auf der Seite **SUPPORT** > **Tools** > **Gittertopologie** (wählen Sie das Diagrammsymbol nach einem Datenwert) werden Liniendiagramme verwendet, um die Werte von StorageGRID -Attributen darzustellen, die einen Einheitswert haben (z. B. NTP-Frequenzversatz in ppm). Die Wertänderungen werden in regelmäßigen Datenintervallen (Bins) über die Zeit aufgetragen.



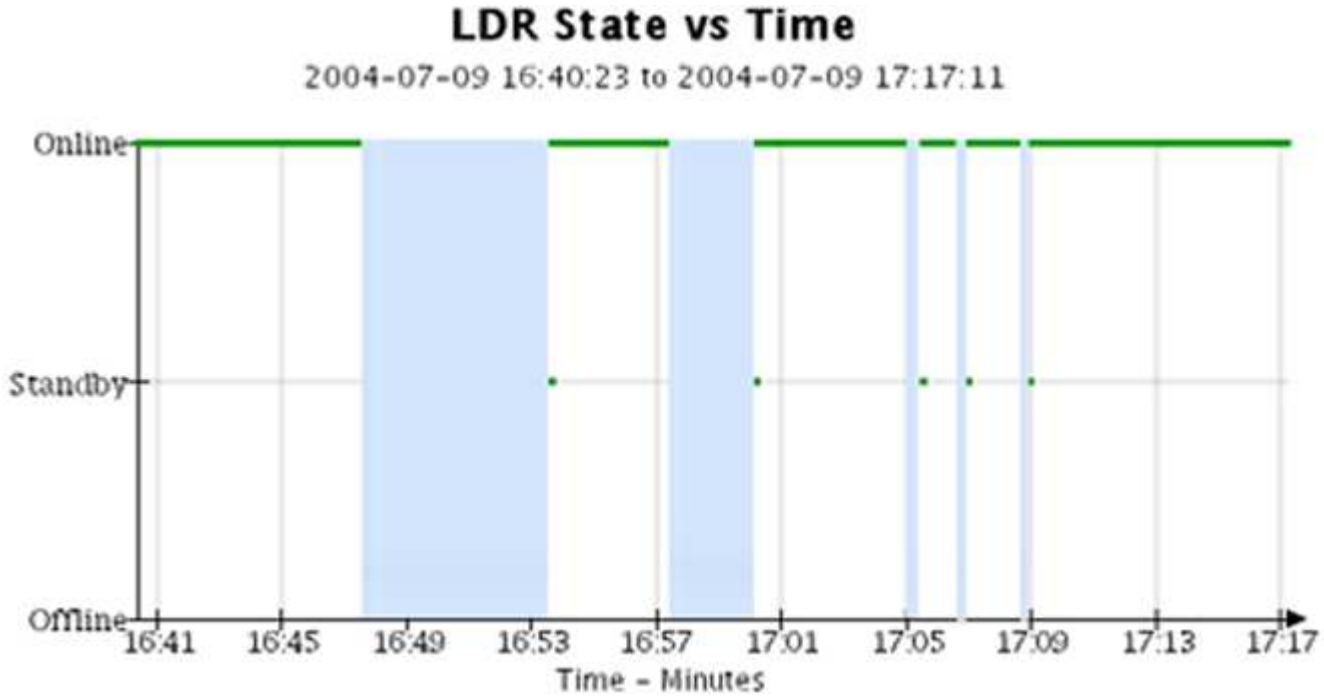
- **Flächendiagramme**: Verfügbar auf der Seite Knoten und auf der Seite **SUPPORT** > **Tools** > **Gittertopologie** (wählen Sie das Diagrammsymbol nach einem Datenwert) werden Flächendiagramme verwendet, um volumetrische Attributmengen wie Objektanzahlen oder Betriebslastwerte darzustellen. Flächendiagramme ähneln Liniendiagrammen, weisen jedoch unterhalb der Linie eine hellbraune Schattierung auf. Die Wertänderungen werden in regelmäßigen Datenintervallen (Bins) über die Zeit aufgetragen.



- Einige Diagramme sind mit einem anderen Diagrammsymbol gekennzeichnet und haben ein anderes Format:



- **Zustandsdiagramm**: Verfügbar auf der Seite **SUPPORT** > **Tools** > **Gittertopologie** (wählen Sie das Diagrammsymbol nach einem Datenwert) werden Zustandsdiagramme verwendet, um Attributwerte darzustellen, die unterschiedliche Zustände darstellen, wie z. B. einen Dienstzustand, der online, Standby oder offline sein kann. Zustandsgraphen ähneln Liniengraphen, der Übergang ist jedoch diskontinuierlich, d. h. der Wert springt von einem Zustandswert zum anderen.



Ähnliche Informationen

- "Anzeigen der Seite „Knoten“"
- "Den Netztopologie-Baum anzeigen"
- "Überprüfen der Supportmetriken"

Diagrammlegende

Die zum Zeichnen von Diagrammen verwendeten Linien und Farben haben eine bestimmte Bedeutung.

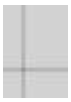
Beispiel	Bedeutung
	Die gemeldeten Attributwerte werden mithilfe dunkelgrüner Linien dargestellt.
	Eine hellgrüne Schattierung um dunkelgrüne Linien weist darauf hin, dass die tatsächlichen Werte in diesem Zeitbereich variieren und für eine schnellere Darstellung in „Binnings“ zusammengefasst wurden. Die dunkle Linie stellt den gewichteten Durchschnitt dar. Der hellgrüne Bereich gibt die Maximal- und Minimalwerte innerhalb des Behälters an. Für Flächendiagramme wird eine hellbraune Schattierung verwendet, um volumetrische Daten anzuzeigen.
	Leere Bereiche (keine dargestellten Daten) zeigen an, dass die Attributwerte nicht verfügbar waren. Der Hintergrund kann blau, grau oder eine Mischung aus Grau und Blau sein, je nach Status des Dienstes, der das Attribut meldet.
	Eine hellblaue Schattierung weist darauf hin, dass einige oder alle Attributwerte zu diesem Zeitpunkt unbestimmt waren. Das Attribut meldete keine Werte, weil sich der Dienst in einem unbekannten Zustand befand.
	Eine graue Schattierung weist darauf hin, dass einige oder alle Attributwerte zu diesem Zeitpunkt nicht bekannt waren, da der Dienst, der die Attribute meldete, administrativ nicht erreichbar war.
	Eine Mischung aus grauer und blauer Schattierung weist darauf hin, dass einige der Attributwerte zu diesem Zeitpunkt unbestimmt waren (weil sich der Dienst in einem unbekannten Zustand befand), während andere nicht bekannt waren, weil der Dienst, der die Attribute meldete, administrativ nicht erreichbar war.

Diagramme und Grafiken anzeigen

Die Seite „Knoten“ enthält die Diagramme und Grafiken, auf die Sie regelmäßig zugreifen sollten, um Attribute wie Speicherkapazität und Durchsatz zu überwachen. In einigen Fällen, insbesondere bei der Zusammenarbeit mit dem technischen Support, können Sie über die Seite **SUPPORT** > **Tools** > **Grid-Topologie** auf zusätzliche Diagramme zugreifen.

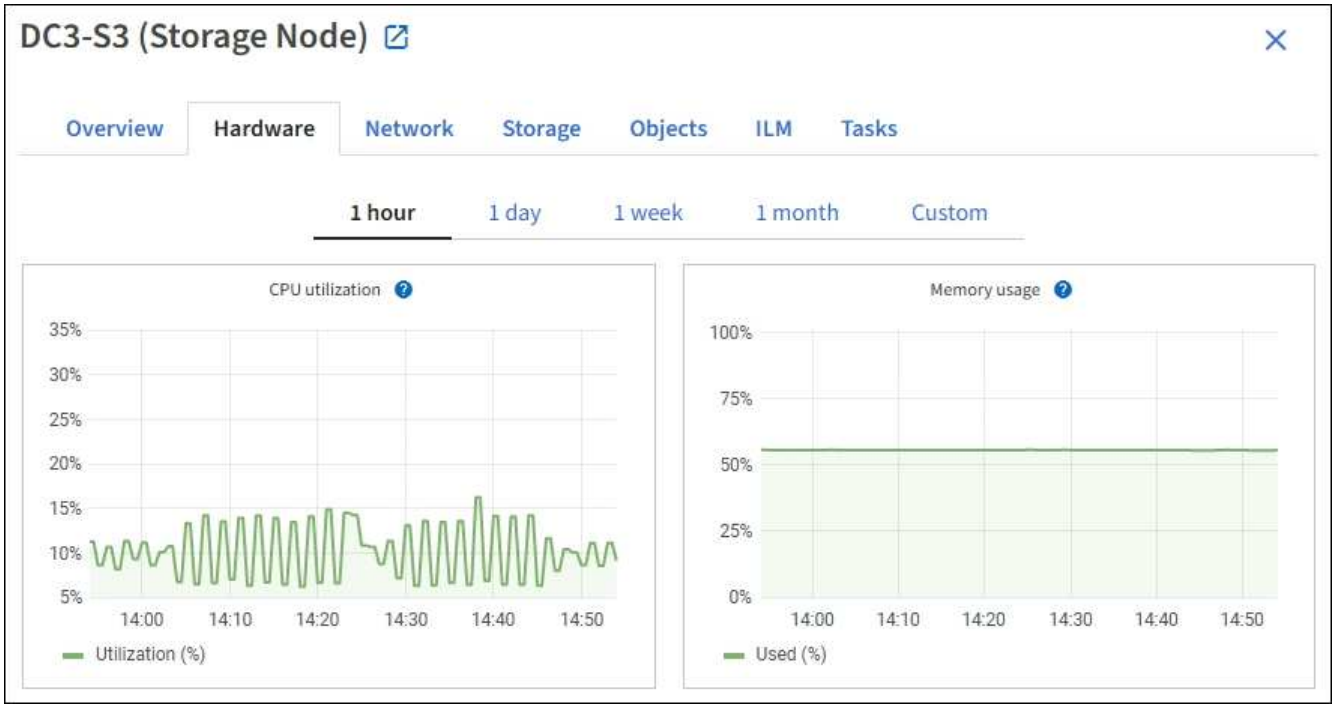
Bevor Sie beginnen

Sie müssen beim Grid Manager mit einem"unterstützter Webbrowser" .

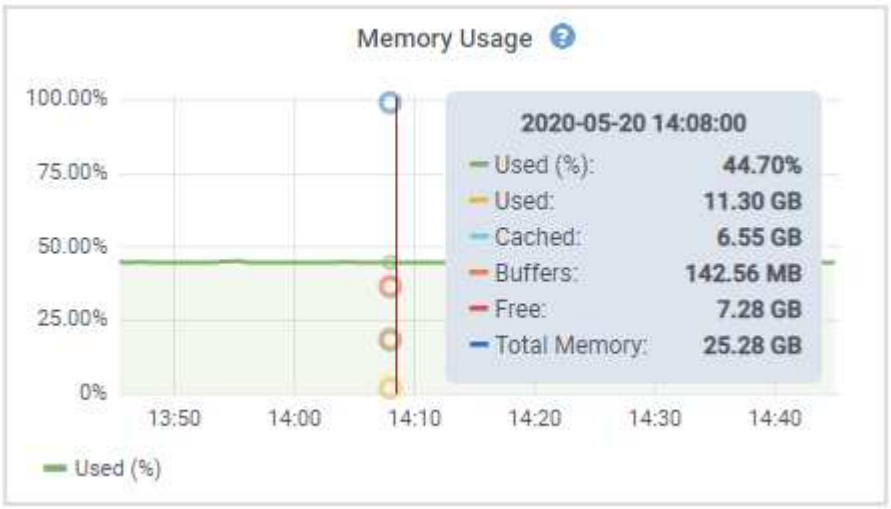
Schritte

1. Wählen Sie **NODES**. Wählen Sie dann einen Knoten, eine Site oder das gesamte Raster aus.
2. Wählen Sie die Registerkarte aus, zu der Sie Informationen anzeigen möchten.

Einige Registerkarten enthalten ein oder mehrere Grafana-Diagramme, mit denen die Werte der Prometheus-Metriken im Zeitverlauf dargestellt werden. Beispielsweise enthält die Registerkarte **KNOTEN** > **Hardware** für einen Knoten zwei Grafana-Diagramme.



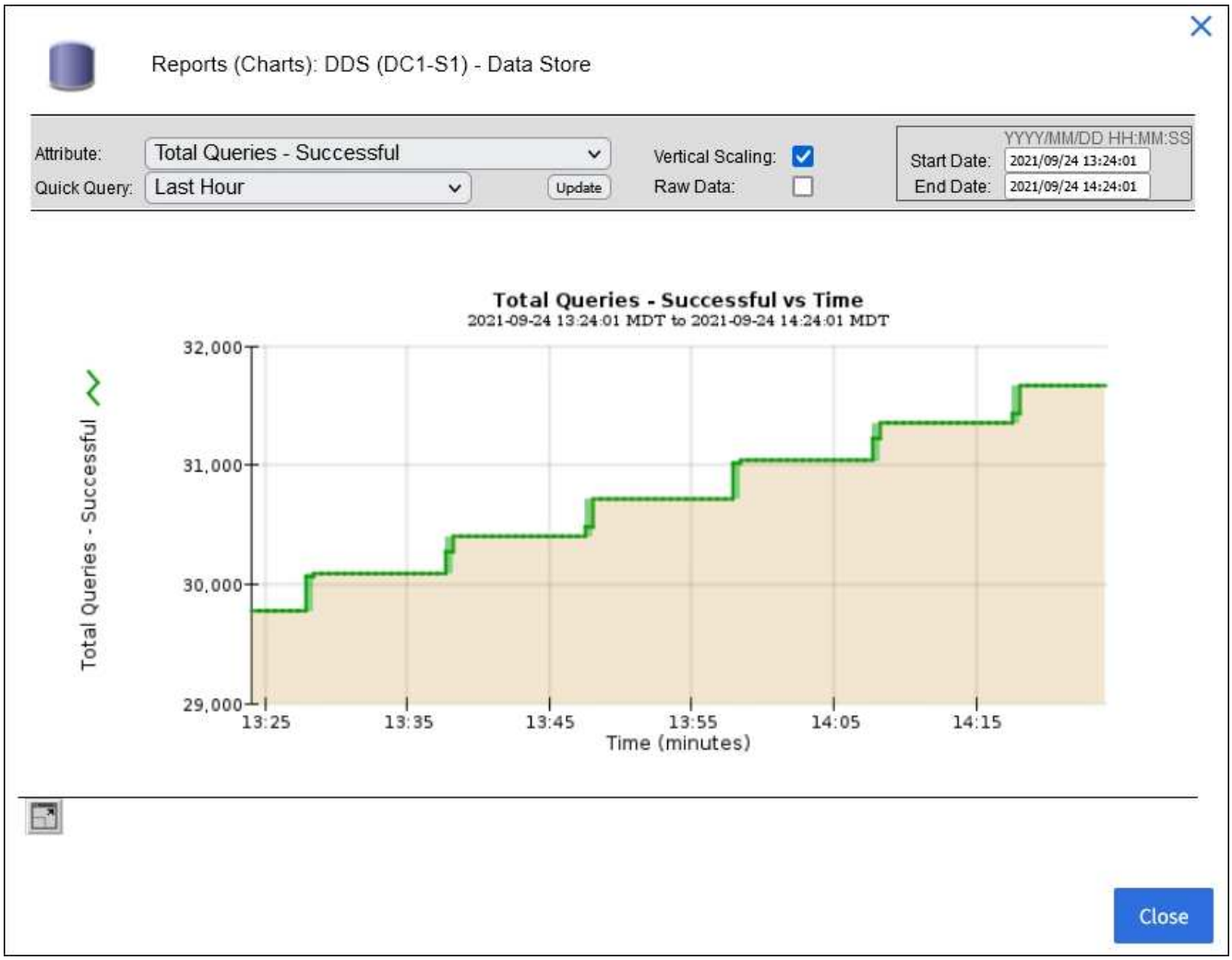
3. Optional können Sie den Cursor über dem Diagramm positionieren, um detailliertere Werte für einen bestimmten Zeitpunkt anzuzeigen.

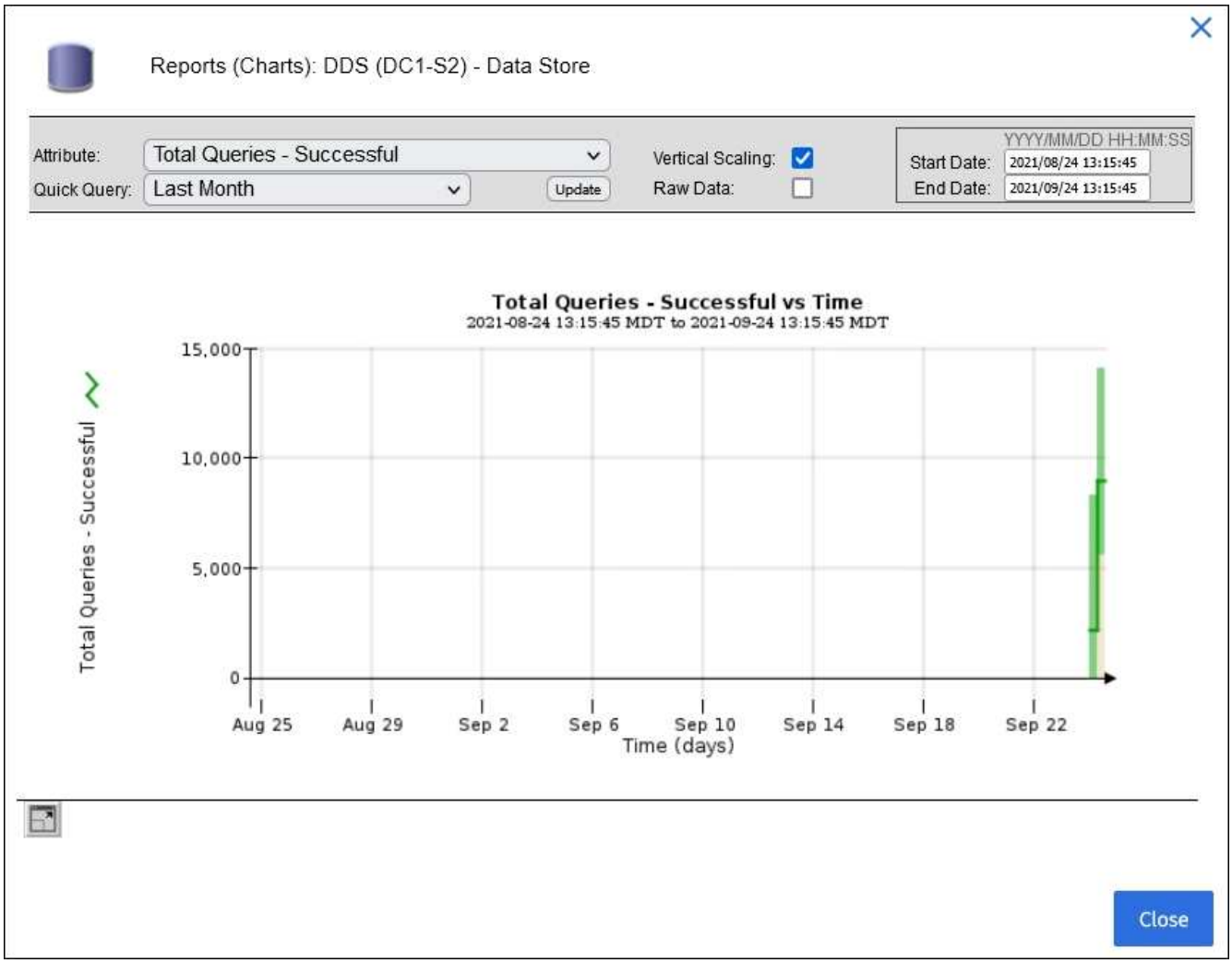


4. Bei Bedarf können Sie häufig ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Wählen Sie in der Tabelle auf der Seite „Knoten“ das Diagrammsymbol rechts neben dem Attributnamen.

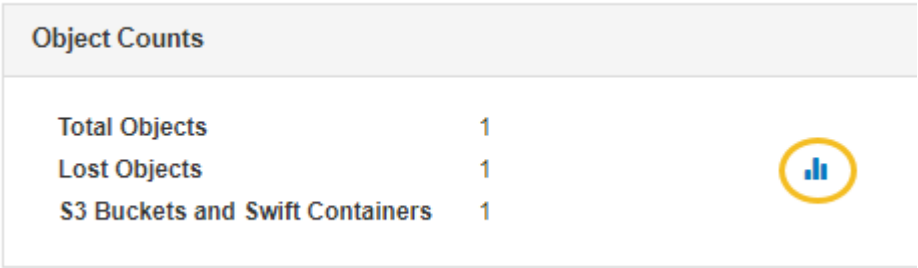
> Diagramme sind nicht für alle Metriken und Attribute verfügbar.

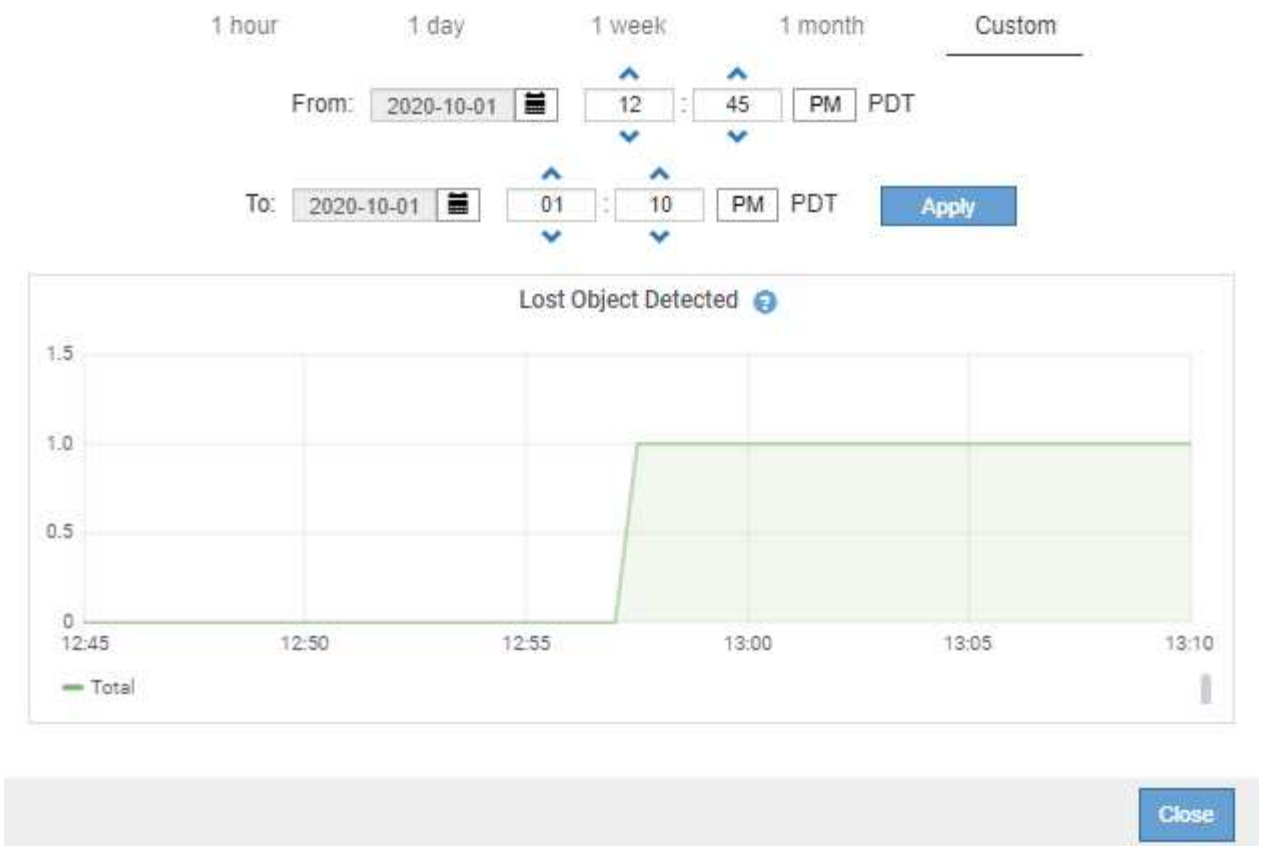
Beispiel 1: Auf der Registerkarte „Objekte“ für einen Speicherknoten können Sie das Diagrammsymbol auswählen um die Gesamtzahl der erfolgreichen Metadatenspeicherabfragen für den Speicherknoten anzuzeigen.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

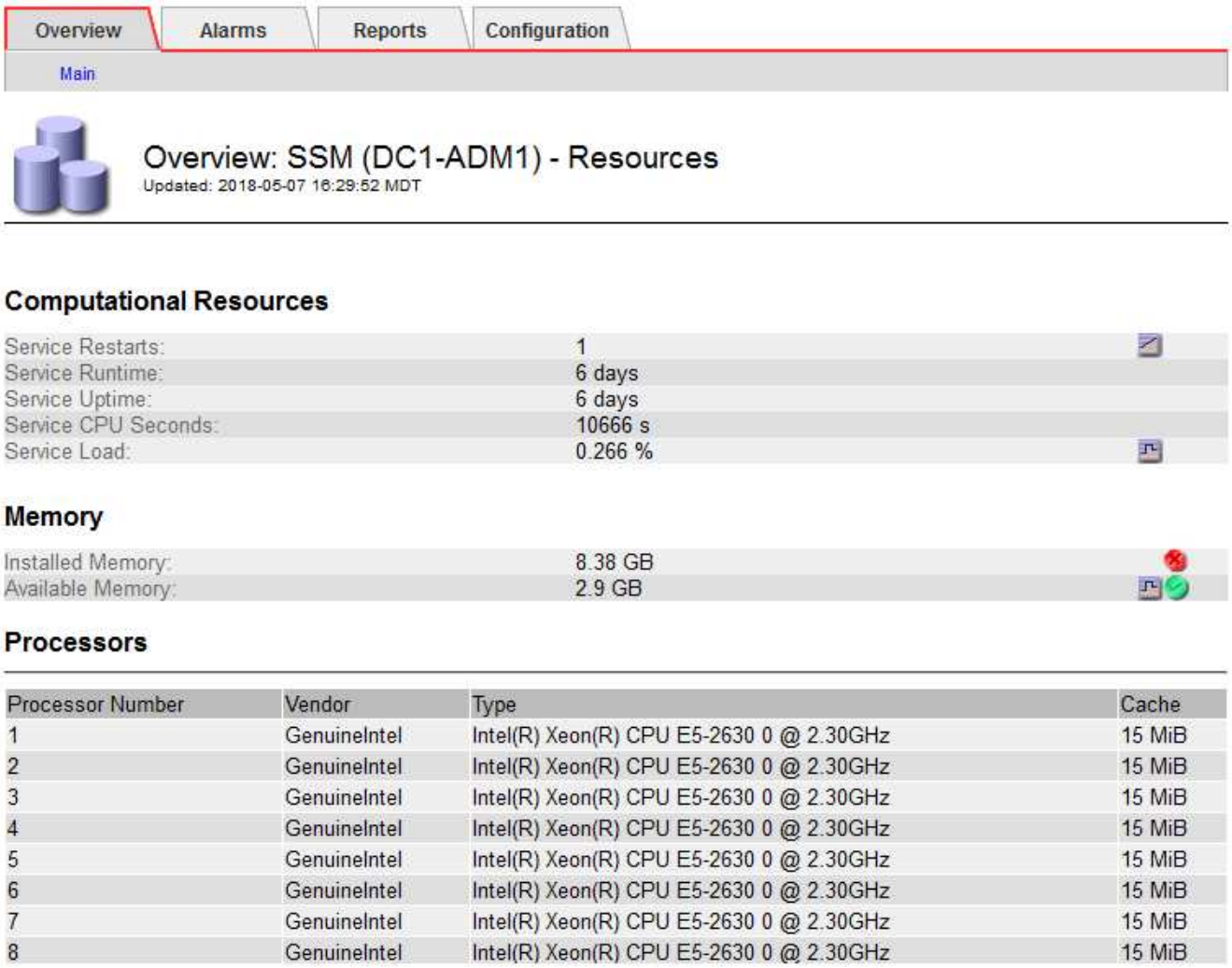


Beispiel 2: Auf der Registerkarte „Objekte“ für einen Speicherknoten können Sie das Diagrammsymbol auswählen um das Grafana-Diagramm mit der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte anzuzeigen.





5. Um Diagramme für Attribute anzuzeigen, die nicht auf der Knotenseite angezeigt werden, wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
6. Wählen Sie ***Grid-Knoten*** > ***Komponente oder Dienst*** > **Übersicht** > **Haupt**.



7. Wählen Sie das Diagrammsymbol neben dem Attribut.

   Die Anzeige wechselt automatisch zur Seite **Berichte** > **Diagramme**. Das Diagramm zeigt die Daten des Attributs für den letzten Tag.

Diagramme erstellen

Diagramme zeigen eine grafische Darstellung von Attributdatenwerten. Sie können über einen Rechenzentrumsstandort, einen Netzknoten, eine Komponente oder einen Dienst berichten.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***Rasterknoten*** > ***Komponente oder Dienst*** > **Berichte** > **Diagramme**.
3. Wählen Sie aus der Dropdown-Liste **Attribut** das Attribut aus, über das berichtet werden soll.
4. Um zu erzwingen, dass die Y-Achse bei Null beginnt, deaktivieren Sie das Kontrollkästchen **Vertikale Skalierung**.

5. Um Werte mit voller Genauigkeit anzuzeigen, aktivieren Sie das Kontrollkästchen **Rohdaten**. Um Werte auf maximal drei Dezimalstellen zu runden (z. B. für als Prozentsätze gemeldete Attribute), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
6. Wählen Sie aus der Dropdown-Liste **Schnellabfrage** den Zeitraum aus, über den berichtet werden soll.

   Wählen Sie die Option „Benutzerdefinierte Abfrage“, um einen bestimmten Zeitraum auszuwählen.

   Das Diagramm wird nach einigen Augenblicken angezeigt. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein.

7. Wenn Sie „Benutzerdefinierte Abfrage“ ausgewählt haben, passen Sie den Zeitraum für das Diagramm an, indem Sie das **Startdatum** und das **Enddatum** eingeben.

   Verwenden Sie das Format *YYYY/MM/DDHH:MM:SS* in Ortszeit. Um dem Format zu entsprechen, sind führende Nullen erforderlich. Beispielsweise schlägt die Validierung bei 2017/4/6 7:30:00 fehl. Das richtige Format ist: 06.04.2017 07:30:00.

8. Wählen Sie **Aktualisieren**.

   Nach einigen Sekunden wird ein Diagramm erstellt. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein. Abhängig von der für die Abfrage eingestellten Zeitdauer wird entweder ein Rohtextbericht oder ein aggregierter Textbericht angezeigt.

Verwenden Sie Textberichte

Textberichte zeigen eine Textdarstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Abhängig vom Zeitraum, über den Sie berichten, werden zwei Arten von Berichten generiert: Rohtextberichte für Zeiträume unter einer Woche und aggregierte Textberichte für Zeiträume über einer Woche.

Rohtextberichte

Ein Rohtextbericht zeigt Details zum ausgewählten Attribut an:

- Empfangszeit: Lokales Datum und Uhrzeit, zu der ein Beispielwert der Daten eines Attributs vom NMS-Dienst verarbeitet wurde.
- Abtastzeit: Lokales Datum und Uhrzeit, zu der ein Attributwert abgetastet oder an der Quelle geändert wurde.
- Wert: Attributwert zum Zeitpunkt der Abtastung.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

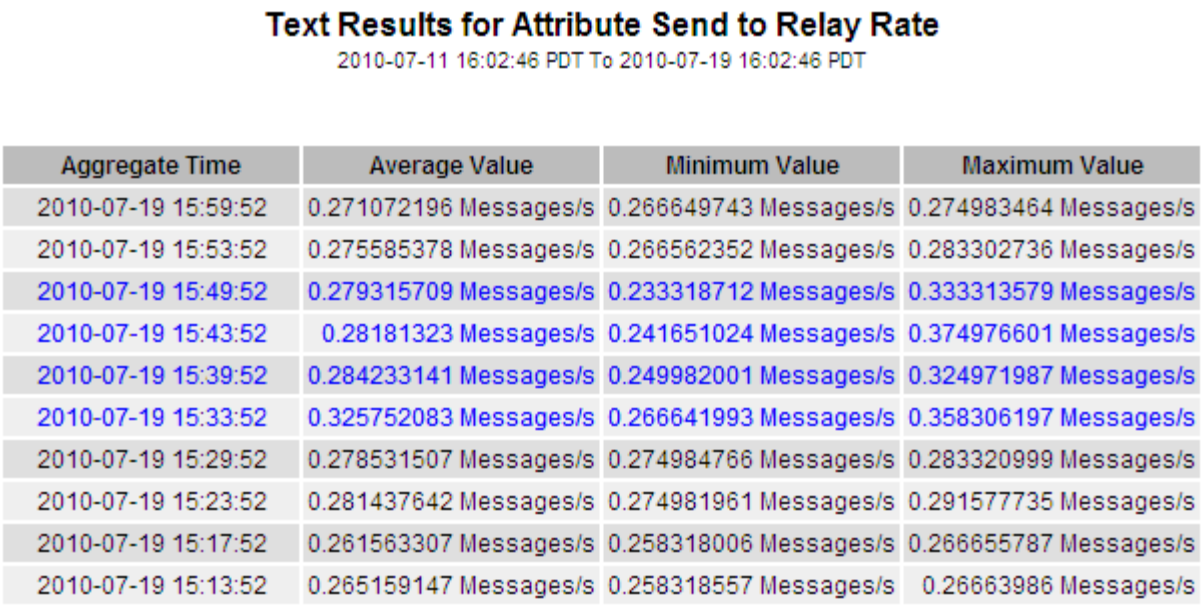
Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Aggregierte Textberichte

Ein aggregierter Textbericht zeigt Daten über einen längeren Zeitraum (normalerweise eine Woche) an als ein Rohtextbericht. Jeder Eintrag ist das Ergebnis der Zusammenfassung mehrerer Attributwerte (eine Ansammlung von Attributwerten) durch den NMS-Dienst im Laufe der Zeit in einen einzigen Eintrag mit Durchschnitts-, Maximal- und Minimalwerten, die aus der Ansammlung abgeleitet werden.

Jeder Eintrag zeigt die folgenden Informationen an:

- Aggregierte Zeit: Letztes lokales Datum und Uhrzeit, zu der der NMS-Dienst eine Reihe geänderter Attributwerte aggregiert (gesammelt) hat.
- Durchschnittswert: Der Durchschnitt des Attributwerts über den aggregierten Zeitraum.
- Mindestwert: Der Mindestwert über den aggregierten Zeitraum.
- Maximalwert: Der Maximalwert über den aggregierten Zeitraum.



Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Textberichte erstellen

Textberichte zeigen eine Textdarstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Sie können über einen Rechenzentrumsstandort, einen Netzknoten, eine Komponente oder einen Dienst berichten.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Bei Attributdaten, bei denen davon auszugehen ist, dass sie sich ständig ändern, werden diese Attributdaten vom NMS-Dienst (an der Quelle) in regelmäßigen Abständen abgetastet. Bei Attributdaten, die sich selten ändern (z. B. Daten, die auf Ereignissen wie Zustands- oder Statusänderungen basieren), wird bei einer Wertänderung ein Attributwert an den NMS-Dienst gesendet.

Die Art des angezeigten Berichts hängt vom konfigurierten Zeitraum ab. Standardmäßig werden aggregierte Textberichte für Zeiträume von mehr als einer Woche erstellt.

Grauer Text zeigt an, dass der Dienst während der Stichprobenentnahme administrativ nicht erreichbar war. Blauer Text zeigt an, dass sich der Dienst in einem unbekannten Zustand befand.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***Grid-Knoten*** > ***Komponente oder Dienst*** > **Berichte** > **Text**.
3. Wählen Sie aus der Dropdown-Liste **Attribut** das Attribut aus, über das berichtet werden soll.
4. Wählen Sie die Anzahl der Ergebnisse pro Seite aus der Dropdown-Liste **Ergebnisse pro Seite** aus.
5. Um Werte auf maximal drei Dezimalstellen zu runden (beispielsweise bei Attributen, die als Prozentsätze angegeben werden), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
6. Wählen Sie aus der Dropdown-Liste **Schnellabfrage** den Zeitraum aus, über den berichtet werden soll.

   Wählen Sie die Option „Benutzerdefinierte Abfrage“, um einen bestimmten Zeitraum auszuwählen.

Der Bericht erscheint nach wenigen Augenblicken. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein.

7. Wenn Sie „Benutzerdefinierte Abfrage“ ausgewählt haben, müssen Sie den Berichtszeitraum anpassen, indem Sie das **Startdatum** und das **Enddatum** eingeben.

   Verwenden Sie das Format `YYYY/MM/DDHH:MM:SS` in Ortszeit. Um dem Format zu entsprechen, sind führende Nullen erforderlich. Beispielsweise schlägt die Validierung bei 2017/4/6 7:30:00 fehl. Das richtige Format ist: 06.04.2017 07:30:00.

8. Klicken Sie auf **Aktualisieren**.

   Nach wenigen Augenblicken wird ein Textbericht erstellt. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein. Abhängig von der für die Abfrage eingestellten Zeitdauer wird entweder ein Rohtextbericht oder ein aggregierter Textbericht angezeigt.

Textberichte exportieren

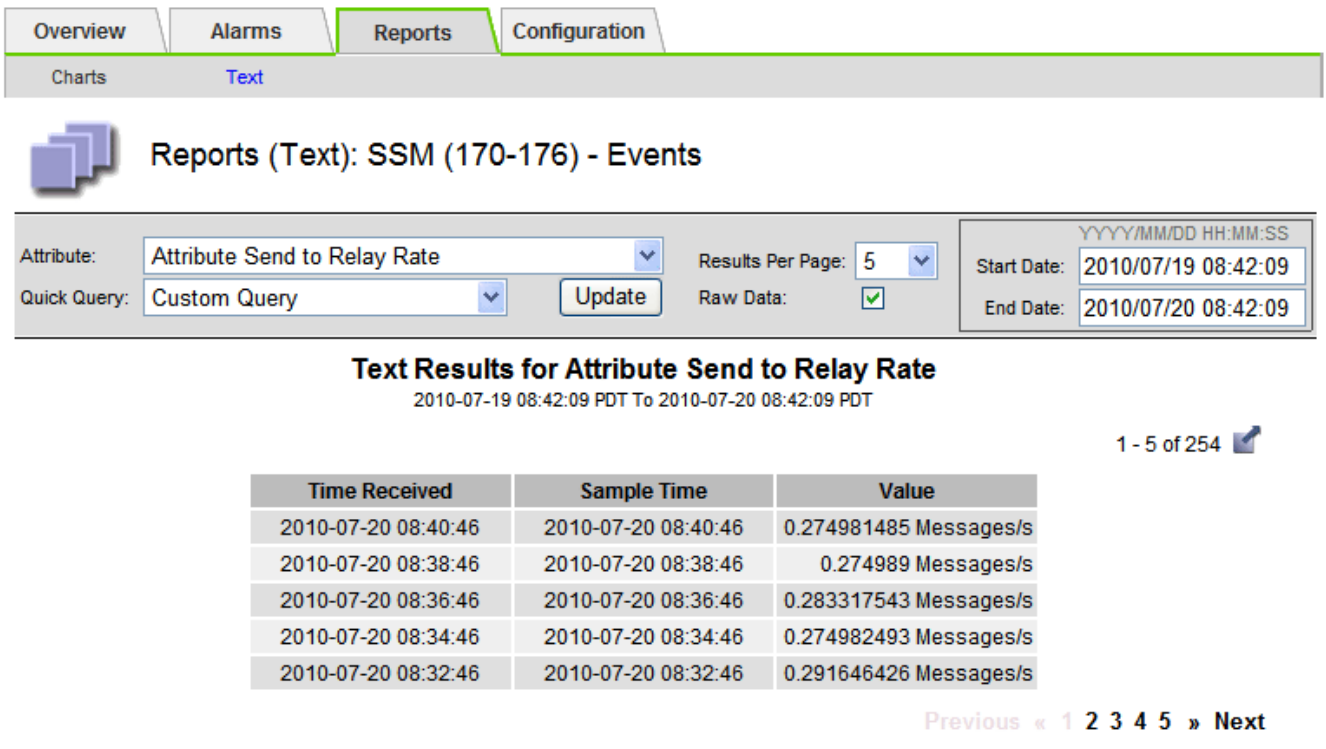
Exportierte Textberichte öffnen eine neue Browser-Registerkarte, in der Sie die Daten auswählen und kopieren können.

Informationen zu diesem Vorgang

Die kopierten Daten können dann in einem neuen Dokument (z. B. einer Tabelle) gespeichert und zur Analyse der Leistung des StorageGRID Systems verwendet werden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Erstellen Sie einen Textbericht.
3. Klicken Sie auf *Exportieren* .



Das Fenster „Textbericht exportieren“ wird geöffnet und zeigt den Bericht an.

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Wählen Sie den Inhalt des Fensters „Textbericht exportieren“ aus und kopieren Sie ihn.

   Diese Daten können nun in ein Drittdokument, beispielsweise eine Tabellenkalkulation, eingefügt werden.

Überwachen Sie die PUT- und GET-Leistung

Sie können die Leistung bestimmter Vorgänge überwachen, beispielsweise das Speichern und Abrufen von Objekten, um Änderungen zu erkennen, die möglicherweise einer weiteren Untersuchung bedürfen.

Informationen zu diesem Vorgang

Um die PUT- und GET-Leistung zu überwachen, können Sie S3-Befehle direkt von einer Workstation aus ausführen oder die Open-Source-Anwendung S3tester verwenden. Mithilfe dieser Methoden können Sie die Leistung unabhängig von externen Faktoren von StorageGRID beurteilen, beispielsweise Problemen mit einer Clientanwendung oder Problemen mit einem externen Netzwerk.

Beachten Sie beim Testen von PUT- und GET-Vorgängen die folgenden Richtlinien:

- Verwenden Sie Objektgrößen, die mit den Objekten vergleichbar sind, die Sie normalerweise in Ihr Raster aufnehmen.
- Führen Sie Vorgänge sowohl für lokale als auch für Remote-Sites durch.

Nachrichten in der"Überwachungsprotokoll" geben die Gesamtzeit an, die zum Ausführen bestimmter Vorgänge erforderlich ist. Um beispielsweise die Gesamtverarbeitungszeit für eine S3-GET-Anforderung zu ermitteln, können Sie den Wert des TIME-Attributs in der SGET-Auditnachricht überprüfen. Sie finden das TIME-Attribut auch in den Audit-Nachrichten für die folgenden S3-Operationen: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Achten Sie bei der Analyse der Ergebnisse auf die durchschnittliche Zeit, die zur Erfüllung einer Anfrage benötigt wird, sowie auf den Gesamtdurchsatz, den Sie erreichen können. Wiederholen Sie dieselben Tests regelmäßig und zeichnen Sie die Ergebnisse auf, damit Sie Trends erkennen können, die möglicherweise

einer Untersuchung bedürfen.

- Du kannst "Laden Sie S3tester von GitHub herunter" .

Überwachen von Objektüberprüfungsvorgängen

Das StorageGRID -System kann die Integrität von Objektdaten auf Speicherknoten überprüfen und sowohl auf beschädigte als auch auf fehlende Objekte prüfen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Zwei"Verifizierungsprozesse" Arbeiten Sie zusammen, um die Datenintegrität sicherzustellen:

- Die **Hintergrundprüfung** läuft automatisch und überprüft kontinuierlich die Richtigkeit der Objektdaten.

  Bei der Hintergrundüberprüfung werden alle Speicherknoten automatisch und kontinuierlich überprüft, um festzustellen, ob beschädigte Kopien replizierter und löschcodierter Objektdaten vorhanden sind. Wenn Probleme gefunden werden, versucht das StorageGRID -System automatisch, die beschädigten Objektdaten durch Kopien zu ersetzen, die an anderer Stelle im System gespeichert sind. Für Objekte in einem Cloud-Speicherpool wird keine Hintergrundüberprüfung ausgeführt.

  > Die Warnung **Unbekanntes beschädigtes Objekt erkannt** wird ausgelöst, wenn das System ein beschädigtes Objekt erkennt, das nicht automatisch korrigiert werden kann.

- Die **Objektexistenzprüfung** kann von einem Benutzer ausgelöst werden, um die Existenz (jedoch nicht die Richtigkeit) von Objektdaten schneller zu überprüfen.

  Die Objektexistenzprüfung überprüft, ob alle erwarteten replizierten Kopien von Objekten und Erasure-Coded-Fragmenten auf einem Speicherknoten vorhanden sind. Die Objektexistenzprüfung bietet eine Möglichkeit, die Integrität von Speichergeräten zu überprüfen, insbesondere wenn ein kürzlich aufgetretenes Hardwareproblem die Datenintegrität beeinträchtigt haben könnte.

Sie sollten die Ergebnisse der Hintergrundüberprüfungen und Objektexistenzprüfungen regelmäßig überprüfen. Untersuchen Sie alle Fälle beschädigter oder fehlender Objektdaten sofort, um die Grundursache zu ermitteln.

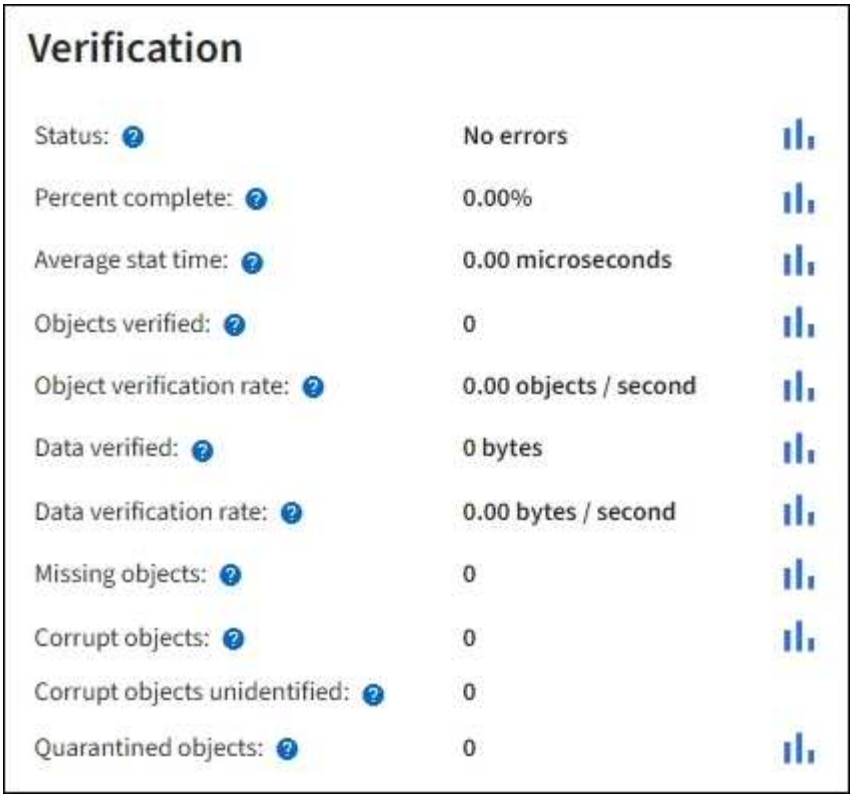
Schritte

1. Überprüfen Sie die Ergebnisse der Hintergrundüberprüfungen:

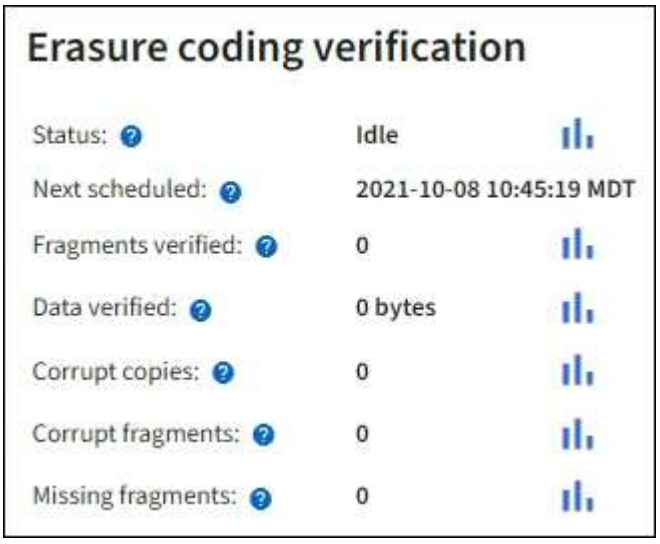
   a. Wählen Sie **NODES** > ***Storage Node*** > **Objects**.

   b. Überprüfen Sie die Überprüfungsergebnisse:

      - Um die Verifizierung der replizierten Objektdaten zu überprüfen, sehen Sie sich die Attribute im Abschnitt „Verifizierung“ an.

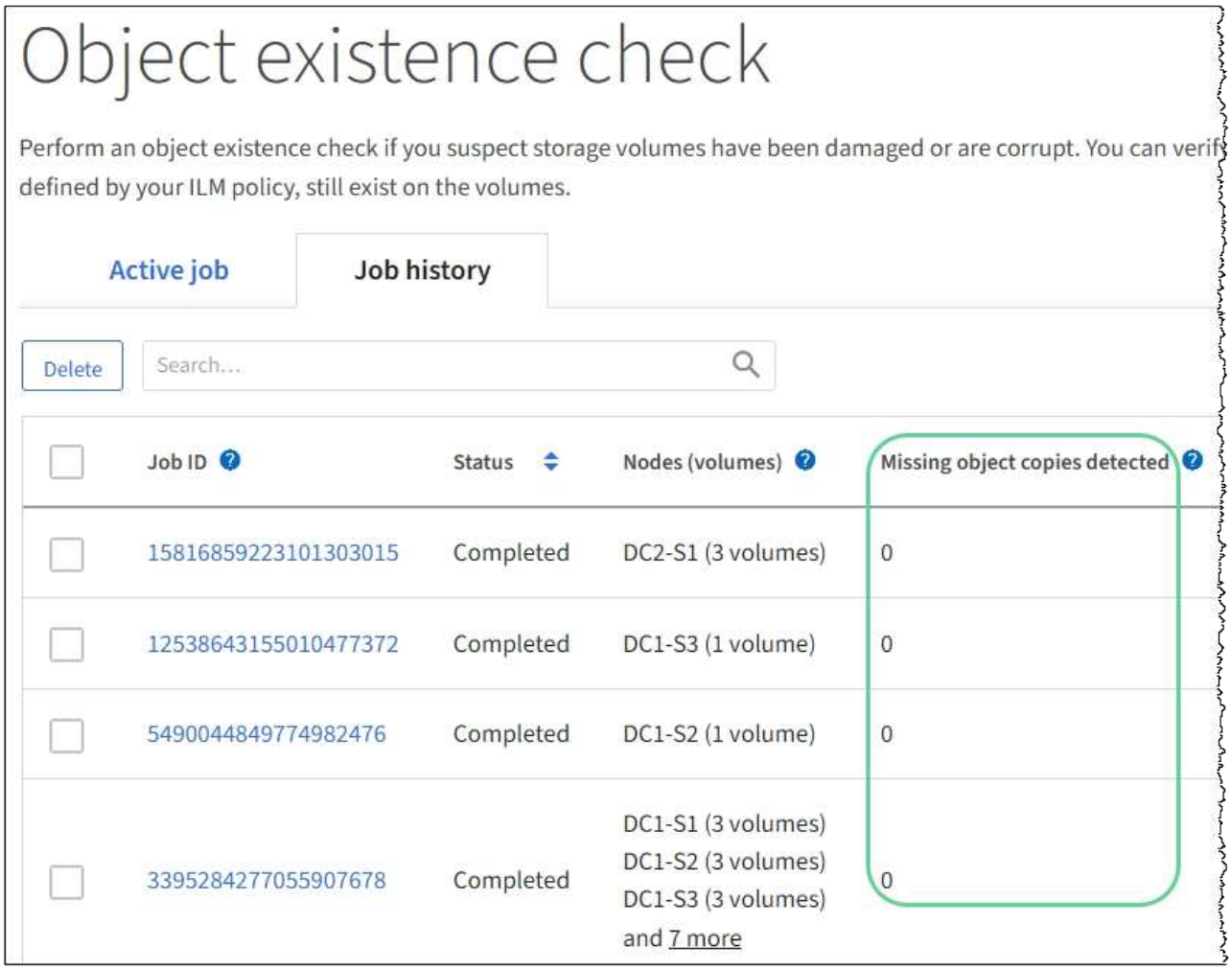


- Um die Erasure-Coding-Fragmentverifizierung zu überprüfen, wählen Sie ***Storage Node*** > **ILM** und sehen Sie sich die Attribute im Abschnitt „Erasure-Coding-Verifizierung“ an.



Wählen Sie das Fragezeichen neben dem Namen eines Attributs, um Hilfetext anzuzeigen.

2. Überprüfen Sie die Ergebnisse der Jobs zur Objektexistenzprüfung:
   a. Wählen Sie **WARTUNG** > **Objektexistenzprüfung** > **Auftragsverlauf**.
   b. Scannen Sie die Spalte „Fehlende Objektkopien erkannt“. Wenn bei einem Auftrag 100 oder mehr Objektkopien fehlen und die Warnung „Objekte verloren“ ausgelöst wurde, wenden Sie sich an den technischen Support.



Überwachen von Ereignissen

Sie können Ereignisse überwachen, die von einem Grid-Knoten erkannt werden, einschließlich benutzerdefinierter Ereignisse, die Sie erstellt haben, um Ereignisse zu verfolgen, die auf dem Syslog-Server protokolliert werden. Die im Grid Manager angezeigte Meldung „Letztes Ereignis“ bietet weitere Informationen zum aktuellsten Ereignis.

Ereignismeldungen werden auch aufgelistet in der `/var/local/log/bycast-err.log` Protokolldatei. Siehe die"Referenz zu Protokolldateien" .

Der SMTT-Alarm (Gesamtereignisse) kann wiederholt durch Probleme wie Netzwerkprobleme, Stromausfälle oder Upgrades ausgelöst werden. Dieser Abschnitt enthält Informationen zur Untersuchung von Ereignissen, damit Sie besser verstehen, warum diese Alarme aufgetreten sind. Wenn ein Ereignis aufgrund eines bekannten Problems aufgetreten ist, können die Ereigniszähler bedenkenlos zurückgesetzt werden.

Schritte

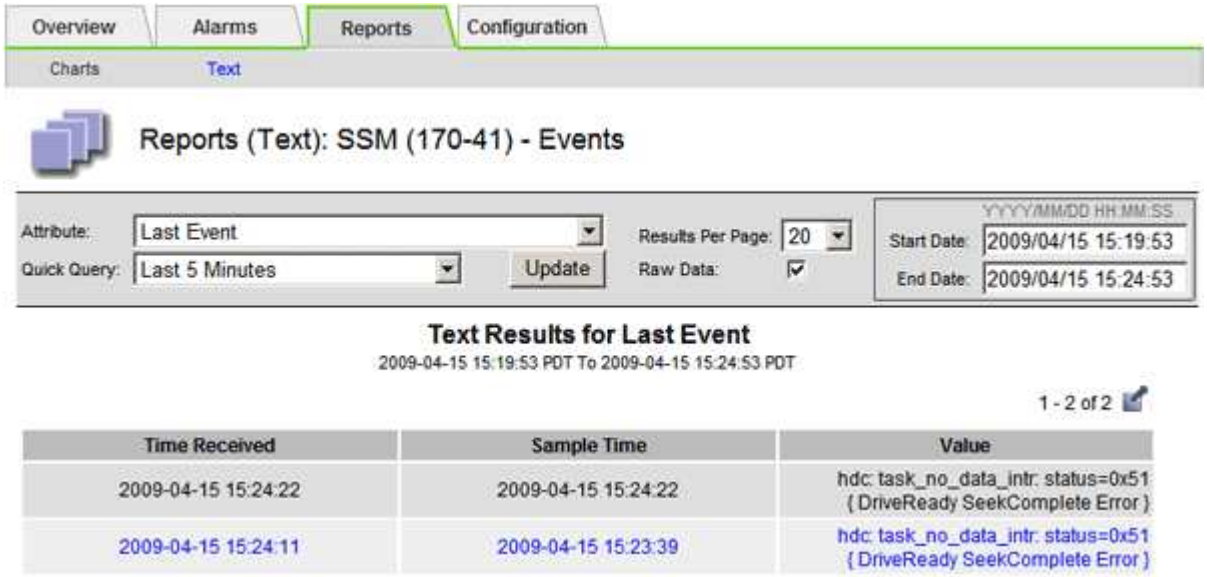
1. Überprüfen Sie die Systemereignisse für jeden Grid-Knoten:
   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
   b. Wählen Sie ***site*** > ***grid node*** > **SSM** > **Events** > **Overview** > **Main**.
2. Erstellen Sie eine Liste früherer Ereignismeldungen, um in der Vergangenheit aufgetretene Probleme

einzugrenzen:

a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
b. Wählen Sie ***site*** > ***grid node*** > **SSM** > **Events** > **Reports**.
c. Wählen Sie **Text** aus.

   Das Attribut **Letztes Ereignis** wird nicht angezeigt in der"Diagrammansicht" . So zeigen Sie es an:

d. Ändern Sie **Attribut** in **Letztes Ereignis**.
e. Wählen Sie optional einen Zeitraum für die **Schnellabfrage** aus.
f. Wählen Sie **Aktualisieren**.



Erstellen Sie benutzerdefinierte Syslog-Ereignisse

Mit benutzerdefinierten Ereignissen können Sie alle Kernel-, Daemon-, Fehler- und Benutzerereignisse auf kritischer Ebene verfolgen, die auf dem Syslog-Server protokolliert werden. Ein benutzerdefiniertes Ereignis kann nützlich sein, um das Auftreten von Systemprotokollmeldungen (und somit Netzwerksicherheitsereignissen und Hardwarefehlern) zu überwachen.

Informationen zu diesem Vorgang

Erwägen Sie die Erstellung benutzerdefinierter Ereignisse, um wiederkehrende Probleme zu überwachen. Die folgenden Überlegungen gelten für benutzerdefinierte Ereignisse.

- Nachdem ein benutzerdefiniertes Ereignis erstellt wurde, wird jedes Vorkommen davon überwacht.
- Um ein benutzerdefiniertes Ereignis basierend auf Schlüsselwörtern in der `/var/local/log/messages` Dateien müssen die Protokolle in diesen Dateien sein:
  - Vom Kernel generiert
  - Von Daemon oder Benutzerprogramm auf Fehler- oder kritischer Ebene generiert

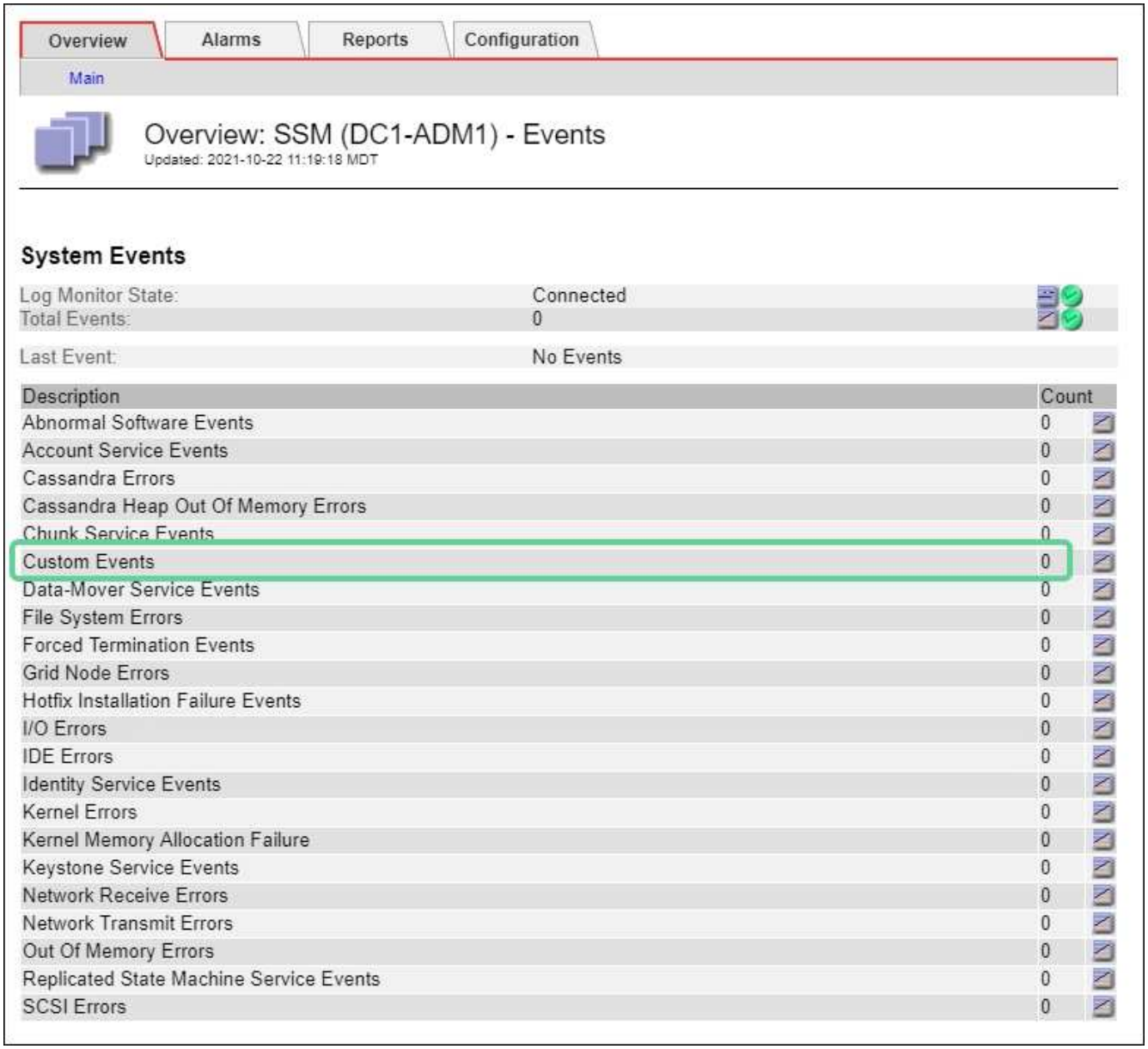
Hinweis: Nicht alle Einträge in der `/var/local/log/messages` Dateien werden abgeglichen, sofern sie nicht die oben genannten Anforderungen erfüllen.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (Legacy)** > **Benutzerdefinierte Ereignisse**.
2. Klicken Sie auf *Bearbeiten* (oder *Einfügen* wenn dies nicht das erste Ereignis ist).
3. Geben Sie eine benutzerdefinierte Ereigniszeichenfolge ein, beispielsweise „Herunterfahren“

4. Wählen Sie **Änderungen übernehmen**.
5. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
6. Wählen Sie ***grid node*** > **SSM** > **Events**.
7. Suchen Sie den Eintrag für benutzerdefinierte Ereignisse in der Ereignistabelle und überwachen Sie den Wert für **Anzahl**.

   Wenn die Anzahl steigt, wird auf diesem Grid-Knoten ein von Ihnen überwachtes benutzerdefiniertes Ereignis ausgelöst.



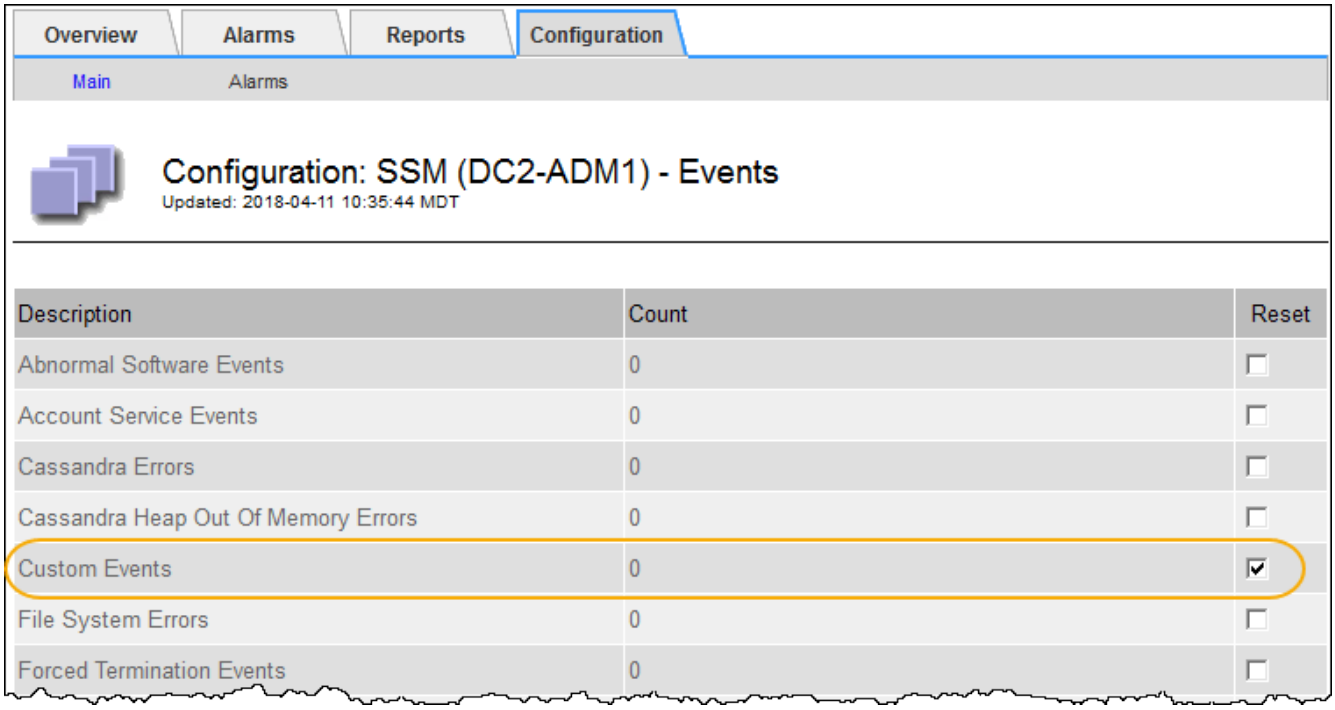
Setzt die Anzahl der benutzerdefinierten Ereignisse auf Null zurück

Wenn Sie den Zähler nur für benutzerdefinierte Ereignisse zurücksetzen möchten, müssen Sie die Seite „Grid-Topologie“ im Support-Menü verwenden.

Das Zurücksetzen eines Zählers führt dazu, dass der Alarm beim nächsten Ereignis ausgelöst wird. Wenn Sie dagegen einen Alarm bestätigen, wird dieser Alarm nur dann erneut ausgelöst, wenn der nächste Schwellenwert erreicht wird.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***grid node*** > **SSM** > **Events** > **Configuration** > **Main**.
3. Aktivieren Sie das Kontrollkästchen **Zurücksetzen** für benutzerdefinierte Ereignisse.



4. Wählen Sie **Änderungen übernehmen**.

Überprüfen von Auditmeldungen

Mithilfe von Audit-Meldungen können Sie die detaillierten Vorgänge Ihres StorageGRID Systems besser verstehen. Sie können Überwachungsprotokolle verwenden, um Probleme zu beheben und die Leistung zu bewerten.

Während des normalen Systembetriebs generieren alle StorageGRID -Dienste folgende Prüfmeldungen:

- Systemprüfungsmeldungen beziehen sich auf das Prüfsystem selbst, den Zustand der Grid-Knoten, die systemweite Aufgabenaktivität und die Sicherungsvorgänge der Dienste.
- Prüfmeldungen zum Objektspeicher beziehen sich auf die Speicherung und Verwaltung von Objekten innerhalb von StorageGRID, einschließlich der Speicherung und Abfrage von Objekten, Übertragungen von Grid-Knoten zu Grid-Knoten und Überprüfungen.
- Wenn eine S3-Clientanwendung eine Anforderung zum Erstellen, Ändern oder Abrufen eines Objekts stellt, werden Prüfmeldungen zum Lesen und Schreiben des Clients protokolliert.

- Management-Audit-Meldungen protokollieren Benutzeranfragen an die Management-API.

Jeder Admin-Knoten speichert Audit-Nachrichten in Textdateien. Die Audit-Freigabe enthält die aktive Datei (audit.log) sowie komprimierte Audit-Protokolle der vorherigen Tage. Jeder Knoten im Raster speichert außerdem eine Kopie der auf dem Knoten generierten Prüfinformationen.

Sie können direkt über die Befehlszeile des Admin-Knotens auf die Audit-Protokolldateien zugreifen.

StorageGRID kann standardmäßig Audit-Informationen senden, oder Sie können das Ziel ändern:

- StorageGRID verwendet standardmäßig lokale Knoten-Auditziele.
- Prüfprotokolleinträge von Grid Manager und Tenant Manager können an einen Speicherknoten gesendet werden.
- Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert.
- "Erfahren Sie mehr über die Konfiguration von Audit-Meldungen und Protokollzielen" .

Weitere Informationen zur Audit-Protokolldatei, zum Format der Audit-Meldungen, zu den Typen der Audit-Meldungen und zu den verfügbaren Tools zur Analyse der Audit-Meldungen finden Sie unter"Überprüfen der Überwachungsprotokolle" .

Erfassen von Protokolldateien und Systemdaten

Mit dem Grid Manager können Sie Protokolldateien und Systemdaten (einschließlich Konfigurationsdaten) für Ihr StorageGRID System abrufen.

Bevor Sie beginnen

- Sie müssen beim Grid Manager auf dem primären Admin-Knoten mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die Bereitstellungspassphrase verfügen.

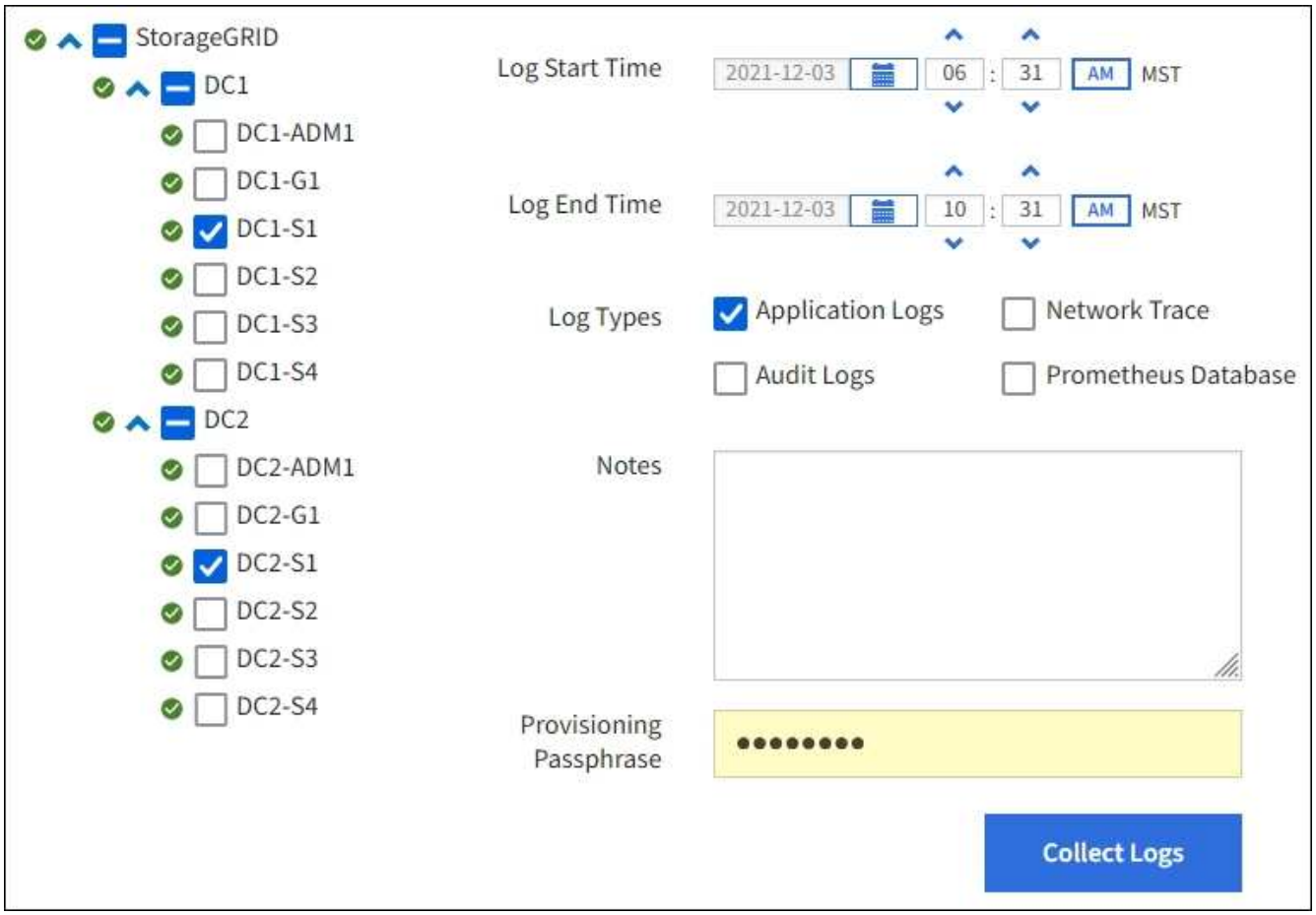
Informationen zu diesem Vorgang

Mit dem Grid Manager können Sie"Protokolldateien" , Systemdaten und Konfigurationsdaten von jedem Grid-Knoten für den von Ihnen ausgewählten Zeitraum. Daten werden gesammelt und in einer .tar.gz-Datei archiviert, die Sie dann auf Ihren lokalen Computer herunterladen können.

Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Protokolle**.



2. Wählen Sie die Grid-Knoten aus, für die Sie Protokolldateien sammeln möchten.

   Bei Bedarf können Sie Protokolldateien für das gesamte Grid oder einen gesamten Rechenzentrumsstandort sammeln.

3. Wählen Sie eine **Startzeit** und eine **Endzeit** aus, um den Zeitbereich der Daten festzulegen, die in die Protokolldateien aufgenommen werden sollen.

   Wenn Sie einen sehr langen Zeitraum auswählen oder Protokolle von allen Knoten in einem großen Raster sammeln, kann das Protokollarchiv zu groß werden, um auf einem Knoten gespeichert zu werden, oder zu groß, um zum Download auf dem primären Admin-Knoten gesammelt zu werden. In diesem Fall müssen Sie die Protokollerfassung mit einem kleineren Datensatz neu starten.

4. Wählen Sie die Protokolltypen aus, die Sie sammeln möchten.
   - **Anwendungsprotokolle**: Anwendungsspezifische Protokolle, die der technische Support am häufigsten zur Fehlerbehebung verwendet. Die gesammelten Protokolle sind eine Teilmenge der verfügbaren Anwendungsprotokolle.
   - **Audit-Protokolle**: Protokolle mit den während des normalen Systembetriebs generierten Audit-Meldungen.
   - **Netzwerkverfolgung**: Protokolle, die zum Debuggen des Netzwerks verwendet werden.
   - **Prometheus-Datenbank**: Zeitreihenmetriken von den Diensten auf allen Knoten.
5. Geben Sie optional Notizen zu den Protokolldateien ein, die Sie im Textfeld **Notizen** sammeln.

   Mithilfe dieser Hinweise können Sie dem technischen Support Informationen zu dem Problem geben, das Sie zum Sammeln der Protokolldateien veranlasst hat. Ihre Notizen werden einer Datei mit dem Namen

hinzugefügt `info.txt` , zusammen mit anderen Informationen zur Protokolldateisammlung. Der `info.txt` Die Datei wird im Protokolldatei-Archivpaket gespeichert.

6. Geben Sie die Bereitstellungspassphrase für Ihr StorageGRID -System in das Textfeld **Bereitstellungspassphrase** ein.
7. Wählen Sie **Protokolle sammeln**.

   Wenn Sie eine neue Anfrage senden, wird die vorherige Sammlung von Protokolldateien gelöscht.

   Auf der Seite „Protokolle“ können Sie den Fortschritt der Protokolldateierfassung für jeden Grid-Knoten überwachen.

   Wenn Sie eine Fehlermeldung bezüglich der Protokollgröße erhalten, versuchen Sie, Protokolle für einen kürzeren Zeitraum oder für weniger Knoten zu sammeln.

8. Wählen Sie **Herunterladen**, wenn die Protokolldateierfassung abgeschlossen ist.

   Die Datei *.tar.gz* enthält alle Protokolldateien von allen Grid-Knoten, bei denen die Protokollerfassung erfolgreich war. In der kombinierten *.tar.gz*-Datei befindet sich für jeden Grid-Knoten ein Protokolldateiarchiv.

Nach Abschluss

Sie können das Protokolldatei-Archivpaket bei Bedarf später erneut herunterladen.

Optional können Sie **Löschen** auswählen, um das Protokolldatei-Archivpaket zu entfernen und Speicherplatz freizugeben. Das aktuelle Protokolldatei-Archivpaket wird beim nächsten Sammeln von Protokolldateien automatisch entfernt.

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**.

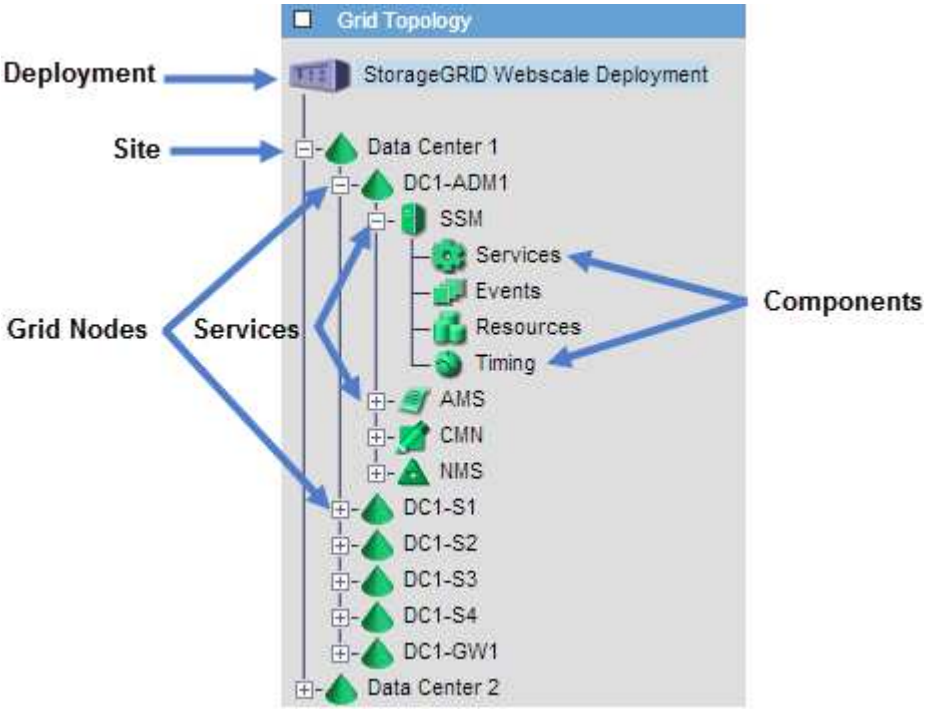
   StorageGRID versucht, ein AutoSupport Paket an die NetApp Support-Site zu senden. Wenn der Versuch erfolgreich ist, werden die Werte **Neuestes Ergebnis** und **Letzter erfolgreicher Zeitpunkt** auf der Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, wird der Wert **Neuestes Ergebnis** 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.

Den Netztopologie-Baum anzeigen

Der Grid-Topologie-Baum bietet Zugriff auf detaillierte Informationen zu StorageGRID -Systemelementen, einschließlich Sites, Grid-Knoten, Diensten und Komponenten. In den meisten Fällen müssen Sie nur auf den Grid-Topologie-Baum zugreifen, wenn Sie in der Dokumentation dazu aufgefordert werden oder wenn Sie mit dem technischen Support zusammenarbeiten.

Um auf den Gittertopologie-Baum zuzugreifen, wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.



Um den Gittertopologie-Baum zu erweitern oder zu reduzieren, klicken Sie auf ⊞ oder ⊟ auf Site-, Knoten- oder Serviceebene. Um alle Elemente der gesamten Site oder in jedem Knoten zu erweitern oder zu reduzieren, halten Sie die Taste **<Strg>** gedrückt und klicken Sie.

StorageGRID -Attribute

Attribute melden Werte und Status für viele Funktionen des StorageGRID Systems. Attributwerte sind für jeden Rasterknoten, jeden Standort und das gesamte Raster verfügbar.

StorageGRID -Attribute werden an mehreren Stellen im Grid Manager verwendet:

- **Knotenseite**: Viele der auf der Knotenseite angezeigten Werte sind StorageGRID -Attribute. (Prometheus-Metriken werden auch auf den Knotenseiten angezeigt.)
- **Gittertopologiebaum**: Attributwerte werden im Gittertopologiebaum angezeigt (**SUPPORT** > **Tools** > **Gittertopologie**).
- **Ereignisse**: Systemereignisse treten auf, wenn bestimmte Attribute einen Fehler oder Störungszustand für einen Knoten aufzeichnen, einschließlich Fehlern wie Netzwerkfehlern.

Attributwerte

Die Attribute werden nach bestem Wissen und Gewissen gemeldet und sind annähernd richtig. Attributaktualisierungen können unter bestimmten Umständen verloren gehen, beispielsweise beim Absturz

eines Dienstes oder beim Ausfall und Wiederaufbau eines Grid-Knotens.

Darüber hinaus können Ausbreitungsverzögerungen die Meldung von Attributen verlangsamen. Aktualisierte Werte für die meisten Attribute werden in festen Intervallen an das StorageGRID System gesendet. Es kann mehrere Minuten dauern, bis eine Aktualisierung im System sichtbar ist, und zwei Attribute, die sich mehr oder weniger gleichzeitig ändern, können zu leicht unterschiedlichen Zeitpunkten gemeldet werden.

Überprüfen der Supportmetriken

Bei der Fehlerbehebung können Sie mit dem technischen Support zusammenarbeiten, um detaillierte Messwerte und Diagramme für Ihr StorageGRID System zu überprüfen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

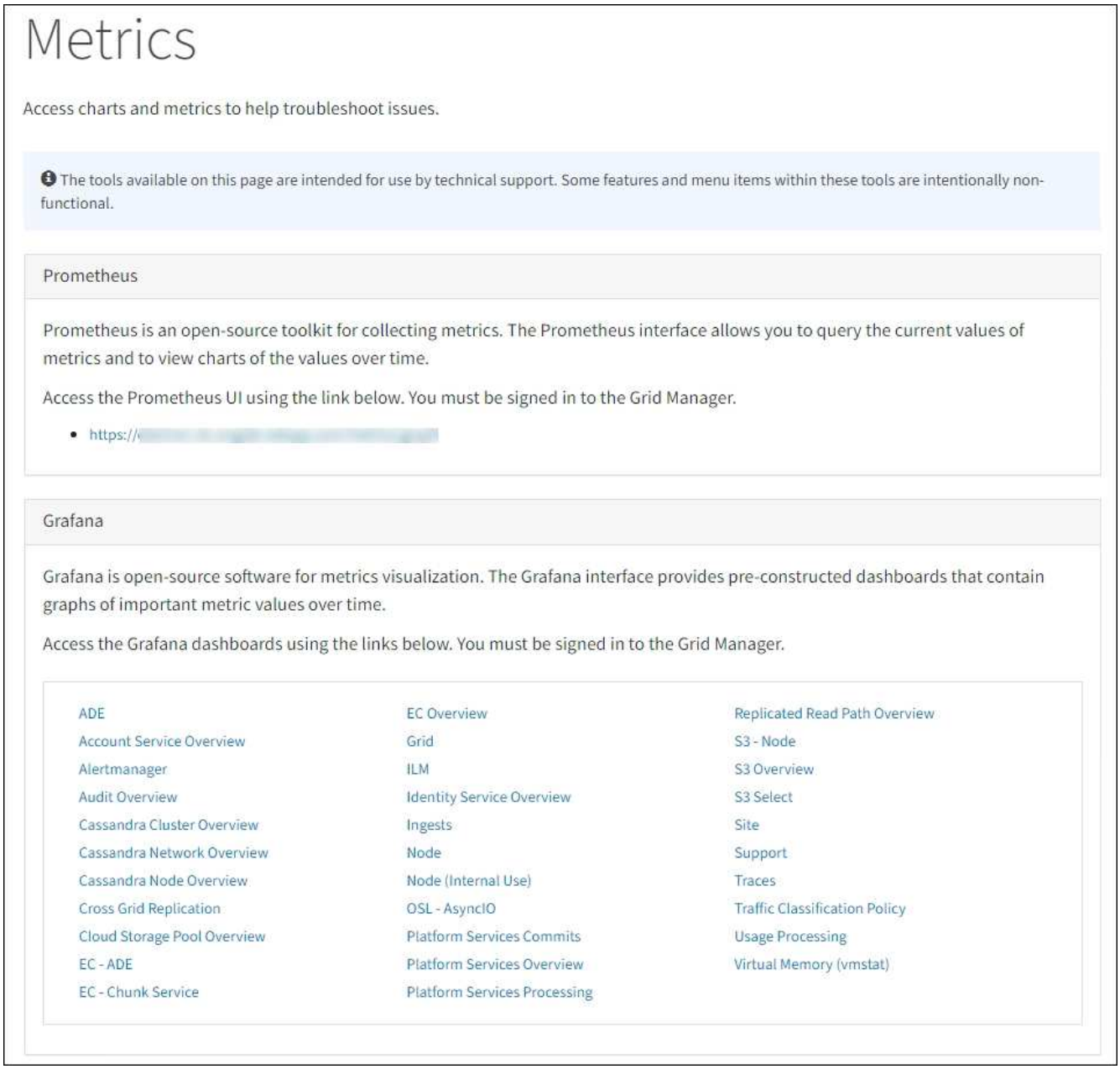
Über die Seite „Metriken“ können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist eine Open-Source-Software zum Sammeln von Metriken. Grafana ist eine Open-Source-Software zur Visualisierung von Metriken.

> ⓘ Die auf der Seite „Metriken“ verfügbaren Tools sind für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe die Liste der"häufig verwendete Prometheus-Metriken" .

Schritte

1. Wählen Sie gemäß den Anweisungen des technischen Supports **SUPPORT** > **Tools** > **Metriken**.

   Ein Beispiel für die Seite „Metriken“ wird hier angezeigt:



2. Um die aktuellen Werte der StorageGRID -Metriken abzufragen und Diagramme der Werte im Zeitverlauf anzuzeigen, klicken Sie auf den Link im Abschnitt „Prometheus“.

   Die Prometheus-Oberfläche wird angezeigt. Sie können diese Schnittstelle verwenden, um Abfragen zu den verfügbaren StorageGRID -Metriken auszuführen und StorageGRID -Metriken im Zeitverlauf grafisch darzustellen.

   > Metriken, deren Namen „*private*“ enthalten, sind nur für den internen Gebrauch bestimmt und können zwischen StorageGRID Versionen ohne Vorankündigung geändert werden.

3. Um auf vorgefertigte Dashboards mit Diagrammen der StorageGRID -Metriken im Zeitverlauf zuzugreifen, klicken Sie auf die Links im Abschnitt „Grafana“.

   Die Grafana-Schnittstelle für den von Ihnen ausgewählten Link wird angezeigt.

Diagnose ausführen

Bei der Fehlerbehebung können Sie mit dem technischen Support zusammenarbeiten, um eine Diagnose Ihres StorageGRID -Systems durchzuführen und die Ergebnisse zu überprüfen.

- "Überprüfen der Supportmetriken"
- "Häufig verwendete Prometheus-Metriken"

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Auf der Seite „Diagnose“ wird eine Reihe von Diagnoseprüfungen zum aktuellen Status des Rasters durchgeführt. Jede Diagnoseprüfung kann einen von drei Status haben:

- **Normal**: Alle Werte liegen im Normalbereich.
- **Achtung**: Einer oder mehrere Werte liegen außerhalb des Normalbereichs.
- **Achtung**: Einer oder mehrere Werte liegen deutlich außerhalb des Normalbereichs.

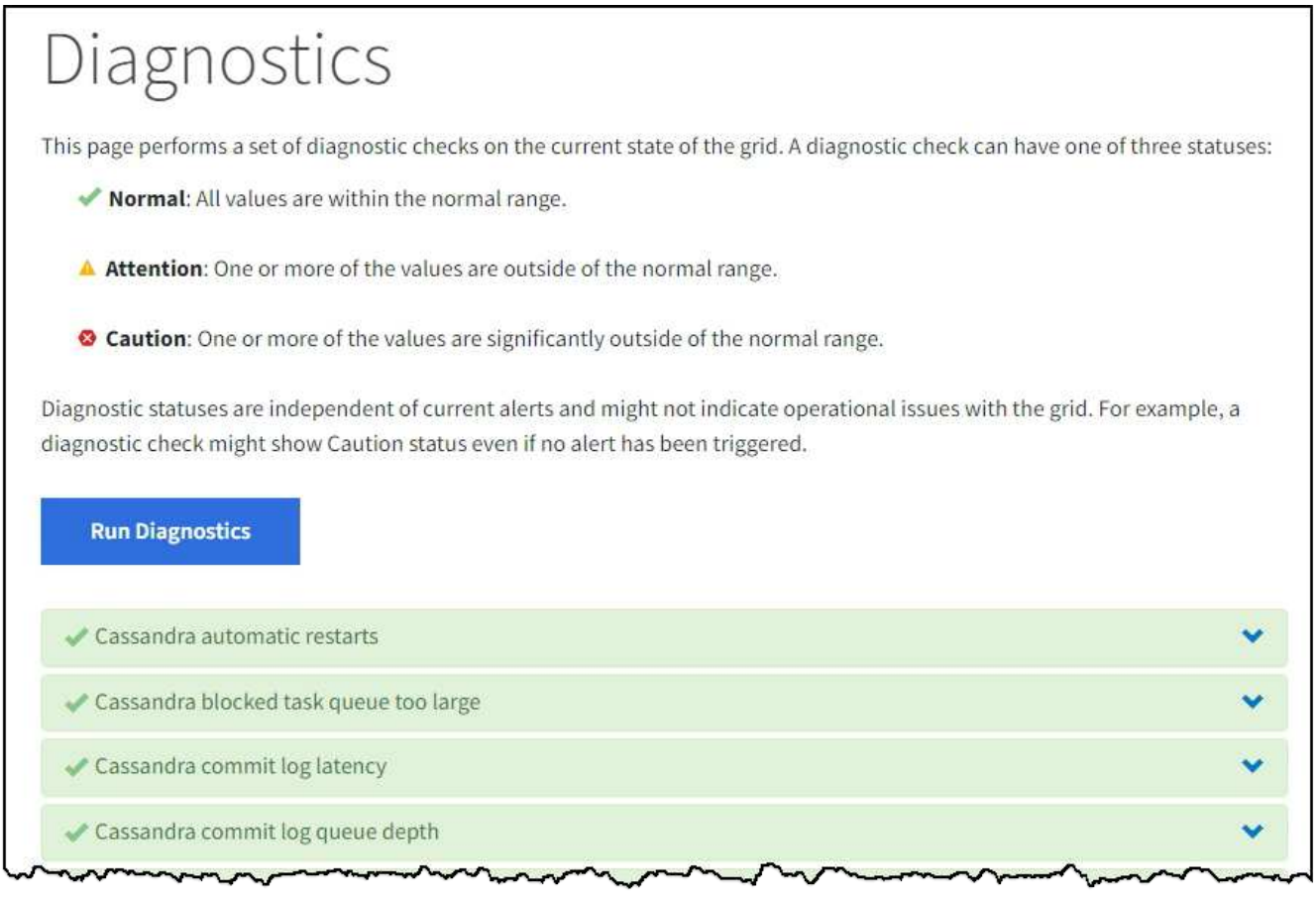
Diagnosestatus sind unabhängig von aktuellen Warnungen und weisen möglicherweise nicht auf Betriebsprobleme mit dem Netz hin. Beispielsweise kann eine Diagnoseprüfung den Status „Vorsicht“ anzeigen, auch wenn kein Alarm ausgelöst wurde.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Diagnose**.

   Die Seite „Diagnose“ wird angezeigt und listet die Ergebnisse für jede Diagnoseprüfung auf. Die Ergebnisse werden nach Schweregrad sortiert (Vorsicht, Achtung und dann Normal). Innerhalb jedes Schweregrads werden die Ergebnisse alphabetisch sortiert.

   In diesem Beispiel haben alle Diagnosen den Status „Normal“.



2. Um mehr über eine bestimmte Diagnose zu erfahren, klicken Sie irgendwo in die Zeile.

   Es werden Details zur Diagnose und ihren aktuellen Ergebnissen angezeigt. Die folgenden Details sind aufgeführt:

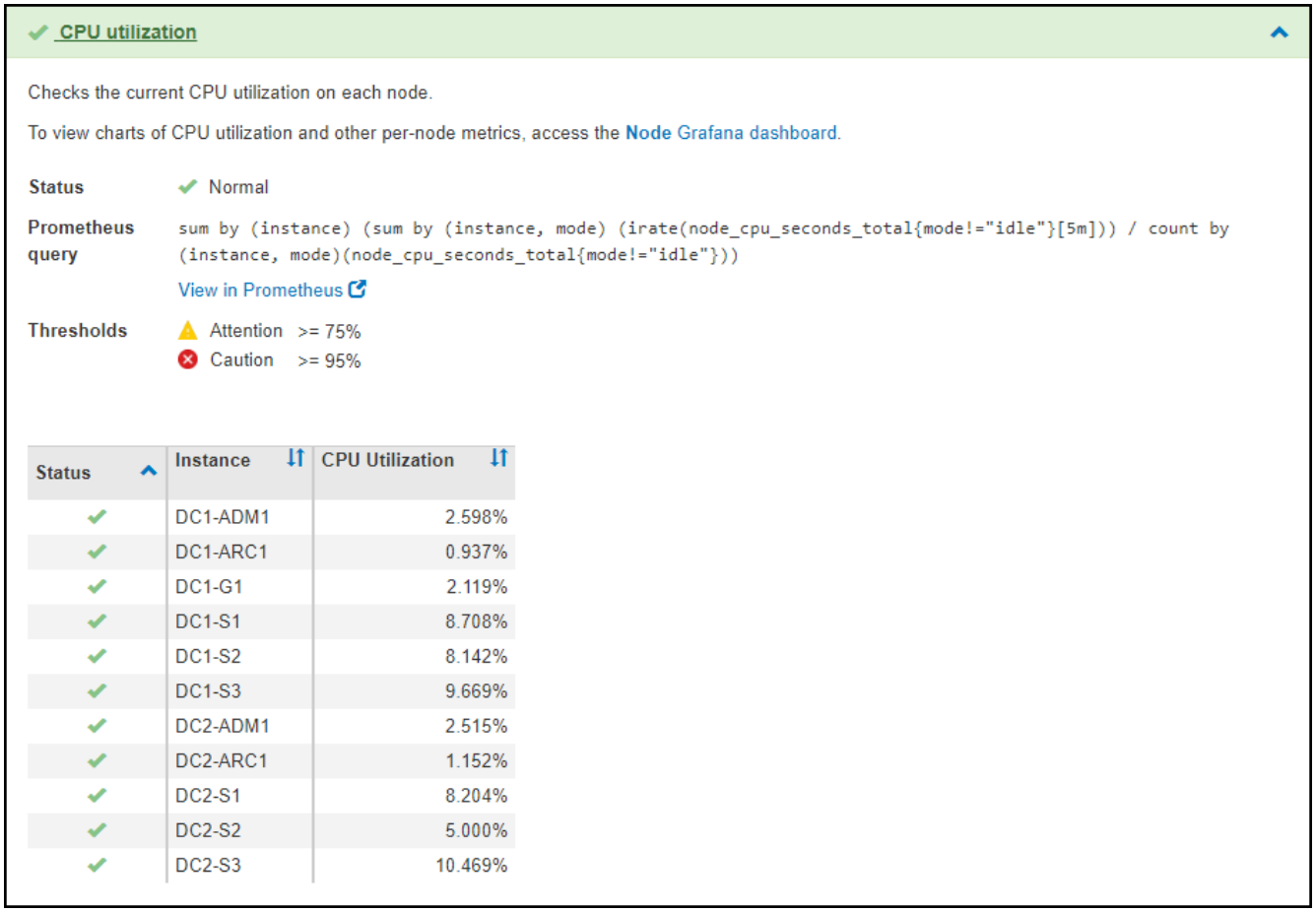
   - **Status**: Der aktuelle Status dieser Diagnose: Normal, Achtung oder Vorsicht.
   - **Prometheus-Abfrage**: Falls für die Diagnose verwendet, der Prometheus-Ausdruck, der zum

Generieren der Statuswerte verwendet wurde. (Nicht für alle Diagnosen wird ein Prometheus-Ausdruck verwendet.)

- **Schwellenwerte**: Sofern für die Diagnose verfügbar, die systemdefinierten Schwellenwerte für jeden abnormalen Diagnosestatus. (Schwellenwerte werden nicht für alle Diagnosen verwendet.)

  Sie können diese Schwellenwerte nicht ändern.

- **Statuswerte**: Eine Tabelle, die den Status und den Wert der Diagnose im gesamten StorageGRID -System anzeigt. In diesem Beispiel wird die aktuelle CPU-Auslastung für jeden Knoten in einem StorageGRID -System angezeigt. Alle Knotenwerte liegen unter den Schwellenwerten „Achtung“ und „Vorsicht“, sodass der Gesamtstatus der Diagnose „Normal“ ist.



3. **Optional**: Um Grafana-Diagramme im Zusammenhang mit dieser Diagnose anzuzeigen, klicken Sie auf den Link **Grafana-Dashboard**.

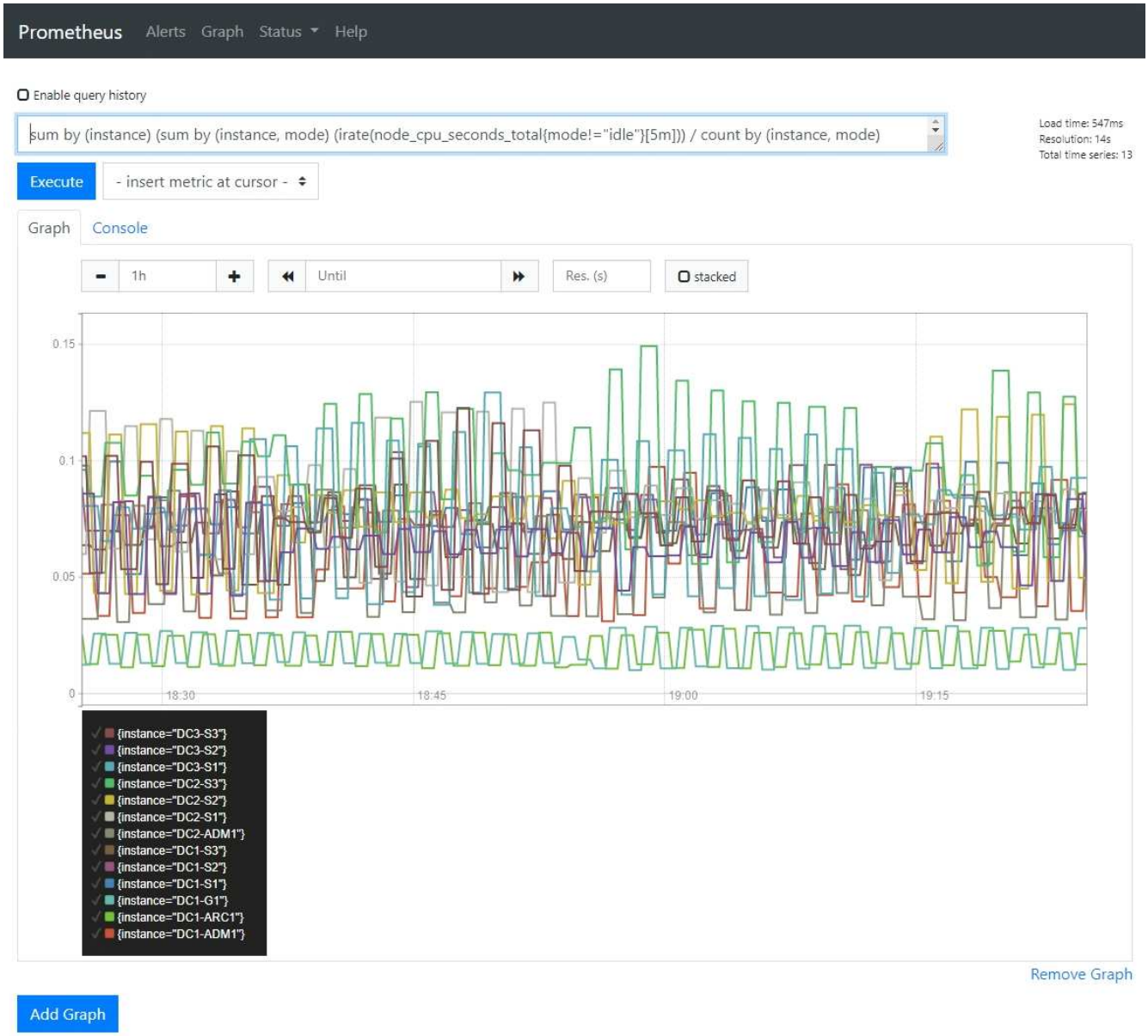
   Dieser Link wird nicht für alle Diagnosen angezeigt.

   Das zugehörige Grafana-Dashboard wird angezeigt. In diesem Beispiel wird das Knoten-Dashboard angezeigt, das die CPU-Auslastung im Zeitverlauf für diesen Knoten sowie andere Grafana-Diagramme für den Knoten anzeigt.

   Sie können auch über den Abschnitt „Grafana“ auf der Seite **SUPPORT** > **Tools** > **Metriken** auf die vorgefertigten Grafana-Dashboards zugreifen.

4. **Optional**: Um ein Diagramm des Prometheus-Ausdrucks im Zeitverlauf anzuzeigen, klicken Sie auf **In Prometheus anzeigen**.

   Es wird ein Prometheus-Diagramm des in der Diagnose verwendeten Ausdrucks angezeigt.



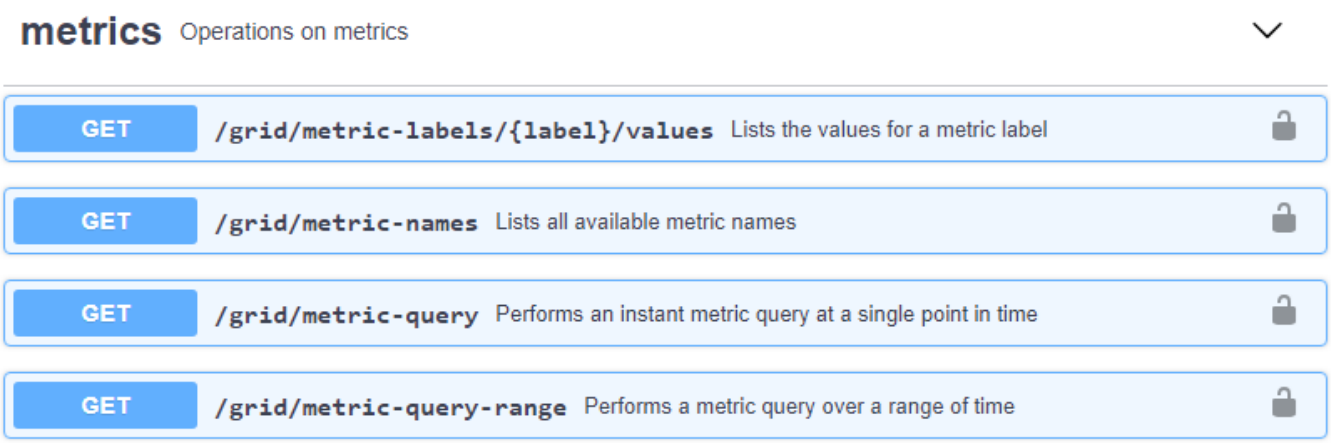
Erstellen Sie benutzerdefinierte Überwachungsanwendungen

Sie können benutzerdefinierte Überwachungsanwendungen und Dashboards mithilfe der StorageGRID -Metriken erstellen, die über die Grid Management API verfügbar sind.

Wenn Sie Metriken überwachen möchten, die nicht auf einer vorhandenen Seite des Grid Managers angezeigt werden, oder wenn Sie benutzerdefinierte Dashboards für StorageGRID erstellen möchten, können Sie die Grid Management-API verwenden, um StorageGRID -Metriken abzufragen.

Sie können auch mit einem externen Überwachungstool wie Grafana direkt auf Prometheus-Metriken zugreifen. Wenn Sie ein externes Tool verwenden, müssen Sie ein administratives Client-Zertifikat hochladen oder generieren, damit StorageGRID das Tool aus Sicherheitsgründen authentifizieren kann. Siehe die"Anweisungen zur Administration von StorageGRID" .

Um die Metrik-API-Operationen anzuzeigen, einschließlich der vollständigen Liste der verfügbaren Metriken, gehen Sie zum Grid Manager. Wählen Sie oben auf der Seite das Hilfesymbol und dann **API-Dokumentation** > **Metriken**
aus.



Die Einzelheiten zur Implementierung einer benutzerdefinierten Überwachungsanwendung gehen über den Rahmen dieser Dokumentation hinaus.

Fehlerbehebung beim StorageGRID -System

Fehlerbehebung bei einem StorageGRID -System

Wenn bei der Verwendung eines StorageGRID -Systems ein Problem auftritt, finden Sie in den Tipps und Richtlinien in diesem Abschnitt Hilfe bei der Ermittlung und Lösung des Problems.

Oft können Sie Probleme selbst lösen. Bei manchen Problemen müssen Sie sich jedoch möglicherweise an den technischen Support wenden.

Definieren Sie das Problem

Der erste Schritt zur Lösung eines Problems besteht darin, das Problem klar zu definieren.

Diese Tabelle enthält Beispiele für die Arten von Informationen, die Sie zur Definition eines Problems sammeln können:

Frage	Beispielantwort
Was macht das StorageGRID -System bzw. was macht es nicht? Was sind die Symptome?	Clientanwendungen melden, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann begann das Problem?	Die Objektaufnahme wurde am 8. Januar 2020 gegen 14:50 Uhr erstmals verweigert.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Benachrichtigung durch Clientanwendung. Habe auch E-Mail-Benachrichtigungen erhalten.
Tritt das Problem ständig auf oder nur manchmal?	Das Problem besteht weiterhin.

Frage	Beispielantwort
Wenn das Problem regelmäßig auftritt, welche Schritte führen dazu, dass es auftritt?	Das Problem tritt jedes Mal auf, wenn ein Client versucht, ein Objekt aufzunehmen.
Wenn das Problem zeitweise auftritt, wann tritt es auf? Notieren Sie die Zeitpunkte aller Vorfälle, die Ihnen bekannt sind.	Das Problem tritt nicht zeitweise auf.
Ist Ihnen dieses Problem schon einmal begegnet? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dieses Problem ist mir zum ersten Mal begegnet.

Bewerten Sie das Risiko und die Auswirkungen auf das System

Nachdem Sie das Problem definiert haben, bewerten Sie dessen Risiko und Auswirkungen auf das StorageGRID -System. Beispielsweise bedeutet das Vorhandensein kritischer Warnungen nicht unbedingt, dass das System keine Kerndienste bereitstellt.

Diese Tabelle fasst die Auswirkungen des Beispielproblems auf den Systembetrieb zusammen:

Frage	Beispielantwort
Kann das StorageGRID -System Inhalte aufnehmen?	NEIN.
Können Clientanwendungen Inhalte abrufen?	Einige Objekte können abgerufen werden, andere nicht.
Sind Daten gefährdet?	NEIN.
Ist die Geschäftsfähigkeit stark beeinträchtigt?	Ja, da Clientanwendungen keine Objekte im StorageGRID -System speichern können und Daten nicht konsistent abgerufen werden können.

Daten sammeln

Nachdem Sie das Problem definiert und sein Risiko und seine Auswirkungen bewertet haben, sammeln Sie Daten für die Analyse. Welche Art von Daten am sinnvollsten zu erfassen ist, hängt von der Art des Problems ab.

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Erstellen Sie eine Zeitleiste der letzten Änderungen	Änderungen an Ihrem StorageGRID -System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	• Erstellen Sie eine Zeitleiste der letzten Änderungen

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Benachrichtigungen überprüfen	Mithilfe von Warnmeldungen können Sie die Grundursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme liefern, die das Problem möglicherweise verursachen. Überprüfen Sie die Liste der aktuellen Warnungen, um festzustellen, ob StorageGRID die Grundursache eines Problems für Sie identifiziert hat. Überprüfen Sie in der Vergangenheit ausgelöste Warnungen, um zusätzliche Erkenntnisse zu erhalten.	• "Aktuelle und gelöste Warnmeldungen anzeigen"
Überwachen von Ereignissen	Zu den Ereignissen zählen alle Systemfehler oder Störungsereignisse für einen Knoten, einschließlich Fehlern wie Netzwerkfehlern. Überwachen Sie Ereignisse, um mehr über Probleme zu erfahren oder bei der Fehlerbehebung zu helfen.	• "Überwachen von Ereignissen"
Identifizieren Sie Trends mithilfe von Diagrammen und Textberichten	Trends können wertvolle Hinweise darauf liefern, wann Probleme erstmals auftraten, und Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	• "Verwenden Sie Diagramme und Grafiken" • "Verwenden Sie Textberichte"
Festlegen von Basislinien	Sammeln Sie Informationen über die Normalwerte verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Basiswerten können wertvolle Hinweise liefern.	• Festlegen von Basislinien
Durchführen von Aufnahme- und Abruftests	Um Leistungsprobleme beim Aufnehmen und Abrufen zu beheben, verwenden Sie eine Workstation zum Speichern und Abrufen von Objekten. Vergleichen Sie die Ergebnisse mit denen, die Sie bei Verwendung der Clientanwendung sehen.	• "Überwachen Sie die PUT- und GET-Leistung"
Überprüfen von Auditmeldungen	Überprüfen Sie die Prüfmeldungen, um die StorageGRID -Vorgänge im Detail zu verfolgen. Die Details in den Prüfmeldungen können bei der Behebung vieler Arten von Problemen hilfreich sein, darunter auch Leistungsprobleme.	• "Überprüfen von Auditmeldungen"

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Überprüfen Sie die Objektstandorte und Speicherintegrität	Wenn Sie Speicherprobleme haben, überprüfen Sie, ob die Objekte dort platziert werden, wo Sie es erwarten. Überprüfen Sie die Integrität der Objektdaten auf einem Speicherknoten.	• "Überwachen von Objektüberprüfungsvorgängen" • "Bestätigen Sie die Speicherorte der Objektdaten" • "Überprüfen der Objektintegrität"
Sammeln Sie Daten für den technischen Support	Der technische Support bittet Sie möglicherweise, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um bei der Behebung von Problemen zu helfen.	• "Erfassen von Protokolldateien und Systemdaten" • "Manuelles Auslösen eines AutoSupport -Pakets" • "Überprüfen der Supportmetriken"

Erstellen Sie eine Zeitleiste der letzten Änderungen

Wenn ein Problem auftritt, sollten Sie berücksichtigen, was sich kürzlich geändert hat und wann diese Änderungen aufgetreten sind.

- Änderungen an Ihrem StorageGRID -System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.
- Mithilfe einer Zeitleiste der Änderungen können Sie ermitteln, welche Änderungen möglicherweise für ein Problem verantwortlich sind und wie sich jede Änderung möglicherweise auf dessen Entwicklung ausgewirkt hat.

Erstellen Sie eine Tabelle mit den letzten Änderungen an Ihrem System, die Informationen darüber enthält, wann die einzelnen Änderungen vorgenommen wurden, sowie alle relevanten Details zu den Änderungen, z. B. Informationen darüber, was sonst noch während der Änderung geschah:

Zeit der Veränderung	Art der Änderung	Details
Beispiel: • Wann haben Sie mit der Knotenwiederherstellung begonnen? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Vorgang unterbrochen?	Was ist passiert? Was hast du gemacht?	Dokumentieren Sie alle relevanten Details zur Änderung. Beispiel: • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Wie sich die Arbeitslast der Clients verändert hat. Achten Sie darauf, ob mehrere Änderungen gleichzeitig vorgenommen wurden. Wurde diese Änderung beispielsweise während eines laufenden Upgrades vorgenommen?

Beispiele für bedeutende aktuelle Änderungen

Hier sind einige Beispiele für potenziell bedeutende Änderungen:

- Wurde das StorageGRID -System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde das System kürzlich aktualisiert? Wurde ein Hotfix angewendet?
- Wurde kürzlich Hardware repariert oder ausgetauscht?
- Wurde die ILM-Richtlinie aktualisiert?
- Hat sich die Arbeitsbelastung des Kunden geändert?
- Hat sich die Clientanwendung oder ihr Verhalten geändert?
- Haben Sie Load Balancer geändert oder eine Hochverfügbarkeitsgruppe von Admin-Knoten oder Gateway-Knoten hinzugefügt oder entfernt?
- Wurden Aufgaben begonnen, deren Erledigung möglicherweise viel Zeit in Anspruch nimmt? Beispiele hierfür sind:
  - Wiederherstellung eines ausgefallenen Speicherknotens
  - Außerbetriebnahme von Speicherknoten
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, z. B. das Hinzufügen eines Mandanten oder das Ändern der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden Plattformdienste kürzlich aktiviert oder geändert?
- Wurde die Compliance vor Kurzem aktiviert?
- Wurden Cloud-Speicherpools hinzugefügt oder entfernt?
- Wurden Änderungen an der Speicherkomprimierung oder -verschlüsselung vorgenommen?
- Gab es Änderungen an der Netzwerkinfrastruktur? Zum Beispiel VLANs, Router oder DNS.
- Wurden Änderungen an NTP-Quellen vorgenommen?
- Wurden Änderungen an den Grid-, Admin- oder Client-Netzwerkschnittstellen vorgenommen?
- Wurden sonstige Änderungen am StorageGRID -System oder seiner Umgebung vorgenommen?

Festlegen von Basislinien

Sie können Basiswerte für Ihr System festlegen, indem Sie die Normalwerte verschiedener Betriebswerte aufzeichnen. In Zukunft können Sie aktuelle Werte mit diesen Basiswerten vergleichen, um abnormale Werte zu erkennen und zu beheben.

Eigentum	Wert	So erhalten Sie
Durchschnittlicher Speicherverbrauch	Verbrauchte GB/Tag Prozent verbraucht/Tag	Gehen Sie zum Grid Manager. Wählen Sie auf der Seite „Knoten“ das gesamte Raster oder eine Site aus und wechseln Sie zur Registerkarte „Speicher“. Suchen Sie im Diagramm „Speichernutzung – Objektdaten“ einen Zeitraum, in dem die Linie relativ stabil ist. Bewegen Sie den Cursor über das Diagramm, um zu schätzen, wie viel Speicherplatz täglich verbraucht wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Durchschnittlicher Metadatenverbrauch	Verbrauchte GB/Tag Prozent verbraucht/Tag	Gehen Sie zum Grid Manager. Wählen Sie auf der Seite „Knoten“ das gesamte Raster oder eine Site aus und wechseln Sie zur Registerkarte „Speicher“. Suchen Sie im Diagramm „Speicherplatznutzung – Objektmetadaten“ einen Zeitraum, in dem die Linie relativ stabil ist. Bewegen Sie den Cursor über das Diagramm, um zu schätzen, wie viel Metadatenspeicher täglich verbraucht wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Rate der S3/Swift-Operationen	Operationen/Sekunde	Wählen Sie im Grid Manager-Dashboard **Leistung** > **S3-Operationen** oder **Leistung** > **Swift-Operationen**. Um die Aufnahme- und Abrufraten sowie die Anzahl für eine bestimmte Site oder einen bestimmten Knoten anzuzeigen, wählen Sie **KNOTEN** > ***Site oder Speicherknoten*** > **Objekte**. Positionieren Sie Ihren Cursor über dem Ingest- und Retrieve-Diagramm für S3.
Fehlgeschlagene S3/Swift-Operationen	Operationen	Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**. Zeigen Sie auf der Registerkarte „Übersicht“ im Abschnitt „API-Operationen“ den Wert für „S3-Operationen – Fehlgeschlagen“ oder „Swift-Operationen – Fehlgeschlagen“ an.

Eigentum	Wert	So erhalten Sie
ILM-Auswertungsrate	Objekte/Sekunde	Wählen Sie auf der Seite „Knoten“ ***grid*** > **ILM** aus. Suchen Sie im ILM-Warteschlangendiagramm einen Zeitraum, in dem die Leitung relativ stabil ist. Positionieren Sie Ihren Cursor über dem Diagramm, um einen Basiswert für die **Bewertungsrate** für Ihr System zu schätzen.
ILM-Scanrate	Objekte/Sekunde	Wählen Sie **NODES** > ***grid*** > **ILM**. Suchen Sie im ILM-Warteschlangendiagramm einen Zeitraum, in dem die Leitung relativ stabil ist. Positionieren Sie Ihren Cursor über dem Diagramm, um einen Basiswert für die **Scanrate** für Ihr System zu schätzen.
Objekte aus Clientvorgängen in der Warteschlange	Objekte/Sekunde	Wählen Sie **NODES** > ***grid*** > **ILM**. Suchen Sie im ILM-Warteschlangendiagramm einen Zeitraum, in dem die Leitung relativ stabil ist. Positionieren Sie Ihren Cursor über dem Diagramm, um einen Basiswert für **in die Warteschlange gestellte Objekte (aus Clientvorgängen)** für Ihr System zu schätzen.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie **NODES** > ***Storage Node*** > **Objects**. Zeigen Sie in der Abfragetabelle den Wert für die durchschnittliche Latenz an.

Daten analysieren

Verwenden Sie die gesammelten Informationen, um die Ursache des Problems und mögliche Lösungen zu ermitteln.

Die Analyse ist problemabhängig, aber im Allgemeinen gilt:

- Lokalisieren Sie mithilfe der Warnungen Fehlerpunkte und Engpässe.
- Rekonstruieren Sie den Problemverlauf mithilfe des Warnverlaufs und der Diagramme.
- Verwenden Sie Diagramme, um Anomalien zu finden und die Problemsituation mit dem Normalbetrieb zu vergleichen.

Checkliste für Eskalationsinformationen

Wenn Sie das Problem nicht selbst lösen können, wenden Sie sich an den technischen Support. Bevor Sie sich an den technischen Support wenden, sammeln Sie die in der folgenden Tabelle aufgeführten Informationen, um die Problemlösung zu erleichtern.

✔	Artikel	Hinweise
	Problemstellung	Was sind die Problemsymptome? Wann begann das Problem? Passiert das ständig oder zeitweise? Wenn es zeitweise auftritt, wann ist es aufgetreten? Definieren Sie das Problem
	Folgenabschätzung	Wie schwerwiegend ist das Problem? Welche Auswirkungen hat dies auf die Clientanwendung? • Hat der Client zuvor eine erfolgreiche Verbindung hergestellt? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID -System-ID	Wählen Sie **WARTUNG** > **System** > **Lizenz**. Die StorageGRID -System-ID wird als Teil der aktuellen Lizenz angezeigt.
	Softwareversion	Wählen Sie oben im Grid Manager das Hilfesymbol und dann **Info** aus, um die StorageGRID -Version anzuzeigen.
	Anpassung	Fassen Sie zusammen, wie Ihr StorageGRID -System konfiguriert ist. Listen Sie beispielsweise Folgendes auf: • Verwendet das Grid Speicherkomprimierung, Speicherverschlüsselung oder Compliance? • Erstellt ILM replizierte oder löschcodierte Objekte? Stellt ILM die Standortredundanz sicher? Verwenden ILM-Regeln die Aufnahmeverhalten „Balanced“, „Strict“ oder „Dual Commit“?
	Protokolldateien und Systemdaten	Sammeln Sie Protokolldateien und Systemdaten für Ihr System. Wählen Sie **SUPPORT** > **Tools** > **Protokolle**. Sie können Protokolle für das gesamte Raster oder für ausgewählte Knoten sammeln. Wenn Sie Protokolle nur für ausgewählte Knoten sammeln, achten Sie darauf, mindestens einen Speicherknoten einzuschließen, der über den ADC-Dienst verfügt. (Die ersten drei Speicherknoten an einem Standort umfassen den ADC-Dienst.) "Erfassen von Protokolldateien und Systemdaten"
	Basisinformationen	Sammeln Sie Basisinformationen zu Aufnahmevorgängen, Abrufvorgängen und Speicherverbrauch. Festlegen von Basislinien

✔	Artikel	Hinweise
	Zeitleiste der jüngsten Änderungen	Erstellen Sie eine Zeitleiste, die alle aktuellen Änderungen am System oder seiner Umgebung zusammenfasst. Erstellen Sie eine Zeitleiste der letzten Änderungen
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie selbst Schritte zur Diagnose oder Fehlerbehebung des Problems unternommen haben, dokumentieren Sie die durchgeführten Schritte und das Ergebnis.

Beheben von Objekt- und Speicherproblemen

Bestätigen Sie die Speicherorte der Objektdaten

Je nach Problem möchten Sie vielleicht"Bestätigen Sie, wo die Objektdaten gespeichert werden" . Sie möchten beispielsweise überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und die Objektdaten am vorgesehenen Ort gespeichert werden.

Bevor Sie beginnen

- Sie müssen über eine Objektkennung verfügen. Dabei kann es sich um eine der folgenden handeln:
  - **UUID**: Die universell eindeutige Kennung des Objekts. Geben Sie die UUID in Großbuchstaben ein.
  - **CBID**: Die eindeutige Kennung des Objekts innerhalb von StorageGRID . Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in Großbuchstaben ein.
  - **S3-Bucket und Objektschlüssel**: Wenn ein Objekt über den"S3-Schnittstelle" verwendet die Clientanwendung eine Bucket- und Objektschlüsselkombination zum Speichern und Identifizieren des Objekts.

Schritte

1. Wählen Sie **ILM** > **Objektmetadatensuche**.
2. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

   Sie können eine UUID, CBID, einen S3-Bucket/Objektschlüssel oder einen Swift-Container/Objektnamen eingeben.

3. Wenn Sie eine bestimmte Version des Objekts suchen möchten, geben Sie die Versions-ID ein (optional).

4. Wählen Sie **Nachschlagen**.

   Der"Ergebnisse der Objektmetadatensuche" erscheinen. Auf dieser Seite sind die folgenden Arten von Informationen aufgeführt:

   - Systemmetadaten, einschließlich der Objekt-ID (UUID), der Versions-ID (optional), des Objektnamens, des Namens des Containers, 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 eine Liste von Objektsegmenten einschließlich Segmentkennungen und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
   - Alle Objektmetadaten im unverarbeiteten, internen Speicherformat. Diese Rohmetadaten umfassen interne Systemmetadaten, deren Beibehaltung von Version zu Version nicht garantiert ist.

     Das folgende Beispiel zeigt die Ergebnisse der Objektmetadatensuche für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Fehler im Objektspeicher (Speichervolumen)

Der zugrunde liegende Speicher auf einem Speicherknoten ist in Objektspeicher unterteilt. Objektspeicher werden auch als Speichervolumes bezeichnet.

Sie können Objektspeicherinformationen für jeden Speicherknoten anzeigen. Objektspeicher werden unten auf der Seite **NODES** > ***Storage Node*** > **Storage** angezeigt.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

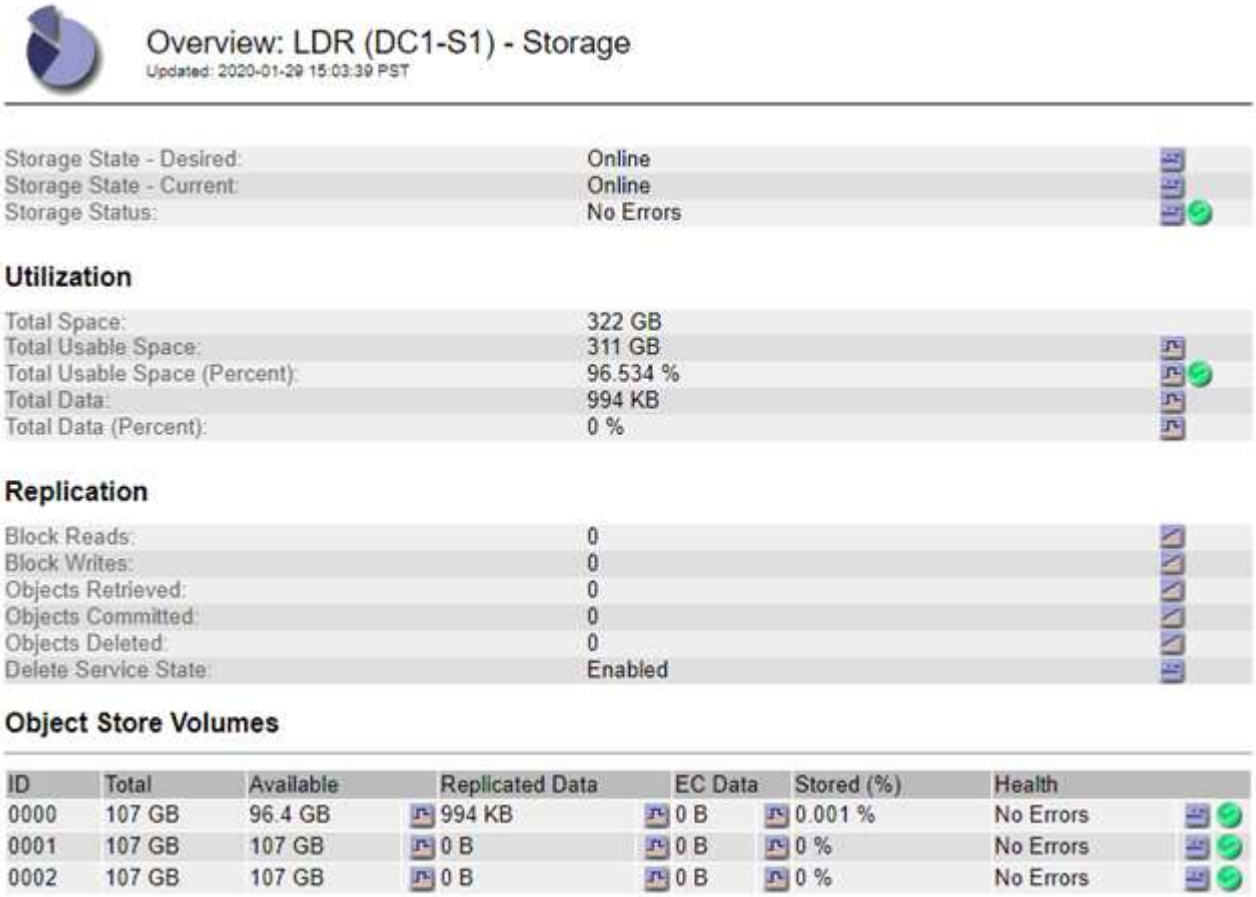
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Mehr sehen"Details zu jedem Speicherknoten" , führen Sie die folgenden Schritte aus:

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Overview** > **Main**.



Abhängig von der Art des Fehlers können sich Fehler bei einem Speichervolumen in"Speichervolumenwarnungen" . Wenn ein Speichervolume ausfällt, sollten Sie das ausgefallene Speichervolume reparieren, um die volle Funktionalität des Speicherknotens so schnell wie möglich wiederherzustellen. Bei Bedarf können Sie auf die Registerkarte **Konfiguration** gehen und"Versetzen Sie den Speicherknoten in einen schreibgeschützten Zustand" damit das StorageGRID -System es zum Datenabruf verwenden kann, während Sie eine vollständige Wiederherstellung des Servers vorbereiten.

Überprüfen der Objektintegrität

Das StorageGRID -System überprüft die Integrität der Objektdaten auf Speicherknoten und sucht nach beschädigten und fehlenden Objekten.

Es gibt zwei Überprüfungsprozesse: Hintergrundüberprüfung und Objektexistenzprüfung (früher Vordergrundüberprüfung genannt). Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung läuft automatisch und prüft kontinuierlich die Richtigkeit der Objektdaten. Die Objektexistenzprüfung kann von einem Benutzer ausgelöst werden, um die Existenz (jedoch nicht die Richtigkeit) von Objekten schneller zu überprüfen.

Was ist eine Hintergrundüberprüfung?

Der Hintergrundüberprüfungsprozess prüft Speicherknoten automatisch und kontinuierlich auf beschädigte

Kopien von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

Bei der Hintergrundüberprüfung wird die Integrität replizierter und löschcodierter Objekte wie folgt überprüft:

- **Replizierte Objekte**: Wenn der Hintergrundüberprüfungsprozess ein beschädigtes repliziertes Objekt findet, wird die beschädigte Kopie von ihrem Speicherort entfernt und an einer anderen Stelle auf dem Speicherknoten unter Quarantäne gestellt. Anschließend wird eine neue, unbeschädigte Kopie erstellt und platziert, um die aktiven ILM-Richtlinien zu erfüllen. Die neue Kopie wird möglicherweise nicht auf dem Speicherknoten abgelegt, der für die Originalkopie verwendet wurde.

  > Beschädigte Objektdaten werden unter Quarantäne gestellt und nicht aus dem System gelöscht, sodass weiterhin auf sie zugegriffen werden kann. Weitere Informationen zum Zugriff auf unter Quarantäne gestellte Objektdaten erhalten Sie beim technischen Support.

- **Erasure-Coded-Objekte**: Wenn der Hintergrundüberprüfungsprozess erkennt, dass ein Fragment eines Erasure-Coded-Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment an Ort und Stelle auf demselben Speicherknoten mithilfe der verbleibenden Daten- und Paritätsfragmente wiederherzustellen. Wenn das beschädigte Fragment nicht wiederhergestellt werden kann, wird versucht, eine weitere Kopie des Objekts abzurufen. Wenn der Abruf erfolgreich ist, wird eine ILM-Auswertung durchgeführt, um eine Ersatzkopie des löschcodierten Objekts zu erstellen.

  Der Hintergrundüberprüfungsprozess prüft nur Objekte auf Speicherknoten. Es werden keine Objekte in einem Cloud-Speicherpool überprüft. Objekte müssen älter als vier Tage sein, um für die Hintergrundüberprüfung in Frage zu kommen.

Die Hintergrundüberprüfung läuft kontinuierlich und ist so konzipiert, dass sie die normalen Systemaktivitäten nicht beeinträchtigt. Die Hintergrundüberprüfung kann nicht gestoppt werden. Sie können jedoch die Hintergrundüberprüfungsrate erhöhen, um den Inhalt eines Speicherknotens schneller zu überprüfen, wenn Sie ein Problem vermuten.

Warnungen im Zusammenhang mit der Hintergrundüberprüfung

Wenn das System ein beschädigtes Objekt erkennt, das es nicht automatisch korrigieren kann (weil die Beschädigung die Identifizierung des Objekts verhindert), wird die Warnung **Unbekanntes beschädigtes Objekt erkannt** ausgelöst.

Wenn die Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, weil keine andere Kopie gefunden werden kann, wird die Warnung „Objekte verloren“ ausgelöst.

Ändern Sie die Hintergrundüberprüfungsrate

Sie können die Rate ändern, mit der die Hintergrundüberprüfung replizierte Objektdaten auf einem Speicherknoten prüft, wenn Sie Bedenken hinsichtlich der Datenintegrität haben.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Sie können die Überprüfungsrate für die Hintergrundüberprüfung auf einem Speicherknoten ändern:

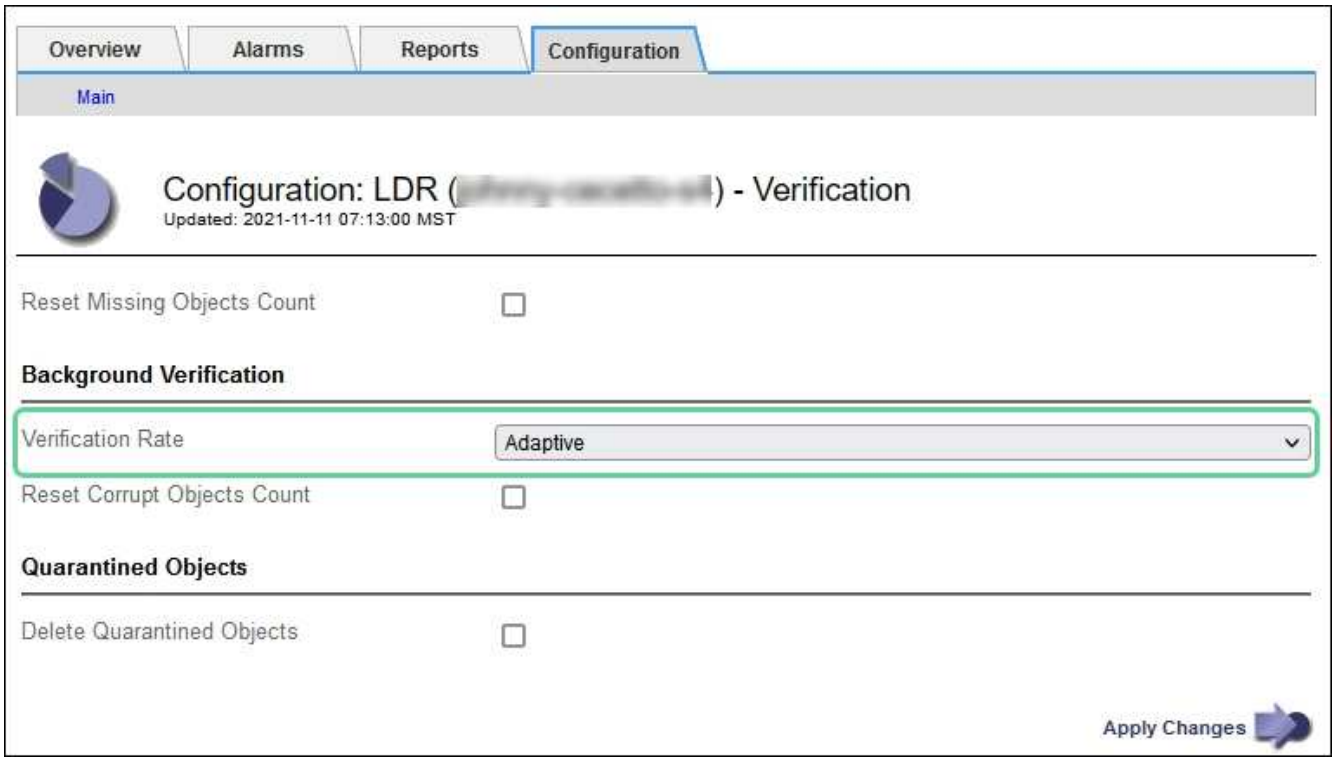
- Adaptiv: Standardeinstellung. Die Aufgabe ist für eine Überprüfung mit maximal 4 MB/s oder 10 Objekten/s ausgelegt (je nachdem, was zuerst überschritten wird).

- Hoch: Die Speicherüberprüfung erfolgt schnell, mit einer Geschwindigkeit, die normale Systemaktivitäten verlangsamen kann.

Verwenden Sie die hohe Überprüfungsrate nur, wenn Sie vermuten, dass ein Hardware- oder Softwarefehler die Objektdaten beschädigt haben könnte. Nachdem die Hintergrundüberprüfung mit hoher Priorität abgeschlossen ist, wird die Überprüfungsrate automatisch auf „Adaptiv“ zurückgesetzt.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***Speicherknoten*** > **LDR** > **Verifizierung**.
3. Wählen Sie **Konfiguration** > **Haupt**.
4. Gehen Sie zu **LDR** > **Verifizierung** > **Konfiguration** > **Haupt**.
5. Wählen Sie unter „Hintergrundüberprüfung“ **Überprüfungsrate** > **Hoch** oder **Überprüfungsrate** > **Adaptiv**.



6. Klicken Sie auf **Änderungen übernehmen**.
7. Überwachen Sie die Ergebnisse der Hintergrundüberprüfung für replizierte Objekte.
   a. Gehen Sie zu **NODES** > ***Storage Node*** > **Objects**.
   b. Überwachen Sie im Abschnitt „Überprüfung“ die Werte für **Beschädigte Objekte** und **Unidentifizierte beschädigte Objekte**.

      Wenn bei der Hintergrundüberprüfung beschädigte replizierte Objektdaten gefunden werden, wird die Metrik **Beschädigte Objekte** erhöht und StorageGRID versucht, die Objektkennung wie folgt aus den Daten zu extrahieren:

      - Wenn die Objektkennung extrahiert werden kann, erstellt StorageGRID automatisch eine neue Kopie der Objektdaten. Die neue Kopie kann überall im StorageGRID -System erstellt werden, wo die aktiven ILM-Richtlinien erfüllt werden.

- Wenn die Objektkennung nicht extrahiert werden kann (weil sie beschädigt wurde), wird die Metrik **Beschädigte Objekte nicht identifiziert** erhöht und die Warnung **Unidentifiziertes beschädigtes Objekt erkannt** ausgelöst.

c. Wenn beschädigte replizierte Objektdaten gefunden werden, wenden Sie sich an den technischen Support, um die Grundursache der Beschädigung zu ermitteln.

8. Überwachen Sie die Ergebnisse der Hintergrundüberprüfung für Erasure-Codierte Objekte.

   Wenn bei der Hintergrundüberprüfung beschädigte Fragmente von Erasure-Coded-Objektdaten gefunden werden, wird das Attribut „Beschädigte Fragmente erkannt“ erhöht. StorageGRID stellt das Problem wieder her, indem das beschädigte Fragment an Ort und Stelle auf demselben Speicherknoten neu erstellt wird.

   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
   b. Wählen Sie ***Speicherknoten*** > **LDR** > **Erasure Coding**.
   c. Überwachen Sie in der Tabelle „Verifizierungsergebnisse“ das Attribut „Beschädigte Fragmente erkannt“ (ECCD).

9. Nachdem beschädigte Objekte automatisch vom StorageGRID System wiederhergestellt wurden, setzen Sie die Anzahl der beschädigten Objekte zurück.
   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
   b. Wählen Sie ***Speicherknoten*** > **LDR** > **Verifizierung** > **Konfiguration**.
   c. Wählen Sie **Anzahl beschädigter Objekte zurücksetzen**.
   d. Klicken Sie auf **Änderungen übernehmen**.

10. Wenn Sie sicher sind, dass die unter Quarantäne gestellten Objekte nicht benötigt werden, können Sie sie löschen.

    > Wenn die Warnung „Objekte verloren“ ausgelöst wurde, möchte der technische Support möglicherweise auf unter Quarantäne gestellte Objekte zugreifen, um das zugrunde liegende Problem zu beheben oder eine Datenwiederherstellung zu versuchen.

    a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
    b. Wählen Sie ***Speicherknoten*** > **LDR** > **Verifizierung** > **Konfiguration**.
    c. Wählen Sie **Unter Quarantäne gestellte Objekte löschen**.
    d. Wählen Sie **Änderungen übernehmen**.

Was ist eine Objektexistenzprüfung?

Die Objektexistenzprüfung überprüft, ob alle erwarteten replizierten Kopien von Objekten und Erasure-Coded-Fragmenten auf einem Speicherknoten vorhanden sind. Bei der Objekt-Existenzprüfung werden nicht die Objektdaten selbst überprüft (dies geschieht durch die Hintergrundüberprüfung). Stattdessen bietet sie eine Möglichkeit, die Integrität von Speichergeräten zu überprüfen, insbesondere wenn ein kürzlich aufgetretenes Hardwareproblem die Datenintegrität beeinträchtigt haben könnte.

Im Gegensatz zur Hintergrundüberprüfung, die automatisch erfolgt, müssen Sie einen Job zur Überprüfung der Objektexistenz manuell starten.

Die Objektexistenzprüfung liest die Metadaten für jedes in StorageGRID gespeicherte Objekt und überprüft die Existenz sowohl replizierter Objektkopien als auch löschcodierter Objektfragmente. Mit fehlenden Daten wird wie folgt verfahren:

- **Replizierte Kopien**: Wenn eine Kopie der replizierten Objektdaten fehlt, versucht StorageGRID automatisch, die Kopie durch eine an anderer Stelle im System gespeicherte Kopie zu ersetzen. Der Speicherknoten führt eine vorhandene Kopie durch eine ILM-Auswertung aus, die ergibt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da eine andere Kopie fehlt. Eine neue Kopie wird erstellt und platziert, um die aktiven ILM-Richtlinien des Systems zu erfüllen. Diese neue Kopie wird möglicherweise nicht am selben Ort abgelegt, an dem die fehlende Kopie gespeichert war.
- **Erasure-Coded-Fragmente**: Wenn ein Fragment eines Erasure-Coded-Objekts fehlt, versucht StorageGRID automatisch, das fehlende Fragment an Ort und Stelle auf demselben Speicherknoten mithilfe der verbleibenden Fragmente wiederherzustellen. Wenn das fehlende Fragment nicht wiederhergestellt werden kann (weil zu viele Fragmente verloren gegangen sind), versucht ILM, eine weitere Kopie des Objekts zu finden, mit der es ein neues Erasure-Coded-Fragment generieren kann.

Führen Sie eine Objekt-Existenzprüfung durch

Sie erstellen und führen jeweils einen Job zur Objektexistenzprüfung aus. Wenn Sie einen Job erstellen, wählen Sie die Speicherknoten und Volumes aus, die Sie überprüfen möchten. Sie wählen auch die Konsistenz für den Auftrag aus.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben sichergestellt, dass die Speicherknoten, die Sie überprüfen möchten, online sind. Wählen Sie **NODES** aus, um die Knotentabelle anzuzeigen. Stellen Sie sicher, dass neben dem Knotennamen der Knoten, die Sie überprüfen möchten, keine Warnsymbole angezeigt werden.
- Sie haben sichergestellt, dass die folgenden Prozeduren auf den Knoten, die Sie überprüfen möchten, **nicht** ausgeführt werden:
  - Netzerweiterung zum Hinzufügen eines Speicherknotens
  - Außerbetriebnahme von Speicherknoten
  - Wiederherstellung eines ausgefallenen Speichervolumes
  - Wiederherstellung eines Speicherknotens mit einem ausgefallenen Systemlaufwerk
  - EC-Neugewichtung
  - Appliance-Knotenklon

Die Objektexistenzprüfung liefert keine nützlichen Informationen, während diese Verfahren ausgeführt werden.

Informationen zu diesem Vorgang

Die Ausführung eines Objektexistenzprüfungsauftrags kann Tage oder Wochen dauern, abhängig von der Anzahl der Objekte im Raster, den ausgewählten Speicherknoten und Datenträgern und der ausgewählten Konsistenz. Sie können jeweils nur einen Job ausführen, aber Sie können mehrere Speicherknoten und Volumes gleichzeitig auswählen.

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Objektexistenzprüfung**.
2. Wählen Sie **Job erstellen**. Der Assistent „Job zur Objektexistenzprüfung erstellen“ wird angezeigt.
3. Wählen Sie die Knoten aus, die die Volumes enthalten, die Sie überprüfen möchten. Um alle Online-Knoten auszuwählen, aktivieren Sie das Kontrollkästchen **Knotenname** in der Spaltenüberschrift.

   Sie können nach Knotennamen oder Site suchen.

Sie können keine Knoten auswählen, die nicht mit dem Raster verbunden sind.

4. Wählen Sie **Weiter**.
5. Wählen Sie für jeden Knoten in der Liste ein oder mehrere Volumes aus. Sie können anhand der Speichervolumenummer oder des Knotennamens nach Volumes suchen.

   Um alle Volumes für jeden ausgewählten Knoten auszuwählen, aktivieren Sie das Kontrollkästchen **Speichervolume** in der Spaltenüberschrift.

6. Wählen Sie **Weiter**.
7. Wählen Sie die Konsistenz für den Auftrag aus.

   Die Konsistenz bestimmt, wie viele Kopien der Objektmetadaten für die Objektexistenzprüfung verwendet werden.

   - **Strong-Site**: Zwei Kopien der Metadaten an einer einzigen Site.
   - **Stark-global**: Zwei Kopien der Metadaten an jedem Standort.
   - **Alle** (Standard): Alle drei Kopien der Metadaten an jedem Standort.

     Weitere Informationen zur Konsistenz finden Sie in den Beschreibungen im Assistenten.

8. Wählen Sie **Weiter**.
9. Überprüfen und bestätigen Sie Ihre Auswahl. Sie können **Zurück** auswählen, um zu einem vorherigen Schritt im Assistenten zu gelangen und Ihre Auswahl zu aktualisieren.

   Ein Job zur Objektexistenzprüfung wird generiert und ausgeführt, bis eines der folgenden Ereignisse eintritt:

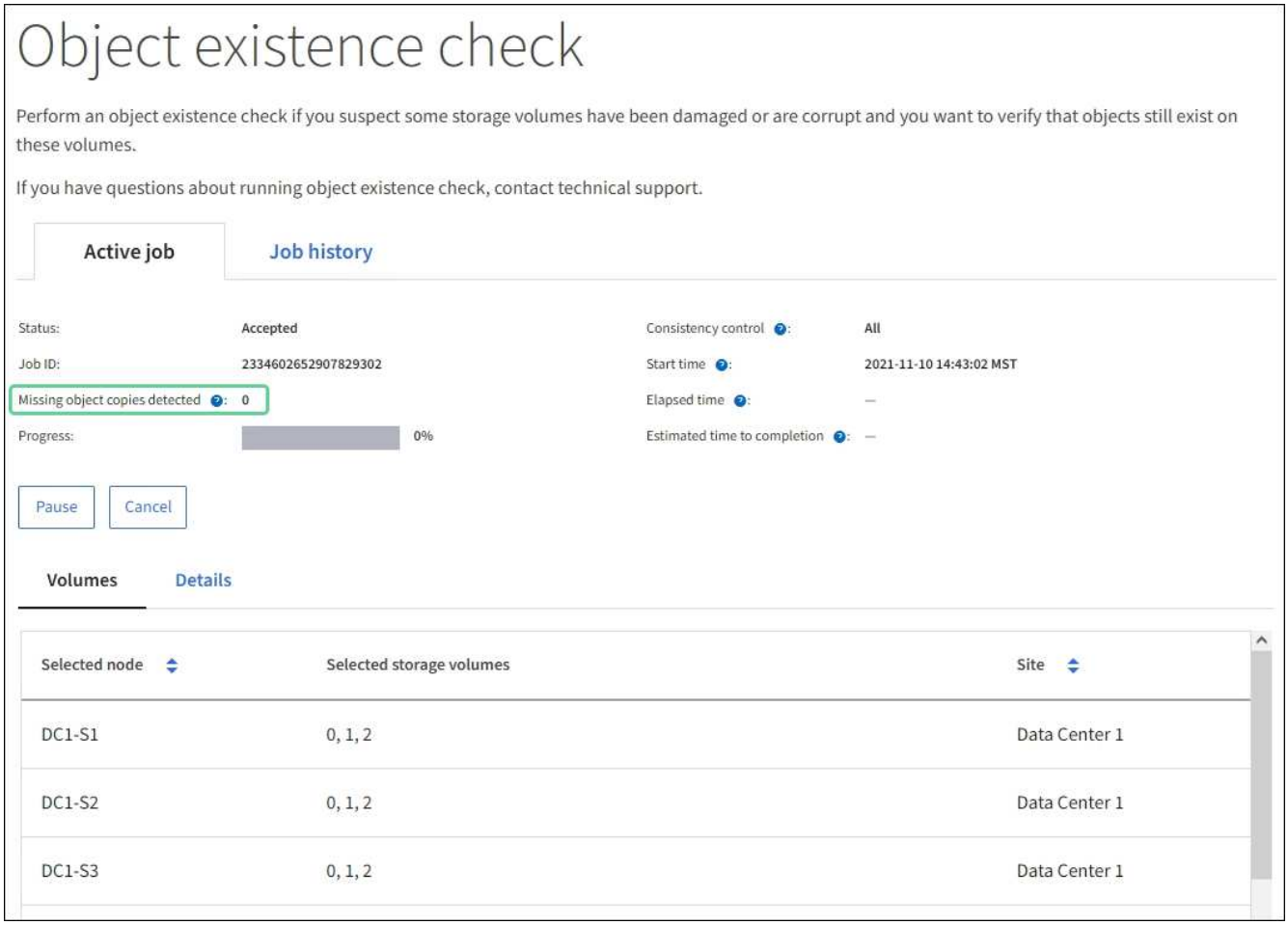
   - Der Auftrag ist abgeschlossen.
   - Sie pausieren oder brechen den Auftrag ab. Sie können einen Job fortsetzen, den Sie angehalten haben, aber Sie können einen Job nicht fortsetzen, den Sie abgebrochen haben.
   - Der Job stockt. Die Warnung „Prüfung der Objektexistenz ist ins Stocken geraten“ wird ausgelöst. Befolgen Sie die für die Warnung angegebenen Korrekturmaßnahmen.
   - Der Auftrag schlägt fehl. Die Warnung **Prüfung der Objektexistenz fehlgeschlagen** wird ausgelöst. Befolgen Sie die für die Warnung angegebenen Korrekturmaßnahmen.
   - Es wird die Meldung „Dienst nicht verfügbar“ oder „Interner Serverfehler“ angezeigt. Aktualisieren Sie die Seite nach einer Minute, um den Auftrag weiter zu überwachen.

   > Bei Bedarf können Sie von der Seite zur Objektexistenzprüfung weg navigieren und zurückkehren, um die Überwachung des Auftrags fortzusetzen.

10. Zeigen Sie während der Ausführung des Auftrags die Registerkarte **Aktiver Auftrag** an und notieren Sie sich den Wert „Fehlende Objektkopien erkannt“.

    Dieser Wert stellt die Gesamtzahl der fehlenden Kopien replizierter Objekte und löschcodierter Objekte mit einem oder mehreren fehlenden Fragmenten dar.

    Wenn die Anzahl der erkannten fehlenden Objektkopien größer als 100 ist, liegt möglicherweise ein Problem mit dem Speicher des Speicherknotens vor.



11. Führen Sie nach Abschluss des Auftrags alle weiteren erforderlichen Aktionen aus:
    - Wenn „Fehlende Objektkopien erkannt“ null ist, wurden keine Probleme gefunden. Es ist keine Aktion erforderlich.
    - Wenn die Anzahl der erkannten fehlenden Objektkopien größer als Null ist und die Warnung **Objekte verloren** nicht ausgelöst wurde, wurden alle fehlenden Kopien vom System repariert. Stellen Sie sicher, dass alle Hardwareprobleme behoben wurden, um zukünftige Schäden an Objektkopien zu verhindern.
    - Wenn die Anzahl der erkannten fehlenden Objektkopien größer als Null ist und die Warnung „Objekte verloren“ ausgelöst wurde, kann die Datenintegrität beeinträchtigt sein. Wenden Sie sich an den technischen Support.
    - Sie können verlorene Objektkopien untersuchen, indem Sie mit grep die LLST-Auditmeldungen extrahieren: `grep LLST audit_file_name` .

      Dieses Verfahren ist ähnlich wie bei"Untersuchung verlorener Gegenstände" , obwohl Sie für Objektkopien nach `LLST` anstatt `OLST` .

12. Wenn Sie für den Job die starke Site- oder starke globale Konsistenz ausgewählt haben, warten Sie ungefähr drei Wochen, bis die Metadatenkonsistenz erreicht ist, und führen Sie den Job dann erneut auf denselben Volumes aus.

    Wenn StorageGRID Zeit hatte, die Metadatenkonsistenz für die im Job enthaltenen Knoten und Volumes zu erreichen, kann eine erneute Ausführung des Jobs fälschlicherweise als fehlend gemeldete Objektkopien löschen oder dazu führen, dass zusätzliche Objektkopien überprüft werden, wenn diese fehlten.

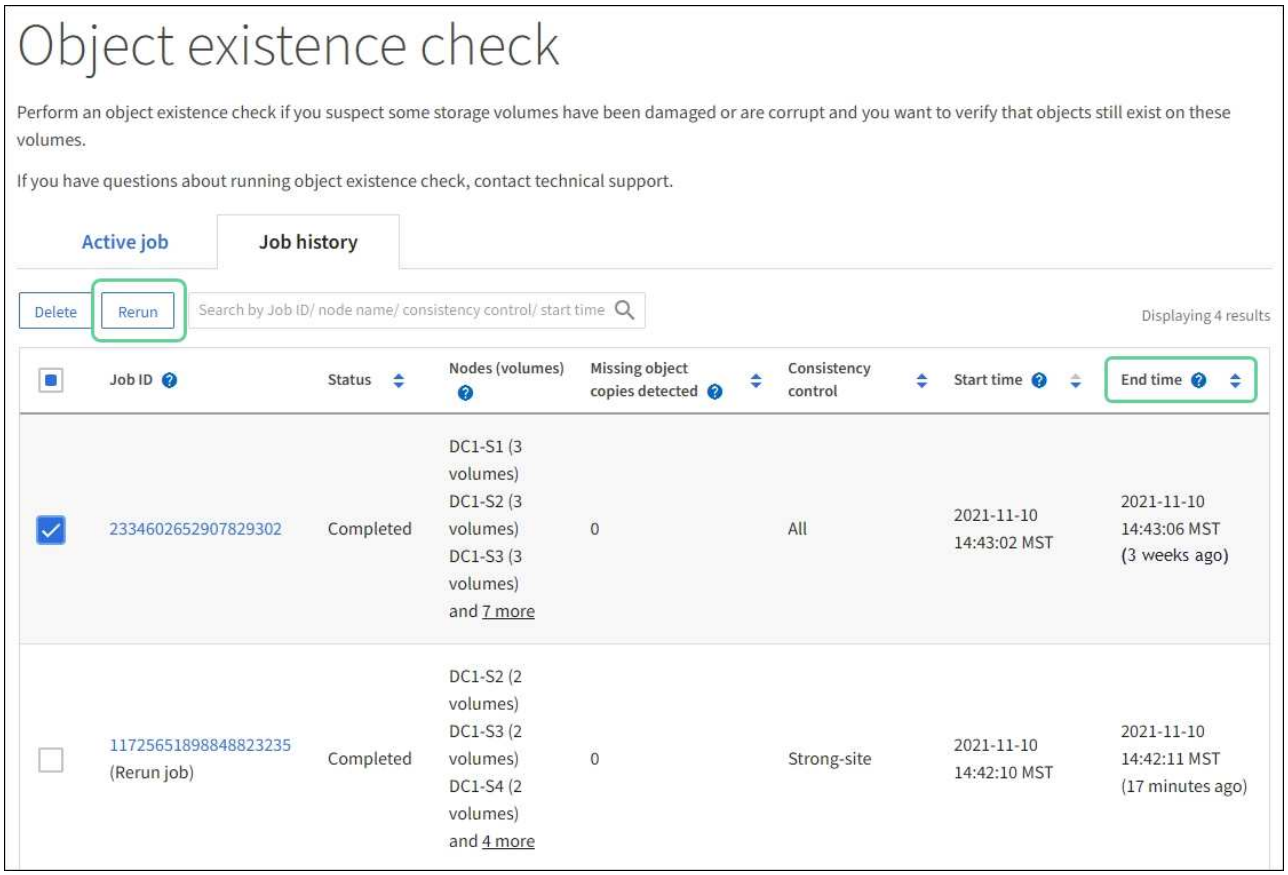
a. Wählen Sie **WARTUNG** > **Objektexistenzprüfung** > **Auftragsverlauf**.

b. Bestimmen Sie, welche Jobs zur erneuten Ausführung bereit sind:

   i. Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.

   ii. Durchsuchen Sie für diese Jobs die Spalte „Konsistenzkontrolle“ nach „Strong-Site“ oder „Strong-Global“.

c. Aktivieren Sie das Kontrollkästchen für jeden Job, den Sie erneut ausführen möchten, und wählen Sie dann **Erneut ausführen**.



d. Überprüfen Sie im Assistenten „Jobs erneut ausführen“ die ausgewählten Knoten und Volumes sowie die Konsistenz.

e. Wenn Sie bereit sind, die Jobs erneut auszuführen, wählen Sie **Erneut ausführen**.

Die Registerkarte „Aktiver Job“ wird angezeigt. Alle von Ihnen ausgewählten Jobs werden als ein Job mit einer starken Site-Konsistenz erneut ausgeführt. Im Feld **Verwandte Jobs** im Abschnitt „Details“ werden die Job-IDs für die ursprünglichen Jobs aufgelistet.

Nach Abschluss

Wenn Sie weiterhin Bedenken hinsichtlich der Datenintegrität haben, gehen Sie zu **SUPPORT** > **Tools** > **Grid-Topologie** > ***Site*** > ***Storage Node*** > **LDR** > **Verifizierung** > **Konfiguration** > **Main** und erhöhen Sie die Hintergrundüberprüfungsrate. Die Hintergrundüberprüfung prüft die Richtigkeit aller gespeicherten Objektdaten und behebt alle gefundenen Probleme. Durch das möglichst schnelle Auffinden und Beheben potenzieller Probleme wird das Risiko eines Datenverlusts verringert.

Fehlerbehebung bei der Warnung „S3 PUT-Objektgröße zu groß“

Die Warnung „S3 PUT-Objektgröße zu groß“ wird ausgelöst, wenn ein Mandant einen nicht mehrteiligen PutObject-Vorgang versucht, der die S3-Größenbeschränkung von 5 GiB überschreitet.

Bevor Sie beginnen

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

Ermitteln Sie, welche Mandanten Objekte verwenden, die größer als 5 GiB sind, damit Sie sie benachrichtigen können.

Schritte

1. Gehen Sie zu **KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**.
2. Wenn die Client-Schreibvorgänge normal sind, greifen Sie auf das Prüfprotokoll zu:

   a. Eingeben `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 `#` .

   e. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden.

   Das Prüfprotokollverzeichnis und die entsprechenden Knoten hängen von Ihren Prüfzieleinstellungen ab.

Option	Ziel
Lokale Knoten (Standard)	`/var/local/log/localaudit.log`
Admin-Knoten/lokale Knoten	• Admin-Knoten (primär und nicht primär): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Die Datei ist in diesem Modus normalerweise leer oder fehlt.
Externer Syslog-Server	`/var/local/log/localaudit.log`

   Geben Sie je nach Ihren Audit-Zieleinstellungen Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

   Weitere Informationen finden Sie unter"Auswählen von Zielen für Auditinformationen" .

   f. Ermitteln Sie, welche Mandanten Objekte verwenden, die größer als 5 GiB sind.

      i. Eingeben `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

ii. Sehen Sie sich für jede Prüfnachricht in den Ergebnissen Folgendes an: `S3AI` Feld, um die Mandantenkonto-ID zu bestimmen. Verwenden Sie die anderen Felder in der Nachricht, um zu bestimmen, welche IP-Adresse vom Client, dem Bucket und dem Objekt verwendet wurde:

Code	Beschreibung
SAIP	Quell-IP
S3AI	Mandanten-ID
S3BK	Eimer
S3KY	Objekt
CSIZ	Größe (Bytes)

Beispiel für Audit-Protokollergebnisse

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"933908492661540043 43"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::933908492661540043 43:root"][SBAI(CSTR):"933908492661540043 43"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Wenn Client-Schreibvorgänge nicht normal sind, verwenden Sie die Mandanten-ID aus der Warnung, um den Mandanten zu identifizieren:

   a. Gehen Sie zu **SUPPORT** > **Tools** > **Protokolle**. Sammeln Sie Anwendungsprotokolle für den Speicherknoten in der Warnung. Geben Sie 15 Minuten vor und nach der Warnung an.

   b. Extrahieren Sie die Datei und gehen Sie zu `bycast.log` :

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. Suchen Sie im Protokoll nach `method=PUT` und identifizieren Sie den Client in der `clientIP` Feld.

      Beispiel bycast.log

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Informieren Sie die Mieter, dass die maximale PutObject-Größe 5 GiB beträgt und dass für Objekte, die größer als 5 GiB sind, mehrteilige Uploads verwendet werden sollen.
5. Ignorieren Sie die Warnung eine Woche lang, wenn die Anwendung geändert wurde.

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Objekte können aus verschiedenen Gründen abgerufen werden, darunter Leseanforderungen einer Clientanwendung, Hintergrundüberprüfungen replizierter Objektdaten, ILM-Neubewertungen und die Wiederherstellung von Objektdaten während der Wiederherstellung eines Speicherknotens.

Das StorageGRID -System verwendet Standortinformationen in den Metadaten eines Objekts, um zu bestimmen, von welchem Standort das Objekt abgerufen werden soll. Wenn am erwarteten Speicherort keine Kopie des Objekts gefunden wird, versucht das System, eine weitere Kopie des Objekts von einer anderen Stelle im System abzurufen, wobei davon ausgegangen wird, dass die ILM-Richtlinie eine Regel zum Erstellen von zwei oder mehr Kopien des Objekts enthält.

Wenn dieser Abruf erfolgreich ist, ersetzt das StorageGRID -System die fehlende Kopie des Objekts. Andernfalls wird die Warnung „Objekte verloren“ wie folgt ausgelöst:

- Wenn bei replizierten Kopien keine weitere Kopie abgerufen werden kann, gilt das Objekt als verloren und die Warnung wird ausgelöst.
- Wenn bei Erasure-Coded-Kopien eine Kopie nicht vom erwarteten Speicherort abgerufen werden kann, wird das Attribut „Corrupt Copies Detected“ (ECOR) um eins erhöht, bevor versucht wird, eine Kopie von einem anderen Speicherort abzurufen. Wenn keine andere Kopie gefunden wird, wird der Alarm ausgelöst.

Sie sollten alle Warnmeldungen zum Thema „Objektverlust“ sofort untersuchen, um die Grundursache des Verlusts zu ermitteln und festzustellen, ob das Objekt möglicherweise noch in einem Offline- oder anderweitig derzeit nicht verfügbaren Speicherknoten vorhanden ist. Sehen "Untersuchen Sie verlorene Gegenstände" .

Für den Fall, dass Objektdaten ohne Kopien verloren gehen, gibt es keine Wiederherstellungslösung. Sie müssen jedoch den Zähler für verlorene Objekte zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren. Sehen "Zurücksetzen der Anzahl verlorener und fehlender Objekte" .

Untersuchen Sie verlorene Gegenstände

Wenn die Warnung „Objekte verloren“ ausgelöst wird, müssen Sie dies sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

Bevor Sie beginnen

- Sie müssen beim Grid Manager mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

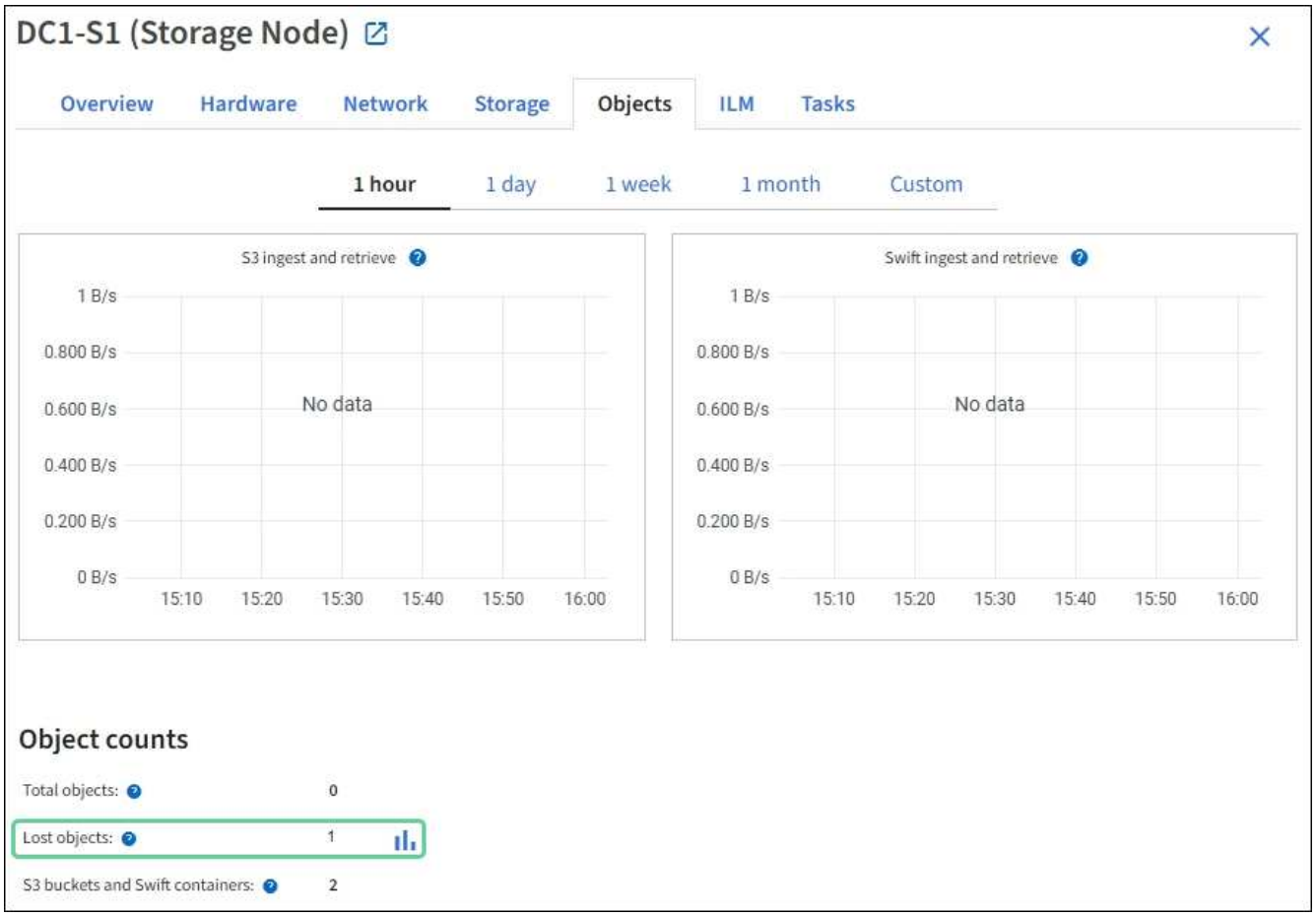
Die Warnung „Objekte verloren“ zeigt an, dass StorageGRID davon ausgeht, dass im Grid keine Kopien eines Objekts vorhanden sind. Möglicherweise sind die Daten dauerhaft verloren gegangen.

Gehen Sie Warnmeldungen zu verlorenen Gegenständen sofort nach. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu verhindern. In einigen Fällen können Sie einen verlorenen Gegenstand möglicherweise wiederherstellen, wenn Sie umgehend handeln.

Schritte

1. Wählen Sie **NODES**.
2. Wählen Sie ***Speicherknoten*** > **Objekte**.
3. Überprüfen Sie die Anzahl der verlorenen Objekte, die in der Objektanzahltabelle angezeigt wird.

   Diese Zahl gibt die Gesamtzahl der Objekte an, die dieser Grid-Knoten im gesamten StorageGRID System als fehlend erkennt. Der Wert ist die Summe der Zähler für verlorene Objekte der Datenspeicherkomponente innerhalb der LDR- und DDS-Dienste.



4. Von einem Admin-Knoten aus,"Zugriff auf das Überwachungsprotokoll" So ermitteln Sie die eindeutige Kennung (UUID) des Objekts, das die Warnung „Objekte verloren“ ausgelöst hat:
   a. Melden Sie sich beim Grid-Knoten an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden.

Das Prüfprotokollverzeichnis und die entsprechenden Knoten hängen von Ihren Prüfzieleinstellungen ab.

Option	Ziel
Lokale Knoten (Standard)	`/var/local/log/localaudit.log`
Admin-Knoten/lokale Knoten	• Admin-Knoten (primär und nicht primär): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Die Datei ist in diesem Modus normalerweise leer oder fehlt.
Externer Syslog-Server	`/var/local/log/localaudit.log`

Geben Sie je nach Ihren Audit-Zieleinstellungen Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

Weitere Informationen finden Sie unter"Auswählen von Zielen für Auditinformationen" .

c. Verwenden Sie grep, um die OLST-Auditmeldungen (Object Lost) zu extrahieren. Eingeben: `grep OLST audit_file_name`

d. Beachten Sie den in der Nachricht enthaltenen UUID-Wert.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Suchen Sie mithilfe der UUID nach den Metadaten für das verlorene Objekt:

a. Wählen Sie **ILM** > **Objektmetadatensuche**.

b. Geben Sie die UUID ein und wählen Sie **Nachschlagen**.

c. Überprüfen Sie die Standorte in den Metadaten und ergreifen Sie die entsprechenden Maßnahmen:

Metadaten	Abschluss
Objekt <Objektkennung> nicht gefunden	Wenn das Objekt nicht gefunden wird, wird die Meldung „ERROR":"“ zurückgegeben. Wenn das Objekt nicht gefunden wird, können Sie die Anzahl der **verlorenen Objekte** zurücksetzen, um die Warnung zu löschen. Das Fehlen eines Objekts weist darauf hin, dass das Objekt absichtlich gelöscht wurde.
Standorte > 0	Wenn in der Ausgabe Standorte aufgeführt sind, kann die Warnung „Objekte verloren“ ein Fehlalarm sein. Bestätigen Sie, dass die Objekte vorhanden sind. Verwenden Sie die in der Ausgabe aufgeführte Knoten-ID und den Dateipfad, um zu bestätigen, dass sich die Objektdatei am aufgeführten Speicherort befindet. (Das Verfahren für"Suche nach möglicherweise verlorenen Gegenständen" erklärt, wie Sie die Knoten-ID verwenden, um den richtigen Speicherknoten zu finden.) Wenn die Objekte vorhanden sind, können Sie die Anzahl der **verlorenen Objekte** zurücksetzen, um die Warnung zu löschen.
Standorte = 0	Wenn in der Ausgabe keine Standorte aufgeführt sind, fehlt das Objekt möglicherweise. Sie können versuchen,"Suchen und Wiederherstellen des Objekts" selbst oder Sie können sich an den technischen Support wenden. Der technische Support wird Sie möglicherweise bitten, festzustellen, ob gerade ein Speicherwiederherstellungsverfahren läuft. Informationen zu"Wiederherstellen von Objektdaten mit Grid Manager" Und"Wiederherstellen von Objektdaten auf einem Speichervolume" .

Suchen und Wiederherstellen potenziell verlorener Objekte

Möglicherweise ist es möglich, Objekte zu finden und wiederherzustellen, die eine **Objekt verloren**-Warnung und einen älteren „Lost Objects“-Alarm (LOST) ausgelöst haben und die Sie als potenziell verloren identifiziert haben.

Bevor Sie beginnen

- Sie haben die UUID eines verlorenen Objekts, wie in"Untersuchen Sie verlorene Gegenstände" .
- Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Sie können dieses Verfahren befolgen, um an anderer Stelle im Raster nach replizierten Kopien des verlorenen Objekts zu suchen. In den meisten Fällen wird der verlorene Gegenstand nicht gefunden. In einigen Fällen können Sie jedoch möglicherweise ein verlorenes repliziertes Objekt finden und wiederherstellen, wenn Sie umgehend Maßnahmen ergreifen.

Wenden Sie sich an den technischen Support, um Hilfe bei diesem Verfahren zu erhalten.

Schritte

1. Durchsuchen Sie von einem Admin-Knoten aus die Prüfprotokolle nach möglichen Objektstandorten:

   a. Melden Sie sich beim Grid-Knoten an:

      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

      ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

      iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

   b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden.

      Das Prüfprotokollverzeichnis und die entsprechenden Knoten hängen von Ihren Prüfzieleinstellungen ab.

Option	Ziel
Lokale Knoten (Standard)	`/var/local/log/localaudit.log`
Admin-Knoten/lokale Knoten	• Admin-Knoten (primär und nicht primär): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Die Datei ist in diesem Modus normalerweise leer oder fehlt.
Externer Syslog-Server	`/var/local/log/localaudit.log`

      Geben Sie je nach Ihren Audit-Zieleinstellungen Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

      Weitere Informationen finden Sie unter"Auswählen von Zielen für Auditinformationen" .

   c. Verwenden Sie grep, um die"Prüfmeldungen im Zusammenhang mit dem möglicherweise verlorenen Objekt" und senden Sie sie an eine Ausgabedatei. Eingeben: `grep uuid-value audit_file_name > output_file_name`

      Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

   d. Verwenden Sie grep, um die LLST-Auditmeldungen (Location Lost) aus dieser Ausgabedatei zu extrahieren. Eingeben: `grep LLST output_file_name`

      Beispiel:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

Eine LLST-Auditnachricht sieht wie diese Beispielnachricht aus.

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

e. Suchen Sie das PCLD-Feld und das NOID-Feld in der LLST-Nachricht.

Falls vorhanden, ist der Wert von PCLD der vollständige Pfad auf der Festplatte zur fehlenden replizierten Objektkopie. Der Wert von NOID ist die Knoten-ID des LDR, in dem eine Kopie des Objekts gefunden werden kann.

Wenn Sie einen Objektspeicherort finden, können Sie das Objekt möglicherweise wiederherstellen.

a. Suchen Sie den Speicherknoten, der dieser LDR-Knoten-ID zugeordnet ist. Wählen Sie im Grid Manager **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie dann ***Data Center*** > ***Storage Node*** > **LDR**.

Die Knoten-ID für den LDR-Dienst befindet sich in der Knoteninformationstabelle. Überprüfen Sie die Informationen für jeden Speicherknoten, bis Sie denjenigen finden, der diesen LDR hostet.

2. Stellen Sie fest, ob das Objekt auf dem in der Prüfnachricht angegebenen Speicherknoten vorhanden ist:

a. Melden Sie sich beim Grid-Knoten an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

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

b. Stellen Sie fest, ob der Dateipfad für das Objekt vorhanden ist.

Verwenden Sie für den Dateipfad des Objekts den PCLD-Wert aus der LLST-Auditnachricht.

Geben Sie beispielsweise Folgendes ein:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Setzen Sie den Objektdateipfad in Befehlen immer in einfache Anführungszeichen, um Sonderzeichen zu maskieren.

- Wenn der Objektpfad nicht gefunden wird, ist das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wurde, fahren Sie mit dem nächsten Schritt fort. Sie können versuchen, das gefundene Objekt wieder in StorageGRID wiederherzustellen.

3. Wenn der Objektpfad gefunden wurde, versuchen Sie, das Objekt in StorageGRID wiederherzustellen:
   a. Ändern Sie vom selben Speicherknoten aus den Besitz der Objektdatei, sodass sie von StorageGRID verwaltet werden kann. Eingeben: `chown ldr-user:bycast 'file_path_of_object'`
   b. Um auf die LDR-Konsole zuzugreifen, greifen Sie per Telnet auf den Localhost 1402 zu. Eingeben: `telnet 0 1402`
   c. Eingeben: `cd /proc/STOR`
   d. Eingeben: `Object_Found 'file_path_of_object'`

      Geben Sie beispielsweise Folgendes ein:

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Ausgabe der `Object_Found` Der Befehl benachrichtigt das Raster über den Standort des Objekts. Außerdem werden dadurch die aktiven ILM-Richtlinien ausgelöst, die zusätzliche Kopien gemäß den Angaben in den einzelnen Richtlinien erstellen.

      Wenn der Speicherknoten, auf dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf jeden Speicherknoten kopieren, der online ist. Platzieren Sie das Objekt in einem beliebigen /var/local/rangedb-Verzeichnis des Online-Speicherknotens. Geben Sie dann die `Object_Found` Befehl unter Verwendung dieses Dateipfads zum Objekt.

      - Wenn das Objekt nicht wiederhergestellt werden kann, `Object_Found` Befehl schlägt fehl. Wenden Sie sich an den technischen Support.
      - Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, wird eine Erfolgsmeldung angezeigt. Beispiel:

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

        Fahren Sie mit dem nächsten Schritt fort.

4. Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, überprüfen Sie, ob die neuen

Speicherorte erstellt wurden:

a. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .

b. Wählen Sie **ILM** > **Objektmetadatensuche**.

c. Geben Sie die UUID ein und wählen Sie **Nachschlagen**.

d. Überprüfen Sie die Metadaten und bestätigen Sie die neuen Standorte.

5. Suchen Sie von einem Admin-Knoten aus in den Prüfprotokollen nach der ORLM-Prüfnachricht für dieses Objekt, um zu bestätigen, dass das Information Lifecycle Management (ILM) die erforderlichen Kopien platziert hat.

a. Melden Sie sich beim Grid-Knoten an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden. SieheUnterschritt 1. b .

c. Verwenden Sie grep, um die mit dem Objekt verknüpften Prüfmeldungen in eine Ausgabedatei zu extrahieren. Eingeben: `grep uuid-value audit_file_name > output_file_name`

Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_restored_object.txt
```

d. Verwenden Sie grep, um die ORLM-Auditmeldungen (Object Rules Met) aus dieser Ausgabedatei zu extrahieren. Eingeben: `grep ORLM output_file_name`

Beispiel:

```
Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
```

Eine ORLM-Auditnachricht sieht wie diese Beispielnachricht aus.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Suchen Sie das LOCS-Feld in der Prüfnachricht.

   Falls vorhanden, ist der Wert von CLDI in LOCS die Knoten-ID und die Volume-ID, auf der eine Objektkopie erstellt wurde. Diese Meldung zeigt an, dass das ILM angewendet wurde und dass zwei Objektkopien an zwei Stellen im Grid erstellt wurden.

6. "Setzen Sie die Anzahl verlorener und fehlender Objekte zurück"im Grid Manager.

Zurücksetzen der Anzahl verlorener und fehlender Objekte

Nachdem Sie das StorageGRID -System untersucht und überprüft haben, dass alle aufgezeichneten verlorenen Objekte dauerhaft verloren sind oder es sich um einen Fehlalarm handelt, können Sie den Wert des Attributs „Lost Objects“ auf Null zurücksetzen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

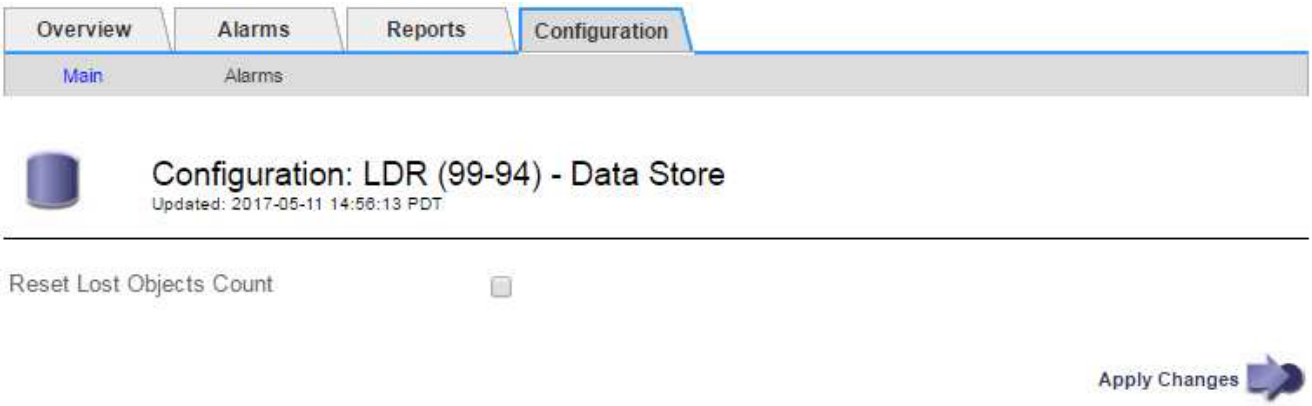
Sie können den Zähler für verlorene Objekte auf einer der folgenden Seiten zurücksetzen:

- **SUPPORT** > **Tools** > **Grid-Topologie** > ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Übersicht** > **Main**
- **SUPPORT** > **Tools** > **Grid-Topologie** > ***Site*** > ***Storage Node*** > **DDS** > **Data Store** > **Übersicht** > **Main**

Diese Anweisungen zeigen das Zurücksetzen des Zählers von der Seite **LDR** > **Datenspeicher**.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Configuration** für den Storage Node, der die Warnung **Objects lost** oder den LOST-Alarm aufweist.
3. Wählen Sie **Anzahl verlorener Objekte zurücksetzen**.



4. Klicken Sie auf **Änderungen übernehmen**.

   Das Attribut „Verlorene Objekte“ wird auf 0 zurückgesetzt und die Warnung „Objekte verloren“ sowie der Alarm „VERLOREN“ werden gelöscht. Dies kann einige Minuten dauern.

5. Optional können Sie andere zugehörige Attributwerte zurücksetzen, die beim Identifizieren des verlorenen Objekts möglicherweise erhöht wurden.

   a. Wählen Sie ***Site*** > ***Storage Node*** > **LDR** > **Erasure Coding** > **Konfiguration**.

   b. Wählen Sie **Anzahl Lesefehler zurücksetzen** und **Anzahl erkannter beschädigter Kopien zurücksetzen**.

   c. Klicken Sie auf **Änderungen übernehmen**.

   d. Wählen Sie ***Site*** > ***Storage Node*** > **LDR** > **Verifizierung** > **Konfiguration**.

   e. Wählen Sie **Anzahl fehlender Objekte zurücksetzen** und **Anzahl beschädigter Objekte zurücksetzen**.

   f. Wenn Sie sicher sind, dass die unter Quarantäne gestellten Objekte nicht benötigt werden, können Sie „Unter Quarantäne gestellte Objekte löschen“ auswählen.

      Quarantäneobjekte werden erstellt, wenn bei der Hintergrundüberprüfung eine beschädigte replizierte Objektkopie identifiziert wird. In den meisten Fällen ersetzt StorageGRID das beschädigte Objekt automatisch und die unter Quarantäne gestellten Objekte können sicher gelöscht werden. Wenn jedoch die Warnung „Objekte verloren“ oder der Alarm „VERLOREN“ ausgelöst wird, möchte der technische Support möglicherweise auf die unter Quarantäne gestellten Objekte zugreifen.

   g. Klicken Sie auf **Änderungen übernehmen**.

   Es kann einige Augenblicke dauern, bis die Attribute zurückgesetzt werden, nachdem Sie auf **Änderungen übernehmen** geklickt haben.

Fehlerbehebung bei der Warnung „Niedriger Objektdatenspeicher“

Die Warnung **Geringer Objektdatenspeicher** überwacht, wie viel Speicherplatz zum Speichern von Objektdaten auf jedem Speicherknoten verfügbar ist.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Die Warnung **Geringer Objektdatenspeicher** wird ausgelöst, wenn die Gesamtmenge der replizierten und löschcodierten Objektdaten auf einem Speicherknoten eine der in der Warnregel konfigurierten Bedingungen erfüllt.

Standardmäßig wird eine wichtige Warnung ausgelöst, wenn diese Bedingung als wahr ausgewertet wird:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In diesem Zustand:

- `storagegrid_storage_utilization_data_bytes`ist eine Schätzung der Gesamtgröße der replizierten und erasure-coded Objektdaten für einen Speicherknoten.

- `storagegrid_storage_utilization_usable_space_bytes`ist die Gesamtmenge des für einen Speicherknoten verbleibenden Objektspeicherplatzes.

Wenn eine größere oder kleinere Warnung „Geringer Objektdatenspeicher“ ausgelöst wird, sollten Sie so schnell wie möglich eine Erweiterungsprozedur durchführen.

Schritte

1. Wählen Sie **WARNUNGEN** > **Aktuell**.

   Die Seite „Warnungen“ wird angezeigt.

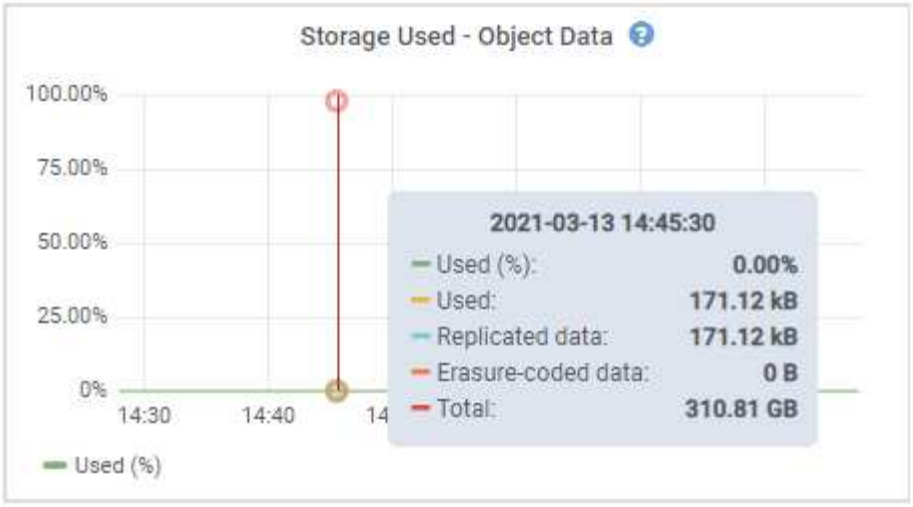
2. Erweitern Sie in der Tabelle der Warnungen bei Bedarf die Warnungsgruppe **Niedriger Objektdatenspeicher** und wählen Sie die Warnung aus, die Sie anzeigen möchten.

   Wählen Sie die Warnung aus, nicht die Überschrift für eine Gruppe von Warnungen.

3. Überprüfen Sie die Details im Dialogfeld und beachten Sie Folgendes:
   - Zeitgesteuert
   - Der Name der Site und des Knotens
   - Die aktuellen Werte der Metriken für diese Warnung
4. Wählen Sie **NODES** > ***Speicherknoten oder -Site*** > **Speicher**.
5. Positionieren Sie den Cursor über dem Diagramm „Speicherplatznutzung – Objektdaten“.

   Es werden folgende Werte angezeigt:

   - **Verwendet (%)**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
   - **Verwendet**: Die Menge des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
   - **Replizierte Daten**: Eine Schätzung der Menge der replizierten Objektdaten auf diesem Knoten, dieser Site oder diesem Raster.
   - **Löschcodierte Daten**: Eine Schätzung der Menge der löschcodierten Objektdaten auf diesem Knoten, dieser Site oder diesem Raster.
   - **Gesamt**: Die Gesamtmenge des nutzbaren Speicherplatzes auf diesem Knoten, dieser Site oder diesem Raster. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` metrisch.



6. Wählen Sie die Zeitsteuerungen über dem Diagramm aus, um die Speichernutzung über verschiedene Zeiträume anzuzeigen.

   Durch die Betrachtung der Speichernutzung im Zeitverlauf können Sie besser nachvollziehen, wie viel Speicher vor und nach dem Auslösen der Warnung verwendet wurde. Außerdem können Sie so abschätzen, wie lange es dauern könnte, bis der verbleibende Speicherplatz des Knotens voll ist.

7. So schnell wie möglich,"Speicherkapazität hinzufügen" zu Ihrem Raster.

   Sie können Speichervolumes (LUNs) zu vorhandenen Speicherknoten hinzufügen oder neue Speicherknoten hinzufügen.

   Weitere Informationen finden Sie unter "Vollständige Speicherknoten verwalten" .

Fehlerbehebung bei Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens „Niedrig“

Wenn Sie benutzerdefinierte Werte für Speichervolume-Wasserzeichen verwenden, müssen Sie möglicherweise die Warnung „Niedriges schreibgeschütztes Wasserzeichen überschreiben“ beheben. Wenn möglich, sollten Sie Ihr System aktualisieren, um die optimierten Werte zu verwenden.

In früheren Versionen waren die drei"Speichervolumen-Wasserzeichen" waren globale Einstellungen – dieselben Werte wurden auf jedes Speichervolumen auf jedem Speicherknoten angewendet. Ab StorageGRID 11.6 kann die Software diese Wasserzeichen für jedes Speichervolumen basierend auf der Größe des Speicherknotens und der relativen Kapazität des Volumens optimieren.

Wenn Sie auf StorageGRID 11.6 oder höher aktualisieren, werden optimierte schreibgeschützte und Lese-/Schreib-Wasserzeichen automatisch auf alle Speichervolumes angewendet, es sei denn, einer der folgenden Punkte trifft zu:

- Ihr System ist fast ausgelastet und könnte keine neuen Daten aufnehmen, wenn optimierte Wasserzeichen angewendet würden. StorageGRID ändert in diesem Fall die Wasserzeicheneinstellungen nicht.
- Sie haben zuvor eines der Wasserzeichen des Speichervolumens auf einen benutzerdefinierten Wert festgelegt. StorageGRID überschreibt benutzerdefinierte Wasserzeicheneinstellungen nicht durch optimierte Werte. StorageGRID kann jedoch die Warnung **Niedriges schreibgeschütztes Wasserzeichen**

außer Kraft setzen auslösen, wenn Ihr benutzerdefinierter Wert für das weiche schreibgeschützte Wasserzeichen des Speichervolumes zu klein ist.

Verstehen Sie die Warnung

Wenn Sie benutzerdefinierte Werte für Speichervolume-Wasserzeichen verwenden, wird möglicherweise für einen oder mehrere Speicherknoten die Warnung **Niedriges schreibgeschütztes Wasserzeichen außer Kraft setzen** ausgelöst.

Jede Instanz der Warnung zeigt an, dass der benutzerdefinierte Wert des weichen schreibgeschützten Wasserzeichens des Speichervolumes kleiner ist als der minimal optimierte Wert für diesen Speicherknoten. Wenn Sie weiterhin die benutzerdefinierte Einstellung verwenden, kann es passieren, dass der Speicherplatz des Speicherknotens kritisch knapp wird, bevor er sicher in den schreibgeschützten Zustand wechseln kann. Auf einige Speichervolumes kann möglicherweise nicht mehr zugegriffen werden (sie werden automatisch ausgehängt), wenn der Knoten seine Kapazitätsgrenze erreicht.

Angenommen, Sie haben das Soft-Read-Only-Wasserzeichen des Speichervolumes zuvor auf 5 GB festgelegt. Nehmen wir nun an, dass StorageGRID die folgenden optimierten Werte für die vier Speichervolumes im Speicherknoten A berechnet hat:

Band 0	12 GB
Band 1	12 GB
Band 2	11 GB
Band 3	15 GB

Die Warnung **Niedriger schreibgeschützter Wasserzeichen-Override** wird für Speicherknoten A ausgelöst, weil Ihr benutzerdefiniertes Wasserzeichen (5 GB) kleiner ist als der minimal optimierte Wert für alle Volumes in diesem Knoten (11 GB). Wenn Sie weiterhin die benutzerdefinierte Einstellung verwenden, kann der Speicherplatz des Knotens möglicherweise kritisch knapp werden, bevor er sicher in den schreibgeschützten Zustand wechseln kann.

Beheben Sie die Warnung

Führen Sie die folgenden Schritte aus, wenn eine oder mehrere Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens „Niedrig“ ausgelöst wurden. Sie können diese Anweisungen auch verwenden, wenn Sie derzeit benutzerdefinierte Wasserzeicheneinstellungen verwenden und optimierte Einstellungen verwenden möchten, auch wenn keine Warnungen ausgelöst wurden.

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" .

Informationen zu diesem Vorgang

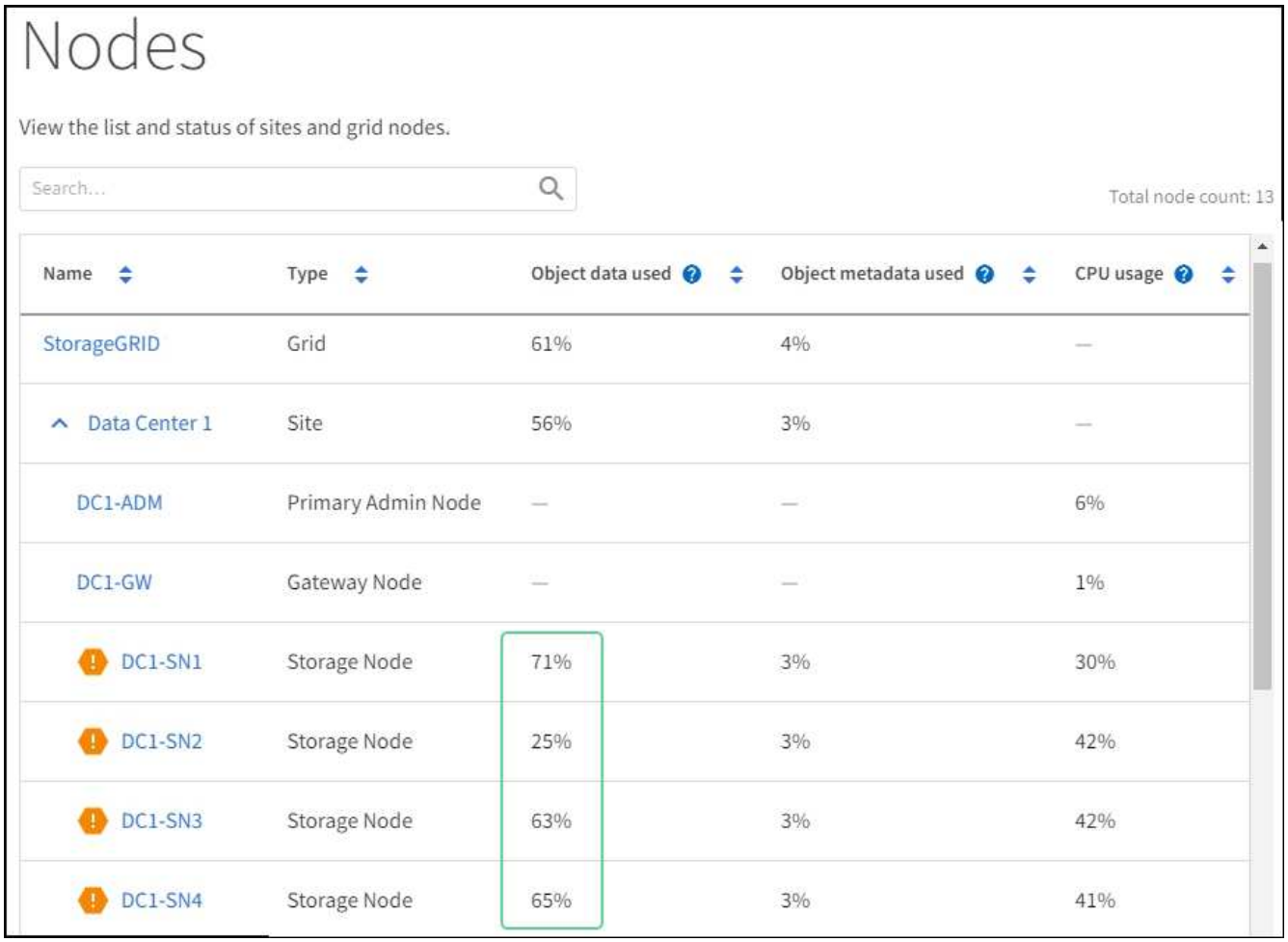
Sie können die Warnung **Niedriger schreibgeschützter Wasserzeichen-Override** beheben, indem Sie die benutzerdefinierten Wasserzeicheneinstellungen auf die neuen Wasserzeichen-Overrides aktualisieren. Wenn jedoch ein oder mehrere Speicherknoten fast voll sind oder Sie spezielle ILM-Anforderungen haben, sollten Sie sich zunächst die optimierten Speicherwasserzeichen ansehen und feststellen, ob deren Verwendung

sicher ist.

Bewerten Sie die Objektdatennutzung für das gesamte Raster

Schritte

1. Wählen Sie **NODES**.
2. Erweitern Sie für jede Site im Raster die Liste der Knoten.
3. Überprüfen Sie die Prozentwerte, die in der Spalte **Verwendete Objektdaten** für jeden Speicherknoten an jedem Standort angezeigt werden.



4. Führen Sie den entsprechenden Schritt aus:
   a. Wenn keiner der Speicherknoten annähernd voll ist (z. B. alle Werte für **verwendete Objektdaten** kleiner als 80 % sind), können Sie mit der Verwendung der Überschreibungseinstellungen beginnen. Gehe zuVerwenden Sie optimierte Wasserzeichen .
   b. Wenn ILM-Regeln ein striktes Ingest-Verhalten verwenden oder wenn bestimmte Speicherpools fast voll sind, führen Sie die Schritte inOptimierte Speicherwasserzeichen anzeigen UndBestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können .

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.

Schritte

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.

5. Beachten Sie den maximal optimierten Wert für jeden Speicherknoten.

[[optimierte Wasserzeichen bestimmen]]Stellen Sie fest, ob Sie optimierte Wasserzeichen verwenden können

Schritte

1. Wählen Sie **NODES**.
2. Wiederholen Sie diese Schritte für jeden Online-Speicherknoten:
   a. Wählen Sie ***Speicherknoten*** > **Speicher**.
   b. Scrollen Sie nach unten zur Tabelle „Objektspeicher“.
   c. Vergleichen Sie den **Verfügbar**-Wert für jeden Objektspeicher (Volume) mit dem maximal optimierten Wasserzeichen, das Sie für diesen Speicherknoten notiert haben.
3. Wenn mindestens ein Volume auf jedem Online-Speicherknoten mehr Speicherplatz zur Verfügung hat als das maximal optimierte Wasserzeichen für diesen Knoten, gehen Sie zuVerwenden Sie optimierte Wasserzeichen um mit der Verwendung der optimierten Wasserzeichen zu beginnen.

   Andernfalls erweitern Sie das Netz so schnell wie möglich. Entweder"Speichervolumes hinzufügen" zu einem bestehenden Knoten oder"neue Speicherknoten hinzufügen" . Gehen Sie dann zuVerwenden Sie optimierte Wasserzeichen um die Wasserzeicheneinstellungen zu aktualisieren.

4. Wenn Sie weiterhin benutzerdefinierte Werte für die Speichervolumen-Wasserzeichen verwenden müssen,"Schweigen" oder"deaktivieren" die Warnung **Niedriges schreibgeschütztes Wasserzeichen überschreiben**.

Auf jedem Speichervolume auf jedem Speicherknoten werden dieselben benutzerdefinierten Wasserzeichenwerte angewendet. Die Verwendung kleinerer Werte als empfohlen für Speichervolume-Wasserzeichen kann dazu führen, dass auf einige Speichervolumes nicht mehr zugegriffen werden kann (sie werden automatisch ausgehängt), wenn der Knoten seine Kapazitätsgrenze erreicht.

Verwenden Sie optimierte Wasserzeichen

Schritte

1. Gehen Sie zu **SUPPORT** > **Sonstiges** > **Speicherwasserzeichen**.
2. Aktivieren Sie das Kontrollkästchen **Optimierte Werte verwenden**.
3. Wählen Sie **Speichern**.

Für jedes Speichervolume gelten jetzt optimierte Wasserzeicheneinstellungen, basierend auf der Größe des Speicherknotens und der relativen Kapazität des Volumes.

Beheben von Metadatenproblemen

Wenn Metadatenprobleme auftreten, werden Sie durch Warnmeldungen über die Ursache der Probleme und empfohlene Maßnahmen informiert. Insbesondere müssen Sie neue Speicherknoten hinzufügen, wenn die Warnung „Geringer Metadatenspeicher“ ausgelöst wird.

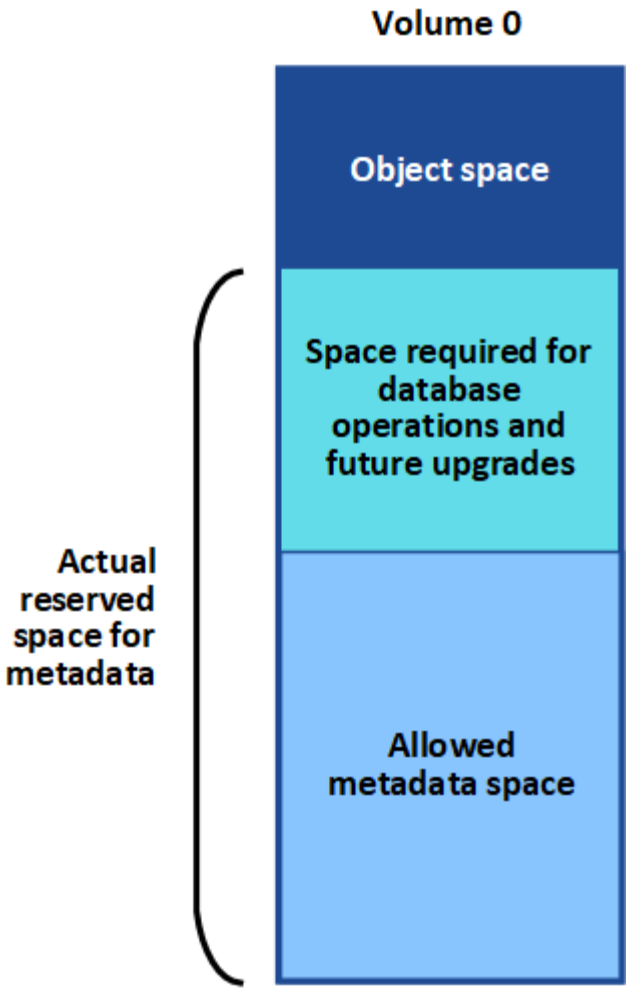
Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Befolgen Sie die empfohlenen Maßnahmen für jede ausgelöste Metadatenwarnung. Wenn die Warnung **Geringer Metadatenspeicher** ausgelöst wird, müssen Sie neue Speicherknoten hinzufügen.

StorageGRID reserviert auf Volume 0 jedes Speicherknotens eine bestimmte Menge Speicherplatz für Objektmetadaten. Dieser Speicherplatz, der als *tatsächlich reservierter Speicherplatz* bezeichnet wird, ist unterteilt in den für Objektmetadaten zulässigen Speicherplatz (den zulässigen Metadatenspeicherplatz) und den für wesentliche Datenbankvorgänge wie Komprimierung und Reparatur erforderlichen Speicherplatz. Der zulässige Metadatenspeicherplatz bestimmt die Gesamtobjektkapazität.



Wenn Objektmetadaten mehr als 100 % des für Metadaten zulässigen Speicherplatzes beanspruchen, können Datenbankvorgänge nicht effizient ausgeführt werden und es treten Fehler auf.

Du kannst"Überwachen Sie die Objektmetadatenkapazität für jeden Speicherknoten" um Ihnen zu helfen, Fehler vorherzusehen und zu korrigieren, bevor sie auftreten.

StorageGRID verwendet die folgende Prometheus-Metrik, um zu messen, wie voll der zulässige Metadatenspeicher ist:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

Wenn dieser Prometheus-Ausdruck bestimmte Schwellenwerte erreicht, wird die Warnung „Geringer Metadatenspeicher“ ausgelöst.

- **Geringfügig**: Objektmetadaten verwenden 70 % oder mehr des zulässigen Metadatenspeicherplatzes. Sie sollten so schnell wie möglich neue Speicherknoten hinzufügen.
- **Schwerwiegend**: Objektmetadaten verwenden 90 % oder mehr des zulässigen Metadatenspeichers. Sie müssen sofort neue Speicherknoten hinzufügen.

Wenn Objektmetadaten 90 % oder mehr des zulässigen Metadatenspeicherplatzes belegen, wird auf dem Dashboard eine Warnung angezeigt. Wenn diese Warnung erscheint, müssen Sie sofort neue Speicherknoten hinzufügen. Sie dürfen niemals zulassen, dass Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes belegen.

- **Kritisch**: Objektmetadaten verwenden 100 % oder mehr des zulässigen Metadatenspeicherplatzes und beginnen, den für wichtige Datenbankvorgänge erforderlichen Speicherplatz zu verbrauchen. Sie müssen die Aufnahme neuer Objekte stoppen und sofort neue Speicherknoten hinzufügen.

Wenn die Größe von Volume 0 kleiner ist als die Speicheroption „Reservierter Speicherplatz für Metadaten“ (z. B. in einer Nicht-Produktionsumgebung), ist die Berechnung für die Warnung „Geringer Metadatenspeicher“ möglicherweise ungenau.

Schritte

1. Wählen Sie **WARNUNGEN** > **Aktuell**.
2. Erweitern Sie in der Tabelle der Warnungen bei Bedarf die Warnungsgruppe **Geringer Metadatenspeicher** und wählen Sie die Warnung aus, die Sie anzeigen möchten.
3. Überprüfen Sie die Details im Warndialogfeld.
4. Wenn eine schwerwiegende oder kritische Warnung „Geringer Metadatenspeicher“ ausgelöst wurde, führen Sie sofort eine Erweiterung durch, um Speicherknoten hinzuzufügen.

Da StorageGRID an jedem Standort vollständige Kopien aller Objektmetadaten speichert, ist die Metadatenkapazität des gesamten Grids durch die Metadatenkapazität des kleinsten Standorts begrenzt. Wenn Sie die Metadatenkapazität einer Site erweitern müssen, sollten Sie auch"Erweitern Sie alle anderen Sites" durch die gleiche Anzahl von Speicherknoten.

Nachdem Sie die Erweiterung durchgeführt haben, verteilt StorageGRID die vorhandenen Objektmetadaten auf die neuen Knoten, wodurch die Gesamtmetadatenkapazität des Grids erhöht wird. Es ist keine Benutzeraktion erforderlich. Die Warnung **Geringer Metadatenspeicher** wird gelöscht.

Beheben von Zertifikatsfehlern

Wenn beim Versuch, über einen Webbrowser, einen S3-Client oder ein externes Überwachungstool eine Verbindung zu StorageGRID herzustellen, ein Sicherheits- oder Zertifikatsproblem auftritt, sollten Sie das Zertifikat überprüfen.

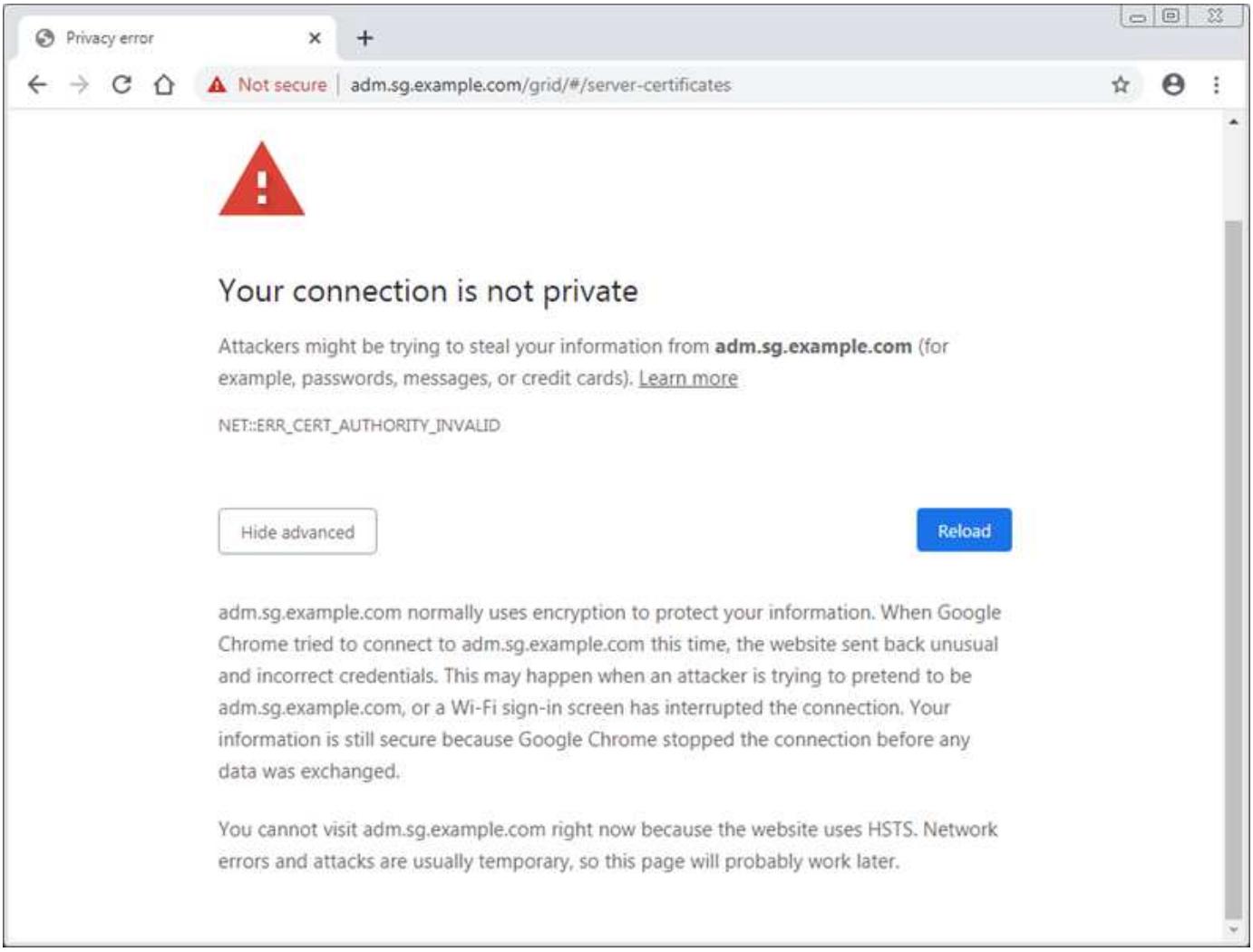
Informationen zu diesem Vorgang

Zertifikatsfehler können Probleme verursachen, wenn Sie versuchen, über den Grid Manager, die Grid Management API, den Tenant Manager oder die Tenant Management API eine Verbindung zu StorageGRID herzustellen. Zertifikatsfehler können auch auftreten, wenn Sie versuchen, eine Verbindung mit einem S3-Client oder einem externen Überwachungstool herzustellen.

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.
- Sie kehren von einem benutzerdefinierten Verwaltungsschnittstellenzertifikat zum Standardserverzertifikat zurück.

Das folgende Beispiel zeigt einen Zertifikatsfehler, wenn das Zertifikat der benutzerdefinierten Verwaltungsschnittstelle abgelaufen ist:



Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des Serverzertifikats für die Verwaltungsschnittstelle** ausgelöst, wenn das Serverzertifikat bald abläuft.

Wenn Sie Client-Zertifikate für die externe Prometheus-Integration verwenden, können Zertifikatsfehler durch das Zertifikat der StorageGRID Verwaltungsschnittstelle oder durch Client-Zertifikate verursacht werden. Die Warnung **Ablauf der auf der Seite „Zertifikate“ konfigurierten Client-Zertifikate** wird ausgelöst, wenn ein Client-Zertifikat bald abläuft.

Schritte

Wenn Sie eine Warnmeldung über ein abgelaufenes Zertifikat erhalten haben, greifen Sie auf die Zertifikatsdetails zu: . Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann"Wählen Sie die entsprechende Zertifikatsregisterkarte aus" .

1. Überprüfen Sie die Gültigkeitsdauer des Zertifikats. + Einige Webbrowser und S3-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.
2. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein neues Zertifikat hoch oder generieren Sie ein neues.
    - Informationen zum Serverzertifikat finden Sie in den Schritten für"Konfigurieren eines

benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager" .

- Informationen zum Ein Client-Zertifikat finden Sie in den Schritten für"Konfigurieren eines Client-Zertifikats" .

3. Versuchen Sie bei Serverzertifikatsfehlern eine oder beide der folgenden Optionen:
   - Stellen Sie sicher, dass der Subject Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass der SAN mit der IP-Adresse oder dem Hostnamen des Knotens übereinstimmt, mit dem Sie eine Verbindung herstellen.
   - Wenn Sie versuchen, über einen Domänennamen eine Verbindung zu StorageGRID herzustellen:
     i. Geben Sie anstelle des Domänennamens die IP-Adresse des Admin-Knotens ein, um den Verbindungsfehler zu umgehen und auf den Grid Manager zuzugreifen.
     ii. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann"Wählen Sie die entsprechende Zertifikatsregisterkarte aus" um ein neues benutzerdefiniertes Zertifikat zu installieren oder mit dem Standardzertifikat fortzufahren.
     iii. In den Anweisungen zur Verwaltung von StorageGRID finden Sie die Schritte für"Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager" .

Beheben von Problemen mit dem Admin-Knoten und der Benutzeroberfläche

Sie können verschiedene Aufgaben ausführen, um die Ursache von Problemen im Zusammenhang mit Admin-Knoten und der StorageGRID Benutzeroberfläche zu ermitteln.

Anmeldefehler beim Admin-Knoten

Wenn bei der Anmeldung bei einem StorageGRID Admin-Knoten ein Fehler auftritt, liegt möglicherweise ein Problem mit einem"Vernetzung" oder "Hardware" Problem, ein Problem mit"Admin-Knoten-Dienste" oder ein"Problem mit der Cassandra-Datenbank" auf verbundenen Speicherknoten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die `Passwords.txt` Datei.
- Du hast"spezifische Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Verwenden Sie diese Richtlinien zur Fehlerbehebung, wenn beim Versuch, sich bei einem Admin-Knoten anzumelden, eine der folgenden Fehlermeldungen angezeigt wird:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Schritte

1. Warten Sie 10 Minuten und versuchen Sie erneut, sich anzumelden.

Wenn der Fehler nicht automatisch behoben wird, fahren Sie mit dem nächsten Schritt fort.

2. Wenn Ihr StorageGRID System über mehr als einen Admin-Knoten verfügt, versuchen Sie, sich von einem anderen Admin-Knoten aus beim Grid Manager anzumelden, um den Status eines nicht verfügbaren Admin-Knotens zu überprüfen.
   - Wenn Sie sich anmelden können, können Sie die Optionen **Dashboard**, **NODES**, **Alerts** und **SUPPORT** verwenden, um die Fehlerursache zu ermitteln.
   - Wenn Sie nur einen Admin-Knoten haben oder sich immer noch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.
3. Stellen Sie fest, ob die Hardware des Knotens offline ist.
4. Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, lesen Sie die Schritte für"Konfigurieren der einmaligen Anmeldung" .

   Möglicherweise müssen Sie SSO für einen einzelnen Admin-Knoten vorübergehend deaktivieren und erneut aktivieren, um etwaige Probleme zu beheben.

   > Wenn SSO aktiviert ist, können Sie sich nicht über einen eingeschränkten Port anmelden. Sie müssen Port 443 verwenden.

5. Stellen Sie fest, ob das von Ihnen verwendete Konto einem Verbundbenutzer gehört.

   Wenn das föderierte Benutzerkonto nicht funktioniert, versuchen Sie, sich beim Grid Manager als lokaler Benutzer, beispielsweise als Root, anzumelden.

   - Wenn sich der lokale Benutzer anmelden kann:
     i. Überprüfen Sie die Warnungen.
     ii. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Identitätsföderation**.
     iii. Klicken Sie auf **Verbindung testen**, um Ihre Verbindungseinstellungen für den LDAP-Server zu validieren.
     iv. Wenn der Test fehlschlägt, beheben Sie alle Konfigurationsfehler.
   - Wenn sich der lokale Benutzer nicht anmelden kann und Sie sicher sind, dass die Anmeldeinformationen korrekt sind, fahren Sie mit dem nächsten Schritt fort.
6. Verwenden Sie Secure Shell (ssh), um sich beim Admin-Knoten anzumelden:
   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 `#` .
7. Zeigen Sie den Status aller auf dem Grid-Knoten ausgeführten Dienste an: `storagegrid-status`

   Stellen Sie sicher, dass alle NMS-, MI-, Nginx- und Mgmt-API-Dienste ausgeführt werden.

   Die Ausgabe wird sofort aktualisiert, wenn sich der Status eines Dienstes ändert.

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. Bestätigen Sie, dass der Dienst nginx-gw ausgeführt wird `# service nginx-gw status`
9. Verwenden Sie Lumberjack, um Protokolle zu sammeln: `# /usr/local/sbin/lumberjack.rb`

   Wenn die fehlgeschlagene Authentifizierung in der Vergangenheit aufgetreten ist, können Sie die Skriptoptionen --start und --end von Lumberjack verwenden, um den entsprechenden Zeitraum anzugeben. Verwenden Sie lumberjack -h, um Einzelheiten zu diesen Optionen zu erfahren.

   Die Ausgabe an das Terminal zeigt an, wohin das Protokollarchiv kopiert wurde.

10. Überprüfen Sie die folgenden Protokolle:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`

- `**/*commands.txt`

11. Wenn Sie keine Probleme mit dem Admin-Knoten feststellen konnten, geben Sie einen der folgenden Befehle ein, um die IP-Adressen der drei Speicherknoten zu ermitteln, auf denen der ADC-Dienst an Ihrem Standort ausgeführt wird. Normalerweise sind dies die ersten drei Speicherknoten, die am Standort installiert wurden.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Admin-Knoten verwenden den ADC-Dienst während des Authentifizierungsprozesses.

12. Melden Sie sich vom Admin-Knoten aus per SSH bei jedem der ADC-Speicherknoten an, indem Sie die von Ihnen identifizierten IP-Adressen verwenden.
13. Zeigen Sie den Status aller auf dem Grid-Knoten ausgeführten Dienste an: `storagegrid-status`

    Stellen Sie sicher, dass alle Dienste idnt, acct, nginx und cassandra ausgeführt werden.

14. Schritte wiederholenVerwenden Sie Lumberjack, um Baumstämme zu sammeln UndProtokolle überprüfen um die Protokolle auf den Speicherknoten zu überprüfen.
15. Wenn Sie das Problem nicht lösen können, wenden Sie sich an den technischen Support.

    Stellen Sie dem technischen Support die gesammelten Protokolle zur Verfügung. Siehe auch "Referenz zu Protokolldateien".

Probleme mit der Benutzeroberfläche

Die Benutzeroberfläche für den Grid Manager oder den Tenant Manager reagiert nach der Aktualisierung der StorageGRID -Software möglicherweise nicht wie erwartet.

Schritte

1. Stellen Sie sicher, dass Sie ein"unterstützter Webbrowser" .
2. Leeren Sie den Cache Ihres Webbrowsers.

   Durch das Leeren des Caches werden veraltete Ressourcen entfernt, die von der vorherigen Version der StorageGRID -Software verwendet wurden, und die Benutzeroberfläche kann wieder ordnungsgemäß funktionieren. Anweisungen finden Sie in der Dokumentation Ihres Webbrowsers.

Beheben von Netzwerk-, Hardware- und Plattformproblemen

Sie können verschiedene Aufgaben ausführen, um die Ursache von Problemen im Zusammenhang mit dem StorageGRID -Netzwerk, der Hardware und der Plattform zu ermitteln.

Fehler „422: Nicht verarbeitbare Entität“

Der Fehler 422: Unprocessable Entity kann aus verschiedenen Gründen auftreten. Überprüfen Sie die Fehlermeldung, um die Ursache Ihres Problems zu ermitteln.

Wenn Sie eine der aufgeführten Fehlermeldungen sehen, ergreifen Sie die empfohlene Maßnahme.

Fehlermeldung	Grundursache und Korrekturmaßnahmen

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires`
`binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Diese Meldung kann auftreten, wenn Sie beim Konfigurieren der Identitätsföderation mit Windows Active Directory (AD) die Option **TLS nicht verwenden** für Transport Layer Security (TLS) auswählen.
	
	Die Verwendung der Option **TLS nicht verwenden** wird für die Verwendung mit AD-Servern, die eine LDAP-Signatur erzwingen, nicht unterstützt. Sie müssen entweder die Option **STARTLS verwenden** oder die Option **LDAPS verwenden** für TLS auswählen.

Fehlermeldung	Grundursache und Korrekturmaßnahmen

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Diese Meldung wird angezeigt, wenn Sie versuchen, eine nicht unterstützte Verschlüsselung zu verwenden, um eine Transport Layer Security (TLS)-Verbindung von StorageGRID zu einem externen System herzustellen, das zur Identifizierung der Föderation oder von Cloud-Speicherpools verwendet wird.
	
	Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss eines der"Von StorageGRID unterstützte Chiffren" für ausgehende TLS-Verbindungen, wie in der Anleitung zur Administration von StorageGRID beschrieben.

MTU-Nichtübereinstimmungswarnung im Netznetzwerk

Die Warnung **MTU-Fehlanpassung im Grid-Netzwerk** wird ausgelöst, wenn die Einstellung der maximalen Übertragungseinheit (MTU) für die Grid-Netzwerkschnittstelle (eth0) zwischen den Knoten im Grid erheblich abweicht.

Informationen zu diesem Vorgang

Die Unterschiede in den MTU-Einstellungen könnten darauf hinweisen, dass einige, aber nicht alle eth0-Netzwerke für Jumbo Frames konfiguriert sind. Eine Nichtübereinstimmung der MTU-Größe von mehr als 1000 kann zu Problemen mit der Netzwerkleistung führen.

Schritte

1. Listen Sie die MTU-Einstellungen für eth0 auf allen Knoten auf.
   - Verwenden Sie die im Grid Manager bereitgestellte Abfrage.
   - Navigieren Sie zu *`primary Admin Node IP address`*`/metrics/graph` und geben Sie die folgende Abfrage ein: `node_network_mtu_bytes{device="eth0"}`
2. "Ändern Sie die MTU-Einstellungen"nach Bedarf, um sicherzustellen, dass sie für die Grid-Netzwerkschnittstelle (eth0) auf allen Knoten gleich sind.
   - Verwenden Sie für Linux- und VMware-basierte Knoten den folgenden Befehl: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Beispiel: `change-ip.py -n node 1500 grid admin`

     Hinweis: Wenn auf Linux-basierten Knoten der gewünschte MTU-Wert für das Netzwerk im Container den bereits auf der Hostschnittstelle konfigurierten Wert überschreitet, müssen Sie zuerst die Hostschnittstelle so konfigurieren, dass sie den gewünschten MTU-Wert hat, und dann die `change-ip.py` Skript zum Ändern des MTU-Werts des Netzwerks im Container.

Verwenden Sie die folgenden Argumente zum Ändern der MTU auf Linux- oder VMware-basierten Knoten.

Positionsargumente	Beschreibung
`mtu`	Die einzustellende MTU. Muss im Bereich von 1280 bis 9216 liegen.
`network`	Die Netzwerke, auf die die MTU angewendet werden soll. Schließen Sie einen oder mehrere der folgenden Netzwerktypen ein: • Netz • Administrator • Kunde

+

Optionale Argumente	Beschreibung
`-h, - help`	Zeigen Sie die Hilfemeldung an und beenden Sie das Programm.
`-n node, --node node`	Der Knoten. Der Standard ist der lokale Knoten.

Knotennetzwerk-Empfangsframe-Fehlerwarnung

Fehler beim Empfang des Knotennetzwerk-Frames-Warnungen können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerkhardware verursacht werden. Diese Warnung wird von selbst gelöscht, nachdem das zugrunde liegende Problem behoben wurde.

Informationen zu diesem Vorgang

Fehler beim Empfang des Knotennetzwerk-Frames-Warnungen können durch die folgenden Probleme mit der Netzwerkhardware verursacht werden, die eine Verbindung zu StorageGRID herstellt:

- Vorwärtsfehlerkorrektur (FEC) ist erforderlich und wird nicht verwendet
- Switch-Port und NIC-MTU stimmen nicht überein
- Hohe Link-Fehlerraten
- NIC-Ringpufferüberlauf

Schritte

1. Befolgen Sie die Schritte zur Fehlerbehebung für alle möglichen Ursachen dieser Warnung in Ihrer Netzwerkkonfiguration.
2. Führen Sie je nach Fehlerursache folgende Schritte durch:

FEC-Fehlanpassung

Diese Schritte gelten nur für Warnungen vom Typ „Knotennetzwerk-Empfangsframefehler“*, die durch eine FEC-Nichtübereinstimmung auf StorageGRID -Geräten verursacht werden.

a. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID Gerät angeschlossen ist.
b. Überprüfen Sie die physische Integrität der Kabel vom Gerät zum Switch.
c. Wenn Sie die FEC-Einstellungen ändern möchten, um zu versuchen, die Warnung zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Link-Konfiguration“ des StorageGRID Appliance Installer für den Modus „**Auto**“ konfiguriert ist (siehe die Anweisungen für Ihr Gerät:
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 und SG1100"
   - "SG100 und SG1000"
d. Ändern Sie die FEC-Einstellungen an den Switch-Ports. Die Ports der StorageGRID Appliance passen ihre FEC-Einstellungen nach Möglichkeit entsprechend an.

   Sie können keine FEC-Einstellungen auf StorageGRID -Geräten konfigurieren. Stattdessen versuchen die Geräte, die FEC-Einstellungen an den Switch-Ports zu ermitteln und zu spiegeln, mit denen sie verbunden sind. Wenn die Verbindungen auf Netzwerkgeschwindigkeiten von 25 GbE oder 100 GbE gezwungen werden, können Switch und NIC möglicherweise keine gemeinsame FEC-Einstellung aushandeln. Ohne eine gemeinsame FEC-Einstellung fällt das Netzwerk in den „No-FEC“-Modus zurück. Wenn FEC nicht aktiviert ist, sind die Verbindungen anfälliger für Fehler, die durch elektrisches Rauschen verursacht werden.

   StorageGRID Geräte unterstützen Firecode (FC) und Reed Solomon (RS) FEC sowie kein FEC.

Switch-Port und NIC-MTU stimmen nicht überein

Wenn die Warnung durch eine Nichtübereinstimmung von Switch-Port und NIC-MTU verursacht wird, überprüfen Sie, ob die auf dem Knoten konfigurierte MTU-Größe mit der MTU-Einstellung für den Switch-Port übereinstimmt.

Die auf dem Knoten konfigurierte MTU-Größe ist möglicherweise kleiner als die Einstellung auf dem Switch-Port, mit dem der Knoten verbunden ist. Wenn ein StorageGRID Knoten einen Ethernet-Frame empfängt, der größer ist als seine MTU (was bei dieser Konfiguration möglich ist), wird möglicherweise die Warnung **Fehler beim Empfang des Frames im Knotennetzwerk** gemeldet. Wenn Sie glauben, dass dies der Fall ist, ändern Sie entweder die MTU des Switch-Ports, sodass sie mit der MTU der StorageGRID Netzwerkschnittstelle übereinstimmt, oder ändern Sie die MTU der StorageGRID -Netzwerkschnittstelle, sodass sie mit dem Switch-Port übereinstimmt, je nach Ihren End-to-End-MTU-Zielen oder -Anforderungen.

Für eine optimale Netzwerkleistung sollten alle Knoten mit ähnlichen MTU-Werten auf ihren Grid-Netzwerkschnittstellen konfiguriert werden. Die Warnung **MTU-Fehlanpassung des Grid-Netzwerks** wird ausgelöst, wenn es bei den MTU-Einstellungen für das Grid-Netzwerk auf einzelnen Knoten einen signifikanten Unterschied gibt. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein. Sehen Fehlerbehebung bei der Warnung „MTU-Fehlanpassung im Grid-Netzwerk“ für weitere Informationen.

Siehe auch "MTU-Einstellung ändern" .

Hohe Link-Fehlerraten

a. Aktivieren Sie FEC, falls noch nicht geschehen.
b. Stellen Sie sicher, dass Ihre Netzwerkverkabelung von guter Qualität ist und nicht beschädigt oder falsch angeschlossen ist.
c. Wenn die Kabel nicht das Problem zu sein scheinen, wenden Sie sich an den technischen Support.

In einer Umgebung mit starkem elektrischen Rauschen stellen Sie möglicherweise hohe Fehlerraten fest.

NIC-Ringpufferüberlauf

Wenn der Fehler auf einen Überlauf des NIC-Ringpuffers zurückzuführen ist, wenden Sie sich an den technischen Support.

Der Ringpuffer kann überlaufen, wenn das StorageGRID -System überlastet ist und Netzwerk-Ereignisse nicht rechtzeitig verarbeiten kann.

3. Beobachten Sie das Problem und wenden Sie sich an den technischen Support, wenn die Warnung nicht behoben wird.

Zeitsynchronisierungsfehler

Möglicherweise treten Probleme mit der Zeitsynchronisierung in Ihrem Raster auf.

Wenn bei der Zeitsynchronisierung Probleme auftreten, überprüfen Sie, ob Sie mindestens vier externe NTP-Quellen angegeben haben, die jeweils eine Stratum 3-Referenz oder besser bereitstellen, und ob alle externen NTP-Quellen normal funktionieren und von Ihren StorageGRID Knoten aus zugänglich sind.

Wann"Angabe der externen NTP-Quelle" Verwenden Sie für eine StorageGRID Installation auf Produktionsebene den Windows-Zeitdienst (W32Time) nicht auf einer Windows-Version vor Windows Server 2016. Der Zeitdienst früherer Windows-Versionen ist nicht genau genug und wird von Microsoft für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, nicht unterstützt.

Linux: Probleme mit der Netzwerkverbindung

Möglicherweise treten Probleme mit der Netzwerkkonnektivität für StorageGRID -Knoten auf, die auf Linux-Hosts gehostet werden.

Klonen von MAC-Adressen

In einigen Fällen können Netzwerkprobleme durch das Klonen von MAC-Adressen gelöst werden. Wenn Sie virtuelle Hosts verwenden, setzen Sie den Wert des MAC-Adressklonschlüssels für jedes Ihrer Netzwerke in Ihrer Knotenkonfigurationsdatei auf „true“. Diese Einstellung bewirkt, dass die MAC-Adresse des StorageGRID -Containers die MAC-Adresse des Hosts verwendet. Informationen zum Erstellen von Knotenkonfigurationsdateien finden Sie in den Anweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" .

> Erstellen Sie separate virtuelle Netzwerkschnittstellen zur Verwendung durch das Linux-Hostbetriebssystem. Die Verwendung derselben Netzwerkschnittstellen für das Linux-Hostbetriebssystem und den StorageGRID Container kann dazu führen, dass das Hostbetriebssystem nicht mehr erreichbar ist, wenn der Promiscuous-Modus auf dem Hypervisor nicht aktiviert wurde.

Weitere Informationen zum Aktivieren des MAC-Klonens finden Sie in den Anweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" .

Promiscuous-Modus

Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen das Empfangen und Senden von Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen erlauben möchten, stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppe für den Promiscuous-Modus, MAC-Adressänderungen und gefälschte Übertragungen auf **Akzeptieren** eingestellt sind. Die auf dem virtuellen Switch festgelegten Werte können durch die Werte auf Portgruppenebene überschrieben werden. Stellen Sie daher sicher, dass die Einstellungen an beiden Stellen identisch sind.

Weitere Informationen zur Verwendung des Promiscuous-Modus finden Sie in den Anweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" .

Linux: Knotenstatus ist „verwaist“

Ein Linux-Knoten in einem verwaisten Zustand weist normalerweise darauf hin, dass entweder der StorageGrid-Dienst oder der StorageGRID -Knoten-Daemon, der den Container des Knotens steuert, unerwartet beendet wurde.

Informationen zu diesem Vorgang

Wenn ein Linux-Knoten meldet, dass er sich in einem verwaisten Zustand befindet, sollten Sie:

- Überprüfen Sie die Protokolle auf Fehler und Nachrichten.
- Versuchen Sie, den Knoten erneut zu starten.
- Verwenden Sie bei Bedarf Container-Engine-Befehle, um den vorhandenen Knotencontainer zu stoppen.
- Starten Sie den Knoten neu.

Schritte

1. Überprüfen Sie die Protokolle sowohl für den Service-Daemon als auch für den verwaisten Knoten auf offensichtliche Fehler oder Meldungen über ein unerwartetes Beenden.
2. Melden Sie sich beim Host als Root oder mit einem Konto mit Sudo-Berechtigung an.
3. Versuchen Sie, den Knoten erneut zu starten, indem Sie den folgenden Befehl ausführen: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Wenn der Knoten verwaist ist, lautet die Antwort

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Stoppen Sie unter Linux die Container-Engine und alle steuernden StorageGrid-Node-Prozesse. Beispiel: `sudo docker stop --time secondscontainer-name`

   Für `seconds` Geben Sie die Anzahl der Sekunden ein, die Sie warten möchten, bis der Container stoppt (normalerweise 15 Minuten oder weniger). Beispiel:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Starten Sie den Knoten neu: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Fehlerbehebung bei der IPv6-Unterstützung

Möglicherweise müssen Sie die IPv6-Unterstützung im Kernel aktivieren, wenn Sie StorageGRID -Knoten auf Linux-Hosts installiert haben und feststellen, dass den Knotencontainern nicht wie erwartet IPv6-Adressen zugewiesen wurden.

Informationen zu diesem Vorgang

So zeigen Sie die einem Grid-Knoten zugewiesene IPv6-Adresse an:

1. Wählen Sie **NODES** und wählen Sie den Knoten aus.
2. Wählen Sie auf der Registerkarte „Übersicht“ neben „IP-Adressen“ die Option „Zusätzliche IP-Adressen anzeigen“ aus.

Wenn die IPv6-Adresse nicht angezeigt wird und der Knoten auf einem Linux-Host installiert ist, führen Sie diese Schritte aus, um die IPv6-Unterstützung im Kernel zu aktivieren.

Schritte

1. Melden Sie sich beim Host als Root oder mit einem Konto mit Sudo-Berechtigung an.
2. Führen Sie den folgenden Befehl aus: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Das Ergebnis sollte 0 sein.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

Wenn das Ergebnis nicht 0 ist, lesen Sie in der Dokumentation Ihres Betriebssystems nach, um `sysctl` Einstellungen. Ändern Sie dann den Wert auf 0, bevor Sie fortfahren.

3. Geben Sie den StorageGRID -Knotencontainer ein: `storagegrid node enter node-name`
4. Führen Sie den folgenden Befehl aus: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Das Ergebnis sollte 1 sein.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

Wenn das Ergebnis nicht 1 ist, gilt dieses Verfahren nicht. Wenden Sie sich an den technischen Support.

5. Verlassen Sie den Container: `exit`

```
root@DC1-S1:~ # exit
```

6. Bearbeiten Sie als Root die folgende Datei: `/var/lib/storagegrid/settings/sysctl.d/net.conf` .

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Suchen Sie die folgenden zwei Zeilen und entfernen Sie die Kommentar-Tags. Speichern und schließen Sie dann die Datei.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Führen Sie diese Befehle aus, um den StorageGRID Container neu zu starten:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Fehlerbehebung bei einem externen Syslog-Server

In der folgenden Tabelle werden die Fehlermeldungen beschrieben, die bei der Verwendung eines externen Syslog-Servers auftreten können, und es werden Korrekturmaßnahmen aufgelistet.

Diese Fehler werden vom Assistenten „Externen Syslog-Server konfigurieren“ angezeigt, wenn beim Senden von Testnachrichten zur Überprüfung der korrekten Konfiguration des externen Syslog-Servers Probleme auftreten.

Probleme zur Laufzeit können gemeldet werden durch"Fehler bei der Weiterleitung des externen Syslog-Servers" Alarm. Wenn Sie diese Warnung erhalten, befolgen Sie die Anweisungen in der Warnung, um die Testnachrichten erneut zu senden, damit Sie detaillierte Fehlermeldungen erhalten.

Weitere Informationen zum Senden von Audit-Informationen an einen externen Syslog-Server finden Sie unter:

- "Überlegungen zur Verwendung eines externen Syslog-Servers"
- "Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server"

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Kann den Hostnamen nicht auflösen	Der von Ihnen für den Syslog-Server eingegebene FQDN konnte nicht in eine IP-Adresse aufgelöst werden. 1. Überprüfen Sie den eingegebenen Hostnamen. Wenn Sie eine IP-Adresse eingegeben haben, stellen Sie sicher, dass es sich um eine gültige IP-Adresse in WXYZ-Notation („dotted decimal“) handelt. 2. Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind. 3. Bestätigen Sie, dass jeder Knoten auf die IP-Adressen für den DNS-Server zugreifen kann.
Verbindung abgelehnt	Eine TCP- oder TLS-Verbindung zum Syslog-Server wurde abgelehnt. Möglicherweise lauscht kein Dienst auf dem TCP- oder TLS-Port des Hosts oder eine Firewall blockiert den Zugriff. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 2. Vergewissern Sie sich, dass auf dem Host für den Syslog-Dienst ein Syslog-Daemon ausgeführt wird, der den angegebenen Port überwacht. 3. Stellen Sie sicher, dass der Zugriff auf TCP/TLS-Verbindungen von den Knoten zur IP und zum Port des Syslog-Servers nicht durch eine Firewall blockiert wird.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Netzwerk nicht erreichbar	Der Syslog-Server befindet sich nicht in einem direkt angeschlossenen Subnetz. Ein Router hat eine ICMP-Fehlermeldung zurückgegeben, um anzuzeigen, dass er die Testnachrichten von den aufgelisteten Knoten nicht an den Syslog-Server weiterleiten konnte. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Knoten die Grid-Netzwerk-Subnetzliste, die Admin-Netzwerk-Subnetzlisten und die Client-Netzwerk-Gateways. Bestätigen Sie, dass diese so konfiguriert sind, dass der Datenverkehr über die erwartete Netzwerkschnittstelle und das Gateway (Grid, Admin oder Client) an den Syslog-Server weitergeleitet wird.
Host nicht erreichbar	Der Syslog-Server befindet sich in einem direkt angeschlossenen Subnetz (Subnetz, das von den aufgelisteten Knoten für ihre Grid-, Admin- oder Client-IP-Adressen verwendet wird). Die Knoten versuchten, Testnachrichten zu senden, erhielten jedoch keine Antworten auf ARP-Anfragen für die MAC-Adresse des Syslog-Servers. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie, ob der Host, auf dem der Syslog-Dienst ausgeführt wird, aktiv ist.
Verbindungs-Timeout	Es wurde ein TCP/TLS-Verbindungsversuch unternommen, aber vom Syslog-Server wurde lange Zeit keine Antwort empfangen. Möglicherweise liegt eine Routing-Fehlkonfiguration vor oder eine Firewall blockiert den Datenverkehr, ohne eine Antwort zu senden (eine häufige Konfiguration). 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Knoten die Grid-Netzwerk-Subnetzliste, die Admin-Netzwerk-Subnetzlisten und die Client-Netzwerk-Gateways. Bestätigen Sie, dass diese so konfiguriert sind, dass der Datenverkehr über die Netzwerkschnittstelle und das Gateway (Grid, Admin oder Client) an den Syslog-Server weitergeleitet wird, über die der Syslog-Server Ihrer Meinung nach erreicht werden soll. 3. Vergewissern Sie sich, dass der Zugriff auf TCP/TLS-Verbindungen von den aufgelisteten Knoten zur IP und zum Port des Syslog-Servers nicht durch eine Firewall blockiert wird.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Verbindung vom Partner geschlossen	Eine TCP-Verbindung zum Syslog-Server wurde erfolgreich hergestellt, später jedoch geschlossen. Gründe hierfür können sein: • Der Syslog-Server wurde möglicherweise neu gestartet oder neu gebootet. • Der Knoten und der Syslog-Server haben möglicherweise unterschiedliche TCP/TLS-Einstellungen. • Eine zwischengeschaltete Firewall schließt möglicherweise inaktive TCP-Verbindungen. • Ein Nicht-Syslog-Server, der den Syslog-Server-Port überwacht, hat möglicherweise die Verbindung geschlossen. So beheben Sie dieses Problem: 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 2. Wenn Sie TLS verwenden, stellen Sie sicher, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. 3. Stellen Sie sicher, dass keine zwischengeschaltete Firewall so konfiguriert ist, dass sie inaktive TCP-Verbindungen schließt.
TLS-Zertifikatfehler	Das vom Syslog-Server empfangene Serverzertifikat war nicht mit dem von Ihnen bereitgestellten CA-Zertifikatpaket und Client-Zertifikat kompatibel. 1. Bestätigen Sie, dass das CA-Zertifikatpaket und das Client-Zertifikat (sofern vorhanden) mit dem Server-Zertifikat auf dem Syslog-Server kompatibel sind. 2. Bestätigen Sie, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Weiterleitung ausgesetzt	Syslog-Datensätze werden nicht mehr an den Syslog-Server weitergeleitet und StorageGRID kann den Grund dafür nicht erkennen. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugprotokolle, um die Grundursache zu ermitteln.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
TLS-Sitzung beendet	Der Syslog-Server hat die TLS-Sitzung beendet und StorageGRID kann den Grund nicht erkennen. 1. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugprotokolle, um die Grundursache zu ermitteln. 2. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 3. Wenn Sie TLS verwenden, stellen Sie sicher, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. 4. Bestätigen Sie, dass das CA-Zertifikatpaket und das Client-Zertifikat (sofern vorhanden) mit dem Server-Zertifikat des Syslog-Servers kompatibel sind. 5. Bestätigen Sie, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Ergebnisabfrage fehlgeschlagen	Der für die Konfiguration und das Testen des Syslog-Servers verwendete Admin-Knoten kann keine Testergebnisse von den aufgelisteten Knoten anfordern. Möglicherweise sind ein oder mehrere Knoten ausgefallen. 1. Befolgen Sie die Standardschritte zur Fehlerbehebung, um sicherzustellen, dass die Knoten online sind und alle erwarteten Dienste ausgeführt werden. 2. Starten Sie den Miscd-Dienst auf den aufgelisteten Knoten neu.

Überprüfen der Überwachungsprotokolle

Prüfmeldungen und Protokolle

Diese Anweisungen enthalten Informationen zur Struktur und zum Inhalt von StorageGRID -Auditmeldungen und Auditprotokollen. Sie können diese Informationen verwenden, um den Prüfpfad der Systemaktivität zu lesen und zu analysieren.

Diese Anweisungen richten sich an Administratoren, die für die Erstellung von Berichten zur Systemaktivität und -nutzung verantwortlich sind, die eine Analyse der Prüfmeldungen des StorageGRID -Systems erfordern.

Um die Textprotokolldatei zu verwenden, müssen Sie Zugriff auf die konfigurierte Audit-Freigabe auf dem Admin-Knoten haben.

Informationen zum Konfigurieren von Überwachungsmeldungsebenen und zur Verwendung eines externen Syslog-Servers finden Sie unter"Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Nachrichtenfluss und -aufbewahrung prüfen

Alle StorageGRID -Dienste generieren während des normalen Systembetriebs Prüfmeldungen. Sie sollten verstehen, wie diese Prüfmeldungen durch das StorageGRID -System zum `audit.log` Datei.

Nachrichtenfluss prüfen

Audit-Nachrichten werden von Admin-Knoten und von den Speicherknoten verarbeitet, die über einen Administrative Domain Controller (ADC)-Dienst verfügen.

Wie im Flussdiagramm der Audit-Nachrichten dargestellt, sendet jeder StorageGRID Knoten seine Audit-Nachrichten an einen der ADC-Dienste am Rechenzentrumsstandort. Der ADC-Dienst wird für die ersten drei an jedem Standort installierten Speicherknoten automatisch aktiviert.

Jeder ADC-Dienst fungiert wiederum als Relay und sendet seine Sammlung von Audit-Nachrichten an jeden Admin-Knoten im StorageGRID -System, wodurch jeder Admin-Knoten eine vollständige Aufzeichnung der Systemaktivität erhält.

Jeder Admin-Knoten speichert Audit-Meldungen in Text-Logdateien; die aktive Logdatei trägt den Namen `audit.log`.

Aufbewahrung von Überwachungsnachrichten

StorageGRID verwendet einen Kopier- und Löschvorgang, um sicherzustellen, dass keine Prüfmeldungen verloren gehen, bevor sie in das Prüfprotokoll geschrieben werden können.

Wenn ein Knoten eine Prüfnachricht generiert oder weiterleitet, wird die Nachricht in einer Prüfnachrichtenwarteschlange auf der Systemfestplatte des Grid-Knotens gespeichert. Eine Kopie der Nachricht wird immer in einer Audit-Nachrichtenwarteschlange aufbewahrt, bis die Nachricht in die Audit-Protokolldatei im Admin-Knoten geschrieben wird. `/var/local/log` Verzeichnis. Dadurch wird verhindert, dass während des Transports eine Prüfnachricht verloren geht.

Die Warteschlange der Prüfnachrichten kann aufgrund von Netzwerkverbindungsproblemen oder unzureichender Prüfkapazität vorübergehend größer werden. Wenn die Warteschlangen größer werden, verbrauchen sie mehr verfügbaren Speicherplatz in den einzelnen Knoten. `/var/local/` Verzeichnis. Wenn das Problem weiterhin besteht und das Prüfnachrichtenverzeichnis eines Knotens zu voll wird, priorisieren die einzelnen Knoten die Verarbeitung ihres Rückstands und sind vorübergehend für neue Nachrichten nicht verfügbar.

Insbesondere können die folgenden Verhaltensweisen auftreten:

- Wenn die `/var/local/log` Wenn das von einem Admin-Knoten verwendete Verzeichnis voll ist, wird der Admin-Knoten als für neue Prüfmeldungen nicht verfügbar gekennzeichnet, bis das Verzeichnis nicht mehr voll ist. S3-Client-Anfragen sind nicht betroffen. Der XAMS-Alarm (Unreachable Audit Repositories) wird ausgelöst, wenn ein Audit-Repository nicht erreichbar ist.
- Wenn die `/var/local/` Wenn das von einem Speicherknoten mit dem ADC-Dienst verwendete Verzeichnis zu 92 % gefüllt ist, wird der Knoten als für Prüfmeldungen nicht verfügbar gekennzeichnet, bis das Verzeichnis nur noch zu 87 % gefüllt ist. S3-Client-Anfragen an andere Knoten sind nicht betroffen. Der NRLY-Alarm (Available Audit Relays) wird ausgelöst, wenn Audit-Relays nicht erreichbar sind.

  > Wenn keine Storage Nodes mit dem ADC-Dienst verfügbar sind, speichern die Storage Nodes die Audit-Nachrichten lokal im `/var/local/log/localaudit.log` Datei.

- Wenn die `/var/local/` Das von einem Speicherknoten verwendete Verzeichnis ist zu 85 % gefüllt. Der Knoten lehnt S3-Client-Anfragen mit `503 Service Unavailable`.

Die folgenden Arten von Problemen können dazu führen, dass die Warteschlangen für

Überwachungsnachrichten sehr groß werden:

- Der Ausfall eines Admin-Knotens oder eines Speicherknotens mit dem ADC-Dienst. Wenn einer der Systemknoten ausfällt, kann es bei den übrigen Knoten zu einem Rückstau kommen.
- Eine anhaltende Aktivitätsrate, die die Prüfkapazität des Systems übersteigt.
- Der `/var/local/` Der Speicherplatz auf einem ADC-Speicherknoten wird aus Gründen voll, die nichts mit Prüfmeldungen zu tun haben. In diesem Fall akzeptiert der Knoten keine neuen Prüfnachrichten mehr und priorisiert seinen aktuellen Rückstand, was zu Rückständen auf anderen Knoten führen kann.

Alarm bei großer Audit-Warteschlange und Alarm bei in die Warteschlange gestellten Audit-Nachrichten (AMQS)

Damit Sie die Größe der Warteschlangen für Prüfnachrichten im Laufe der Zeit überwachen können, werden die Warnung „Große Prüfwarteschlange“ und der alte AMQS-Alarm ausgelöst, wenn die Anzahl der Nachrichten in einer Speicherknotenwarteschlange oder einer Admin-Knotenwarteschlange bestimmte Schwellenwerte erreicht.

Wenn die Warnung **Große Prüfwarteschlange** oder der alte AMQS-Alarm ausgelöst wird, überprüfen Sie zunächst die Systemlast. Wenn in letzter Zeit eine erhebliche Anzahl von Transaktionen stattgefunden hat, sollten sich die Warnung und der Alarm mit der Zeit auflösen und können ignoriert werden.

Wenn die Warnung oder der Alarm weiterhin besteht und an Schwere zunimmt, sehen Sie sich ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage hinweg stetig ansteigt, hat die Prüflast wahrscheinlich die Prüfkapazität des Systems überschritten. Reduzieren Sie die Client-Betriebsrate oder verringern Sie die Anzahl der protokollierten Prüfmeldungen, indem Sie die Prüfstufe für Client-Schreibvorgänge und Client-Lesevorgänge auf „Fehler“ oder „Aus“ ändern. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Doppelte Nachrichten

Das StorageGRID -System verfolgt einen konservativen Ansatz, wenn ein Netzwerk- oder Knotenausfall auftritt. Aus diesem Grund können im Überwachungsprotokoll doppelte Nachrichten vorhanden sein.

Zugriff auf die Überwachungsprotokolldatei

Der Audit-Share enthält die aktiven `audit.log` Datei und alle komprimierten Prüfprotokolldateien. Sie können direkt über die Befehlszeile des Admin-Knotens auf die Audit-Protokolldateien zugreifen.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die `Passwords.txt` Datei.
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Schritte

1. Melden Sie sich bei einem 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. Wechseln Sie zum Verzeichnis mit den Audit-Protokolldateien:

```
cd /var/local/log
```

3. Zeigen Sie bei Bedarf die aktuelle oder eine gespeicherte Überwachungsprotokolldatei an.

Rotation der Überwachungsprotokolldateien

Audit-Protokolldateien werden auf einem Admin-Knoten gespeichert `/var/local/log` Verzeichnis. Die aktiven Audit-Protokolldateien heißen `audit.log` .

> Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Einmal täglich wird der aktive `audit.log` Datei wird gespeichert und eine neue `audit.log` Datei wird gestartet. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format *`yyyy-mm-dd.txt`* . Wenn an einem Tag mehr als ein Prüfprotokoll erstellt wird, verwenden die Dateinamen das Datum, an dem die Datei gespeichert wurde, gefolgt von einer Zahl im Format *`yyyy-mm-dd.txt.n`* . Zum Beispiel, `2018-04-15.txt` Und `2018-04-15.txt.1` sind die erste und zweite Protokolldatei, die am 15. April 2018 erstellt und gespeichert wurden.

Nach einem Tag wird die gespeicherte Datei komprimiert und umbenannt, im Format *`yyyy-mm-dd.txt.gz`* , wodurch das ursprüngliche Datum erhalten bleibt. Im Laufe der Zeit führt dies dazu, dass der für Prüfprotokolle auf dem Admin-Knoten zugewiesene Speicherplatz verbraucht wird. Ein Skript überwacht den Speicherplatzverbrauch des Audit-Protokolls und löscht Protokolldateien nach Bedarf, um Speicherplatz im `/var/local/log` Verzeichnis. Prüfprotokolle werden basierend auf dem Datum ihrer Erstellung gelöscht, wobei die ältesten zuerst gelöscht werden. Sie können die Aktionen des Skripts in der folgenden Datei überwachen: `/var/local/log/manage-audit.log` .

Dieses Beispiel zeigt die aktive `audit.log` Datei, die Datei vom Vortag(`2018-04-15.txt`) und die komprimierte Datei für den Vortag(`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Audit-Protokolldateiformat

Audit-Protokolldateiformat

Die Audit-Protokolldateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Meldungen.

Jede Prüfnachricht enthält Folgendes:

- Die koordinierte Weltzeit (UTC) des Ereignisses, das die Prüfnachricht ausgelöst hat (ATIM) im ISO 8601-Format, gefolgt von einem Leerzeichen:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, Wo *UUUUUU* sind Mikrosekunden.

- Die Prüfnachricht selbst, eingeschlossen in eckige Klammern und beginnend mit `AUDT` .

Das folgende Beispiel zeigt drei Audit-Meldungen in einer Audit-Protokolldatei (Zeilenumbrüche zur besseren Lesbarkeit hinzugefügt). Diese Nachrichten wurden generiert, als ein Mandant einen S3-Bucket erstellte und diesem Bucket zwei Objekte hinzufügte.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

In ihrem Standardformat sind die Prüfmeldungen in den Prüfprotokolldateien nicht einfach zu lesen oder zu interpretieren. Sie können die"Audit-Erklärtool" um vereinfachte Zusammenfassungen der Audit-Meldungen im Audit-Protokoll zu erhalten. Sie können die"Auditsummen-Tool" um zusammenzufassen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge dauerten.

Verwenden Sie das Audit-Explain-Tool

Sie können die `audit-explain` Tool zum Übersetzen der Audit-Meldungen im Audit-Protokoll in ein leicht lesbares Format.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die `Passwords.txt` Datei.
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Informationen zu diesem Vorgang

Der `audit-explain` Das auf dem primären Admin-Knoten verfügbare Tool bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Audit-Protokoll.

> Der `audit-explain` Das Tool ist in erster Linie für die Verwendung durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitung `audit-explain` Abfragen können eine große Menge an CPU-Leistung verbrauchen, was sich auf den Betrieb von StorageGRID auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-explain` Werkzeug. Diese vier"SPUT" Es wurden Prüfmeldungen generiert, als der S3-Mandant mit der Konto-ID 92484777680322627870 S3-PUT-Anfragen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und diesem Bucket drei Objekte hinzuzufügen.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Der `audit-explain` Das Tool kann Folgendes:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Verarbeiten Sie mehrere Dateien gleichzeitig. Beispiel:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- Akzeptieren Sie Eingaben von einer Pipe, die es Ihnen ermöglicht, die Eingabe mithilfe der `grep` Befehl oder andere Mittel. Beispiel:

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Da Audit-Protokolle sehr groß und langsam zu analysieren sein können, können Sie Zeit sparen, indem Sie Teile filtern, die Sie ansehen möchten, und ausführen `audit-explain` auf die Teile, statt auf die gesamte Datei.

> Der `audit-explain` Das Tool akzeptiert keine komprimierten Dateien als Pipe-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie deren Dateinamen als Befehlszeilenargumente an oder verwenden Sie die `zcat` Tool, um die Dateien zuerst zu dekomprimieren. Beispiel:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Verwenden Sie die `help (-h)` Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-explain -h
```

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. Geben Sie den folgenden Befehl ein, wobei `/var/local/log/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   Der `audit-explain` Das Tool druckt für Menschen lesbare Interpretationen aller Nachrichten in der bzw. den angegebenen Dateien.

   > Um die Zeilenlänge zu reduzieren und die Lesbarkeit zu verbessern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel sehen möchten, verwenden Sie den Zeitstempel(`-t`) Option.

Verwenden Sie das Audit-Sum-Tool

Sie können die `audit-sum` Tool zum Zählen der Prüfnachrichten zum Schreiben, Lesen, Kopfzeilen und Löschen und zum Anzeigen der minimalen, maximalen und durchschnittlichen Zeit (oder Größe) für jeden Vorgangstyp.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die `Passwords.txt` Datei.
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Informationen zu diesem Vorgang

Der `audit-sum` Das auf dem primären Admin-Knoten verfügbare Tool fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

> Der `audit-sum` Das Tool ist in erster Linie für die Verwendung durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitung `audit-sum` Abfragen können eine große Menge an CPU-Leistung verbrauchen, was sich auf den Betrieb von StorageGRID auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerten.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Der `audit-sum` Das Tool stellt Anzahl und Zeit für die folgenden S3-, Swift- und ILM-Auditmeldungen in einem Audit-Protokoll bereit.

> Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, wenn Funktionen veraltet sind. Wenn Sie auf einen Prüfcode stoßen, der hier nicht aufgeführt ist, überprüfen Sie die vorherigen Versionen dieses Themas auf ältere SG-Versionen. Beispiel: "StorageGRID 11.8 Dokumentation zum Verwenden des Auditsummentools" .

Code	Beschreibung	Siehe
IDEL	Von ILM initiiertes Löschen: Protokolliert, wenn ILM den Löschvorgang eines Objekts startet.	"IDEL: Von ILM initiiertes Löschen"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	"SDEL: S3 LÖSCHEN"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Buckets zu überprüfen.	"SHEA: S3 KOPF"

Code	Beschreibung	Siehe
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	"WDEL: Schnelles LÖSCHEN"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Container.	"WGET: Schnelles GET"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Containers zu überprüfen.	"WHEA: Schneller Kopf"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Containers.	"WPUT: Schnelles PUT"

Der `audit-sum` Das Tool kann Folgendes:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Verarbeiten Sie mehrere Dateien gleichzeitig. Beispiel:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- Akzeptieren Sie Eingaben von einer Pipe, die es Ihnen ermöglicht, die Eingabe mithilfe der `grep` Befehl oder andere Mittel. Beispiel:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> Dieses Tool akzeptiert keine komprimierten Dateien als Pipe-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie deren Dateinamen als Befehlszeilenargumente an oder verwenden Sie die `zcat` Tool, um die Dateien zuerst zu dekomprimieren. Beispiel:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Sie können Befehlszeilenoptionen verwenden, um Vorgänge für Buckets getrennt von Vorgängen für Objekte

zusammenzufassen oder um Meldungszusammenfassungen nach Bucket-Name, Zeitraum oder Zieltyp zu gruppieren. Standardmäßig zeigen die Zusammenfassungen die minimale, maximale und durchschnittliche Betriebszeit an, Sie können jedoch die `size (-s)` Option, stattdessen die Objektgröße zu betrachten.

Verwenden Sie die `help (-h)` Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-sum -h
```

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. Wenn Sie alle Nachrichten im Zusammenhang mit Schreib-, Lese-, Head- und Löschvorgängen analysieren möchten, führen Sie die folgenden Schritte aus:
   a. Geben Sie den folgenden Befehl ein, wobei `/var/local/log/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerten.

      ```
        message group           count     min(sec)        max(sec)
      average(sec)
        =============           =====     ========        ========
      ============
        IDEL                      274
        SDEL                   213371        0.004          20.934
      0.352
        SGET                   201906        0.010        1740.290
      1.132
        SHEA                    22716        0.005           2.349
      0.272
        SPUT                 1771398        0.011        1770.563
      0.487
      ```

      In diesem Beispiel sind SGET-Operationen (S3 GET) mit durchschnittlich 1,13 Sekunden am langsamsten, aber SGET- und SPUT-Operationen (S3 PUT) weisen beide lange Worst-Case-Zeiten von etwa 1.770 Sekunden auf.

   b. Um die 10 langsamsten Abrufvorgänge anzuzeigen, verwenden Sie den Befehl grep, um nur SGET-Nachrichten auszuwählen und die Option für die lange Ausgabe hinzuzufügen(`-l`), um Objektpfade

einzuschließen:

```
grep SGET audit.log | audit-sum -l
```

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, sodass Sie das Prüfprotokoll nach anderen Nachrichten durchsuchen können, die sich auf diese bestimmten Objekte beziehen.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
Anhand dieser Beispielausgabe können Sie erkennen, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von etwa 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe ist für die langsamen Abrufzeiten im schlimmsten Fall verantwortlich.

3. Wenn Sie bestimmen möchten, welche Objektgrößen in Ihr Raster aufgenommen und daraus abgerufen werden, verwenden Sie die Größenoption(`-s`):

```
audit-sum -s audit.log
```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

In diesem Beispiel liegt die durchschnittliche Objektgröße für SPUT unter 2,5 MB, die durchschnittliche Größe für SGET ist jedoch viel größer. Die Anzahl der SPUT-Nachrichten ist viel höher als die Anzahl der SGET-Nachrichten, was darauf hindeutet, dass die meisten Objekte nie abgerufen werden.

4. Wenn Sie feststellen möchten, ob die Abrufe gestern langsam waren:

   a. Führen Sie den Befehl für das entsprechende Überwachungsprotokoll aus und verwenden Sie die Option „Nach Zeit gruppieren“.(`-gt`), gefolgt vom Zeitraum (z. B. 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Diese Ergebnisse zeigen, dass der S3 GET-Verkehr zwischen 06:00 und 07:00 Uhr seinen Höhepunkt erreichte. Auch die Höchst- und Durchschnittszeiten sind zu diesen Zeiten erheblich höher und steigen nicht allmählich an, wenn die Anzahl steigt. Dies deutet darauf hin, dass irgendwo die Kapazität überschritten wurde, vielleicht im Netzwerk oder bei der Fähigkeit des Grids, Anfragen zu verarbeiten.

b. Um zu ermitteln, welche Objektgröße gestern stündlich abgerufen wurde, fügen Sie die Option „Größe“ hinzu(`-s`) zum Befehl:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Diese Ergebnisse deuten darauf hin, dass einige sehr große Abrufe stattfanden, als der gesamte Abrufverkehr seinen Höhepunkt erreichte.

c. Um weitere Details anzuzeigen, verwenden Sie die"Audit-Erklärtool" um alle SGET-Operationen während dieser Stunde zu überprüfen:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Wenn die Ausgabe des grep-Befehls voraussichtlich viele Zeilen umfasst, fügen Sie die `less` Befehl, um den Inhalt der Prüfprotokolldatei seitenweise (bildschirmweise) anzuzeigen.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen für Buckets langsamer sind als SPUT-Operationen für Objekte:

a. Beginnen Sie mit der `-go` Option, die Nachrichten für Objekt- und Bucket-Operationen separat gruppiert:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets andere Leistungsmerkmale aufweisen als SPUT-Operationen für Objekte.

b. Um zu ermitteln, welche Buckets die langsamsten SPUT-Operationen haben, verwenden Sie die `-gb` Option, die Nachrichten nach Bucket gruppiert:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Um zu bestimmen, welche Buckets die größte SPUT-Objektgröße haben, verwenden Sie sowohl die `-gb` und die `-s` Optionen:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Format der Prüfnachricht

Format der Prüfnachricht

Die innerhalb des StorageGRID -Systems ausgetauschten Prüfnachrichten enthalten für alle Nachrichten gemeinsame Standardinformationen und spezifische Inhalte, die das gemeldete Ereignis oder die gemeldete Aktivität beschreiben.

Wenn die zusammenfassenden Informationen der"Audit-Erklärung" Und"Auditsumme" Wenn die Tools nicht ausreichen, lesen Sie diesen Abschnitt, um das allgemeine Format aller Prüfmeldungen zu verstehen.

Nachfolgend sehen Sie ein Beispiel für eine Audit-Meldung, wie sie in der Audit-Protokolldatei erscheinen könnte:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Jede Prüfnachricht enthält eine Zeichenfolge von Attributelementen. Die gesamte Zeichenfolge ist in Klammern eingeschlossen(`[ ]`), und jedes Attributelement in der Zeichenfolge weist die folgenden Eigenschaften auf:

- In Klammern eingeschlossen `[ ]`
- Eingeführt durch die Zeichenfolge `AUDT` , was auf eine Prüfmeldung hinweist
- Ohne Trennzeichen (keine Kommas oder Leerzeichen) davor oder danach
- Beendet durch ein Zeilenvorschubzeichen `\n`

Jedes Element enthält einen Attributcode, einen Datentyp und einen Wert, die in diesem Format gemeldet werden:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Die Anzahl der Attributelemente in der Nachricht hängt vom Ereignistyp der Nachricht ab. Die Attributelemente sind in keiner bestimmten Reihenfolge aufgelistet.

Die folgende Liste beschreibt die Attributelemente:

- `ATTR`ist ein vierstelliger Code für das gemeldete Attribut. Es gibt einige Attribute, die allen Prüfmeldungen gemeinsam sind, und andere, die ereignisspezifisch sind.
- `type`ist eine vierstellige Kennung des Programmierdatentyps des Werts, z. B. UI64, FC32 usw. Der Typ ist in Klammern eingeschlossen `( ).
- `value`ist der Inhalt des Attributs, normalerweise ein numerischer oder Textwert. Auf Werte folgt immer ein Doppelpunkt(:`). Werte des Datentyps CSTR sind in doppelte Anführungszeichen " " eingeschlossen.

Datentypen

Zum Speichern von Informationen in Prüfmeldungen werden unterschiedliche Datentypen verwendet.

Typ	Beschreibung
UI32	Vorzeichenloser Long Integer (32 Bit); kann die Zahlen 0 bis 4.294.967.295 speichern.
UI64	Vorzeichenloser Double Long Integer (64 Bit); kann die Zahlen 0 bis 18.446.744.073.709.551.615 speichern.
FC32	Vierstellige Konstante; ein 32-Bit-Ganzzahlwert ohne Vorzeichen, der als vier ASCII-Zeichen dargestellt wird, z. B. „ABCD“.
IPAD	Wird für IP-Adressen verwendet.
CSTR	Ein Array mit variabler Länge aus UTF-8-Zeichen. Zeichen können mit den folgenden Konventionen maskiert werden: • Der Backslash ist \\. • Der Wagenrücklauf ist \r. • Doppelte Anführungszeichen sind \". • Zeilenvorschub (neue Zeile) ist \n. • Zeichen können durch ihre hexadezimalen Entsprechungen ersetzt werden (im Format \xHH, wobei HH der Hexadezimalwert ist, der das Zeichen darstellt).

Ereignisspezifische Daten

Jede Prüfmeldung im Prüfprotokoll zeichnet Daten auf, die für ein Systemereignis

spezifisch sind.

Im Anschluss an die Eröffnung `[AUDT:` Container, der die Nachricht selbst identifiziert, der nächste Satz von Attributen liefert Informationen über das Ereignis oder die Aktion, die in der Prüfnachricht beschrieben wird. Diese Attribute werden im folgenden Beispiel hervorgehoben:

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"Konto"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJ
A=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"Konto"\]\[S3BK\(CSTR\):"Bucket"\]
\[S3KY\(CSTR\):"Objekt"\]\[CBID\(UI64\):0xCC128B9B9E428347\] \[UUID\(CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

Der `ATYP` Das Element (im Beispiel unterstrichen) identifiziert, welches Ereignis die Nachricht generiert hat. Diese Beispielnachricht enthält die"SHEA" Nachrichtencode ([ATYP(FC32):SHEA]), der angibt, dass er durch eine erfolgreiche S3-HEAD-Anforderung generiert wurde.

Gemeinsame Elemente in Prüfmeldungen

Alle Prüfmeldungen enthalten die gemeinsamen Elemente.

Code	Typ	Beschreibung
INMITTEN	FC32	Modul-ID: Eine vierstellige Kennung der Modul-ID, die die Nachricht generiert hat. Dies gibt das Codesegment an, innerhalb dessen die Prüfnachricht generiert wurde.
ANID	UI32	Knoten-ID: Die dem Dienst zugewiesene Grid-Knoten-ID, der die Nachricht generiert hat. Jedem Dienst wird bei der Konfiguration und Installation des StorageGRID -Systems eine eindeutige Kennung zugewiesen. Diese ID kann nicht geändert werden.
ASES	UI64	Audit-Sitzungskennung: In früheren Versionen gab dieses Element den Zeitpunkt an, zu dem das Audit-System nach dem Start des Dienstes initialisiert wurde. Dieser Zeitwert wurde in Mikrosekunden seit der Betriebssystem-Epoche (00:00:00 UTC am 1. Januar 1970) gemessen. **Hinweis:** Dieses Element ist veraltet und erscheint nicht mehr in Prüfmeldungen.
ASQN	UI64	Sequenzzähler: In früheren Versionen wurde dieser Zähler für jede generierte Prüfnachricht auf dem Grid-Knoten (ANID) erhöht und beim Neustart des Dienstes auf Null zurückgesetzt. **Hinweis:** Dieses Element ist veraltet und erscheint nicht mehr in Prüfmeldungen.

Code	Typ	Beschreibung
ATID	UI64	Trace-ID: Eine Kennung, die von allen Nachrichten gemeinsam genutzt wird, die durch ein einzelnes Ereignis ausgelöst wurden.
ATIM	UI64	Zeitstempel: Der Zeitpunkt, zu dem das Ereignis generiert wurde, das die Prüfnachricht ausgelöst hat, gemessen in Mikrosekunden seit der Betriebssystem-Epoche (00:00:00 UTC am 1. Januar 1970). Beachten Sie, dass die meisten verfügbaren Tools zum Konvertieren des Zeitstempels in lokales Datum und Uhrzeit auf Millisekunden basieren. Möglicherweise ist eine Rundung oder Kürzung des protokollierten Zeitstempels erforderlich. Die menschenlesbare Zeit, die am Anfang der Audit-Meldung im `audit.log` Datei ist das ATIM-Attribut im ISO 8601-Format. Datum und Uhrzeit werden dargestellt als *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , wobei die `T` ist ein Zeichenfolgenzeichen, das den Beginn des Zeitsegments des Datums angibt. *`UUUUUU`* sind Mikrosekunden.
ATYP	FC32	Ereignistyp: Eine vierstellige Kennung des protokollierten Ereignisses. Dies bestimmt den „Nutzlast“-Inhalt der Nachricht: die enthaltenen Attribute.
BEHAUPTEN	UI32	Version: Die Version der Prüfnachricht. Im Zuge der Weiterentwicklung der StorageGRID -Software können neue Versionen von Diensten neue Funktionen für die Prüfberichterstattung enthalten. Dieses Feld ermöglicht die Abwärtskompatibilität im AMS-Dienst, um Nachrichten aus älteren Dienstversionen zu verarbeiten.
RSLT	FC32	Ergebnis: Das Ergebnis eines Ereignisses, Prozesses oder einer Transaktion. Wenn es für eine Nachricht nicht relevant ist, wird NONE statt SUCS verwendet, damit die Nachricht nicht versehentlich gefiltert wird.

Beispiele für Prüfnachrichten

Detaillierte Informationen finden Sie in jeder Prüfmeldung. Alle Prüfmeldungen verwenden dasselbe Format.

Nachfolgend sehen Sie ein Beispiel für eine Prüfmeldung, wie sie in der `audit.log` Datei:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Die Prüfnachricht enthält Informationen zum aufgezeichneten Ereignis sowie Informationen zur Prüfnachricht selbst.

Um zu ermitteln, welches Ereignis von der Prüfnachricht aufgezeichnet wird, suchen Sie nach dem ATYP-Attribut (unten hervorgehoben):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Der Wert des ATYP-Attributs ist SPUT. "SPUT" stellt eine S3 PUT-Transaktion dar, die die Aufnahme eines Objekts in einen Bucket protokolliert.

Die folgende Prüfmeldung zeigt auch den Bucket an, mit dem das Objekt verknüpft ist:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Um herauszufinden, wann das PUT-Ereignis aufgetreten ist, notieren Sie sich den Zeitstempel „Universal Coordinated Time“ (UTC) am Anfang der Prüfnachricht. Dieser Wert ist eine für Menschen lesbare Version des ATIM-Attributs der Prüfnachricht selbst:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM zeichnet die Zeit in Mikrosekunden seit Beginn der UNIX-Epoche auf. Im Beispiel ist der Wert `1405631878959669` entspricht Donnerstag, 17. Juli 2014, 21:17:59 UTC.

Prüfmeldungen und der Objektlebenszyklus

Wann werden Prüfmeldungen generiert?

Jedes Mal, wenn ein Objekt aufgenommen, abgerufen oder gelöscht wird, werden Prüfmeldungen generiert. Sie können diese Transaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

Die Verknüpfung der Prüfmeldungen erfolgt über protokollspezifische Kennungen.

Protokoll	Code
Verknüpfen von S3-Operationen	S3BK (Bucket), S3KY (Schlüssel) oder beides
Verknüpfen von Swift-Operationen	WCON (Container), WOBJ (Objekt) oder beides
Verknüpfung interner Vorgänge	CBID (interne Kennung des Objekts)

Zeitpunkt der Prüfmeldungen

Aufgrund von Faktoren wie Zeitunterschieden zwischen Grid-Knoten, Objektgröße und Netzwerkverzögerungen kann die Reihenfolge der von den verschiedenen Diensten generierten Prüfmeldungen von der in den Beispielen in diesem Abschnitt gezeigten abweichen.

Objektaufnahmetransaktionen

Sie können Client-Ingest-Transaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

In den folgenden Tabellen sind nicht alle während einer Aufnahmetransaktion generierten Prüfmeldungen aufgeführt. Es sind nur die Nachrichten enthalten, die zum Verfolgen der Aufnahmetransaktion erforderlich sind.

S3-Ingest-Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
SPUT	S3 PUT-Transaktion	Eine S3 PUT-Ingest-Transaktion wurde erfolgreich abgeschlossen.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Objektregeln erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Swift erfasst Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
WPUT	Schnelle PUT-Transaktion	Eine Swift PUT-Ingest-Transaktion wurde erfolgreich abgeschlossen.	CBID, WCON, WOBJ	"WPUT: Schnelles PUT"
ORLM	Objektregeln erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Beispiel: S3-Objektaufnahme

Die folgende Reihe von Prüfmeldungen ist ein Beispiel für die Prüfmeldungen, die generiert und im Prüfprotokoll gespeichert werden, wenn ein S3-Client ein Objekt in einen Speicherknoten (LDR-Dienst) einspeist.

In diesem Beispiel enthält die aktive ILM-Richtlinie die ILM-Regel „2 Kopien erstellen“.

> Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Prüfmeldungen aufgeführt. Es werden nur diejenigen aufgelistet, die sich auf die S3-Ingest-Transaktion (SPUT) beziehen.

In diesem Beispiel wird davon ausgegangen, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Nachricht wird generiert, um anzuzeigen, dass eine S3 PUT-Transaktion ausgegeben wurde, um ein Objekt in einem bestimmten Bucket zu erstellen.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Objektregeln erfüllt

Die ORLM-Nachricht gibt an, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Nachricht enthält die CBID des Objekts und den Namen der angewendeten ILM-Regel.

Bei replizierten Objekten enthält das LOCS-Feld die LDR-Knoten-ID und die Volume-ID der Objektstandorte.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Bei Erasure-Coding-Objekten enthält das LOCS-Feld die Erasure-Coding-Profil-ID und die Erasure-Coding-Gruppen-ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Das PATH-Feld enthält S3-Bucket- und Schlüsselinformationen oder Swift-Container- und Objektinformationen, je nachdem, welche API verwendet wurde.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Objektlöschtransaktionen

Sie können Objektlöschtransaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

In den folgenden Tabellen sind nicht alle während einer Löschtransaktion generierten Prüfmeldungen

aufgeführt. Es sind nur Nachrichten enthalten, die zum Verfolgen der Löschtransaktion erforderlich sind.

S3-Lösch-Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	Es wurde eine Anforderung zum Löschen des Objekts aus einem Bucket gestellt.	CBID, S3KY	"SDEL: S3 LÖSCHEN"

Schnelles Löschen von Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
WDEL	Schnelles Löschen	Es wurde eine Anforderung zum Löschen des Objekts aus einem Container oder dem Container gestellt.	CBID, WOBJ	"WDEL: Schnelles LÖSCHEN"

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt von einem Speicherknoten (LDR-Dienst) löscht, wird eine Prüfnachricht generiert und im Prüfprotokoll gespeichert.

> Im folgenden Beispiel sind nicht alle während einer Löschtransaktion generierten Prüfmeldungen aufgeführt. Es werden nur diejenigen aufgelistet, die sich auf die S3-Löschtransaktion (SDEL) beziehen.

SDEL: S3 Löschen

Das Löschen von Objekten beginnt, wenn der Client eine DeleteObject-Anforderung an einen LDR-Dienst sendet. Die Nachricht enthält den Bucket, aus dem das Objekt gelöscht werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Objektabruftransaktionen

Sie können Objektabruftransaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

In den folgenden Tabellen sind nicht alle Prüfmeldungen aufgeführt, die während einer Abruftransaktion generiert werden. Es sind nur Nachrichten enthalten, die zum Verfolgen der Abruftransaktion erforderlich sind.

S3-Abruf-Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 GET	Anforderung zum Abrufen eines Objekts aus einem Bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Audit-Nachrichten zum schnellen Abrufen

Code	Name	Beschreibung	Verfolgen	Siehe
WGET	Schnelles GET	Anforderung zum Abrufen eines Objekts aus einem Container.	CBID, WCON, WOBJ	"WGET: Schnelles GET"

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Speicherknoten (LDR-Dienst) abruft, wird eine Prüfnachricht generiert und im Prüfprotokoll gespeichert.

Beachten Sie, dass im folgenden Beispiel nicht alle während einer Transaktion generierten Prüfmeldungen aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET: S3 GET

Der Objektabruf beginnt, wenn der Client eine GetObject-Anforderung an einen LDR-Dienst sendet. Die Nachricht enthält den Bucket, aus dem das Objekt abgerufen werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Wenn die Bucket-Richtlinie dies zulässt, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört. Die Prüfnachricht enthält Informationen zum Mandantenkonto des Bucket-Eigentümers, sodass Sie diese anonymen und kontoübergreifenden Anfragen verfolgen können.

In der folgenden Beispielnachricht sendet der Client eine GetObject-Anforderung für ein Objekt, das in einem Bucket gespeichert ist, das ihm nicht gehört. Die Werte für SBAI und SBAC zeichnen die Mandantenkonto-ID

und den Namen des Bucket-Eigentümers auf, die sich von der Mandantenkonto-ID und dem Namen des in S3AI und SACC aufgezeichneten Kunden unterscheiden.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Beispiel: S3 Select auf einem Objekt

Wenn ein S3-Client eine S3 Select-Abfrage für ein Objekt ausgibt, werden Prüfmeldungen generiert und im Prüfprotokoll gespeichert.

Beachten Sie, dass im folgenden Beispiel nicht alle während einer Transaktion generierten Prüfmeldungen aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3 Select-Transaktion (SelectObjectContent) beziehen.

Jede Abfrage führt zu zwei Prüfmeldungen: eine, die die Autorisierung der S3 Select-Anfrage durchführt (das S3SR-Feld ist auf „select“ gesetzt) und eine nachfolgende Standard-GET-Operation, die die Daten während der Verarbeitung aus dem Speicher abruft.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Metadaten-Update-Nachrichten

Audit-Nachrichten werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

Audit-Meldungen zur S3-Metadatenaktualisierung

Code	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3-Metadaten aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert.	CBID, S3KY, HTRH	"SUPD: S3-Metadaten aktualisiert"

Beispiel: S3-Metadaten-Update

Das Beispiel zeigt eine erfolgreiche Transaktion zum Aktualisieren der Metadaten für ein vorhandenes S3-Objekt.

SUPD: S3-Metadaten-Update

Der S3-Client stellt eine Anfrage (SUPD), um die angegebenen Metadaten zu aktualisieren(`x-amz-meta-\*`) für das S3-Objekt (S3KY). In diesem Beispiel sind Anforderungsheader im Feld HTRH enthalten, da es als Audit-Protokollheader konfiguriert wurde (**KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**). Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Prüfmeldungen

Beschreibungen der Prüfnachrichten

Detaillierte Beschreibungen der vom System zurückgegebenen Prüfmeldungen finden Sie in den folgenden Abschnitten. Jede Prüfnachricht wird zunächst in einer Tabelle aufgelistet, in der verwandte Nachrichten nach der Aktivitätsklasse gruppiert werden, die die Nachricht darstellt. Diese Gruppierungen sind sowohl für das Verständnis der überwachten Aktivitätstypen als auch für die Auswahl des gewünschten Typs der Überwachungsnachrichtenfilterung nützlich.

Die Prüfmeldungen werden außerdem alphabetisch nach ihren vierstelligen Codes aufgelistet. Diese alphabetische Liste ermöglicht es Ihnen, Informationen zu bestimmten Nachrichten zu finden.

Die in diesem Kapitel verwendeten vierstelligen Codes sind die ATYP-Werte, die in den Prüfmeldungen zu finden sind, wie in der folgenden Beispielmeldung gezeigt:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Informationen zum Festlegen von Audit-Meldungsebenen, zum Ändern von Protokollzielen und zur Verwendung eines externen Syslog-Servers für Ihre Audit-Informationen finden Sie unter"Konfigurieren von

Überwachungsmeldungen und Protokollzielen"

Kategorien von Überwachungsnachrichten

System-Audit-Meldungen

Die Audit-Meldungen der Kategorie „Systemaudit“ werden für Ereignisse verwendet, die sich auf das Audit-System selbst, den Zustand von Grid-Knoten, die systemweite Aufgabenaktivität (Grid-Tasks) und Dienstsicherungsvorgänge beziehen.

Code	Nachrichtentitel und -beschreibung	Siehe
ECMC	Fehlendes Erasure-Coded-Datenfragment: Zeigt an, dass ein fehlendes Erasure-Coded-Datenfragment erkannt wurde.	"ECMC: Fehlendes Erasure-Coded-Datenfragment"
Kulturhauptstadt Europas	Beschädigtes Erasure-Coded-Datenfragment: Zeigt an, dass ein beschädigtes Erasure-Coded-Datenfragment erkannt wurde.	"ECOC: Beschädigtes Erasure-Coded-Datenfragment"
ETAF	Sicherheitsauthentifizierung fehlgeschlagen: Ein Verbindungsversuch mit Transport Layer Security (TLS) ist fehlgeschlagen.	"ETAF: Sicherheitsauthentifizierung fehlgeschlagen"
GNRG	GNDS-Registrierung: Ein Dienst hat Informationen über sich selbst im StorageGRID System aktualisiert oder registriert.	"GNRG: GNDS-Registrierung"
GNUR	GNDS-Abmeldung: Ein Dienst hat sich selbst vom StorageGRID System abgemeldet.	"GNUR: GNDS-Abmeldung"
GTED	Grid-Aufgabe beendet: Der CMN-Dienst hat die Verarbeitung der Grid-Aufgabe abgeschlossen.	"GTED: Grid-Aufgabe beendet"
GTST	Grid-Aufgabe gestartet: Der CMN-Dienst hat mit der Verarbeitung der Grid-Aufgabe begonnen.	"GTST: Grid-Aufgabe gestartet"
GTSU	Grid-Aufgabe übermittelt: Eine Grid-Aufgabe wurde an den CMN-Dienst übermittelt.	"GTSU: Grid-Aufgabe übermittelt"
LLST	Standort verloren: Diese Prüfmeldung wird generiert, wenn ein Standort verloren geht.	"LLST: Standort verloren"
OLST	Objekt verloren: Ein angefordertes Objekt kann im StorageGRID -System nicht gefunden werden.	"OLST: System hat verlorenes Objekt erkannt"

Code	Nachrichtentitel und -beschreibung	Siehe
SADD	Sicherheitsüberprüfung deaktivieren: Die Protokollierung von Überwachungsnachrichten wurde deaktiviert.	"SADD: Sicherheitsüberprüfung deaktivieren"
SADE	Sicherheitsaudit aktivieren: Die Protokollierung von Audit-Nachrichten wurde wiederhergestellt.	"SADE: Sicherheitsaudit aktivieren"
SVRF	Objektspeicherüberprüfung fehlgeschlagen: Ein Inhaltsblock hat die Überprüfung nicht bestanden.	"SVRF: Objektspeicherüberprüfung fehlgeschlagen"
SVRU	Object Store Verify Unknown: Im Objektspeicher wurden unerwartete Objektdaten erkannt.	"SVRU: Object Store Verify Unbekannt"
SYSD	Knotenstopp: Es wurde ein Herunterfahren angefordert.	"SYSD: Knotenstopp"
SYST	Knoten wird gestoppt: Ein Dienst hat einen ordnungsgemäßen Stopp eingeleitet.	"SYST: Knoten wird gestoppt"
SYSU	Knotenstart: Ein Dienst wurde gestartet. Die Art des vorherigen Herunterfahrens wird in der Nachricht angegeben.	"SYSU: Knotenstart"

Objektspeicher-Auditmeldungen

Die Audit-Meldungen der Kategorie „Objektspeicher-Audit“ werden für Ereignisse im Zusammenhang mit der Speicherung und Verwaltung von Objekten innerhalb des StorageGRID -Systems verwendet. Hierzu gehören die Speicherung und Abfrage von Objekten, Übertragungen von Grid-Knoten zu Grid-Knoten und Überprüfungen.

Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, wenn Funktionen veraltet sind. Wenn Sie auf einen Prüfcode stoßen, der hier nicht aufgeführt ist, überprüfen Sie die vorherigen Versionen dieses Themas auf ältere SG-Versionen. Beispiel: "StorageGRID 11.8 Objektspeicher-Auditmeldungen" .

Code	Beschreibung	Siehe
BROR	Bucket-Nur-Lese-Anforderung: Ein Bucket hat den Nur-Lese-Modus betreten oder verlassen.	"BROR: Bucket-Nur-Lese-Anforderung"
CBSE	Ende der Objektübertragung: Die Quelleinheit hat einen Datenübertragungsvorgang von Grid-Knoten zu Grid-Knoten abgeschlossen.	"CBSE: Objekt senden Ende"

Code	Beschreibung	Siehe
CBRE	Objektempfangsende: Die Zielentität hat einen Datenübertragungsvorgang von Grid-Knoten zu Grid-Knoten abgeschlossen.	"CBRE: Objektempfangsende"
CGRR	Cross-Grid-Replikationsanforderung: StorageGRID hat einen Cross-Grid-Replikationsvorgang versucht, um Objekte zwischen Buckets in einer Grid-Föderationsverbindung zu replizieren.	"CGRR: Cross-Grid-Replikationsanforderung"
EBDL	Löschen eines leeren Buckets: Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, der alle Objekte löscht (führt einen Vorgang zum Leeren des Buckets aus).	"EBDL: Leeren Bucket löschen"
EBKR	Anforderung zum Leeren des Buckets: Ein Benutzer hat eine Anforderung gesendet, den leeren Bucket ein- oder auszuschalten (d. h. Bucket-Objekte zu löschen oder das Löschen von Objekten zu beenden).	"EBKR: Leere Bucket-Anforderung"
SCMT	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	"SCMT: Object Store Commit-Anforderung"
SREM	Object Store Remove: Ein Inhaltsblock wurde aus einem Rasterknoten gelöscht und kann nicht mehr direkt angefordert werden.	"SREM: Objektspeicher entfernen"

Client liest Audit-Nachrichten

Wenn eine S3-Clientanwendung eine Anforderung zum Abrufen eines Objekts stellt, werden Prüfmeldungen zum Lesen des Clients protokolliert.

Code	Beschreibung	Verwendet von	Siehe
S3SL	S3 Select-Anforderung: Protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Nachricht kann Fehlermeldungs- und Fehlercodedetails enthalten. Die Anfrage war möglicherweise nicht erfolgreich.	S3-Client	"S3SL: S3-Auswahlanforderung"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfnachricht das Feld S3SR.	S3-Client	"SGET: S3 GET"

Code	Beschreibung	Verwendet von	Siehe
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Buckets zu überprüfen.	S3-Client	"SHEA: S3 KOPF"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Container.	Swift-Client	"WGET: Schnelles GET"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Containers zu überprüfen.	Swift-Client	"WHEA: Schneller Kopf"

Client schreibt Prüfmeldungen

Client-Schreibprüfmeldungen werden protokolliert, wenn eine S3-Clientanwendung eine Anforderung zum Erstellen oder Ändern eines Objekts stellt.

Code	Beschreibung	Verwendet von	Siehe
OVWR	Objektüberschreiben: Protokolliert eine Transaktion zum Überschreiben eines Objekts mit einem anderen Objekt.	S3- und Swift-Clients	"OVWR: Objektüberschreiben"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfnachricht das Feld S3SR.	S3-Client	"SDEL: S3 LÖSCHEN"
SPOS	S3 POST: Protokolliert eine erfolgreiche Transaktion zum Wiederherstellen eines Objekts aus dem AWS Glacier-Speicher in einem Cloud-Speicherpool.	S3-Client	"SPOS: S3 POST"
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfnachricht das Feld S3SR.	S3-Client	"SPUT: S3 PUT"
SUPD	S3-Metadaten aktualisiert: Protokolliert eine erfolgreiche Transaktion zum Aktualisieren der Metadaten für ein vorhandenes Objekt oder einen vorhandenen Bucket.	S3-Client	"SUPD: S3-Metadaten aktualisiert"

Code	Beschreibung	Verwendet von	Siehe
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	Swift-Client	"WDEL: Schnelles LÖSCHEN"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Containers.	Swift-Client	"WPUT: Schnelles PUT"

Management-Audit-Nachricht

Die Kategorie „Verwaltung“ protokolliert Benutzeranforderungen an die Verwaltungs-API.

Code	Nachrichtentitel und -beschreibung	Siehe
MGAU	Audit-Nachricht der Management-API: Ein Protokoll der Benutzeranforderungen.	"MGAU: Management-Audit-Nachricht"

ILM-Audit-Meldungen

Die Prüfmeldungen der Kategorie „ILM-Prüfung“ werden für Ereignisse im Zusammenhang mit Vorgängen im Zusammenhang mit dem Information Lifecycle Management (ILM) verwendet.

Code	Nachrichtentitel und -beschreibung	Siehe
IDEL	Von ILM initiiertes Löschen: Diese Prüfmeldung wird generiert, wenn ILM den Löschvorgang eines Objekts startet.	"IDEL: Von ILM initiiertes Löschen"
LKCU	Bereinigung überschriebener Objekte. Diese Prüfmeldung wird generiert, wenn ein überschriebenes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	"LKCU: Bereinigung überschriebener Objekte"
ORLM	Objektregeln erfüllt: Diese Prüfmeldung wird generiert, wenn Objektdaten gemäß den ILM-Regeln gespeichert werden.	"ORLM: Objektregeln erfüllt"

Prüfnachrichtenreferenz

BROR: Bucket-Nur-Lese-Anforderung

Der LDR-Dienst generiert diese Prüfnachricht, wenn ein Bucket in den schreibgeschützten Modus wechselt oder diesen verlässt. Beispielsweise wechselt ein Bucket in den schreibgeschützten Modus, während alle Objekte gelöscht werden.

Code	Feld	Beschreibung
BKHD	Bucket-UUID	Die Bucket-ID.

Code	Feld	Beschreibung
BROV	Bucket-Schreibschutz-Anforderungswert	Ob der Bucket schreibgeschützt wird oder den schreibgeschützten Zustand verlässt (1 = schreibgeschützt, 0 = nicht schreibgeschützt).
BROS	Bucket-Schreibschutzgrund	Der Grund, warum der Bucket schreibgeschützt wird oder den schreibgeschützten Zustand verlässt. Beispiel: emptyBucket.
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, das die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.

CBRB: Objektempfang beginnt

Während des normalen Systembetriebs werden Inhaltsblöcke kontinuierlich zwischen verschiedenen Knoten übertragen, während auf Daten zugegriffen, diese repliziert und gespeichert werden. Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen initiiert wird, wird diese Nachricht von der Zielentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.
CTSS	Sequenzzählung starten	Gibt die erste angeforderte Sequenzanzahl an. Bei Erfolg beginnt die Übertragung ab dieser Sequenzzählung.

Code	Feld	Beschreibung
CTES	Erwartete Endsequenzanzahl	Gibt die zuletzt angeforderte Sequenzzählung an. Bei Erfolg gilt die Übertragung als abgeschlossen, wenn diese Sequenzanzahl empfangen wurde.
RSLT	Übertragungsstartstatus	Status zum Zeitpunkt des Überweisungsbeginns: SUCS: Übertragung erfolgreich gestartet.

Diese Prüfmeldung bedeutet, dass ein Knoten-zu-Knoten-Datenübertragungsvorgang für ein einzelnes Inhaltselement initiiert wurde, das durch seine Inhaltsblockkennung identifiziert wird. Der Vorgang fordert Daten von „Start Sequence Count“ bis „Expected End Sequence Count“ an. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und in Kombination mit Speicherüberwachungsmeldungen die Anzahl der Replikate zu überprüfen.

CBRE: Objektempfangsende

Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen abgeschlossen ist, wird diese Nachricht von der Zielentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.
CTSS	Sequenzzählung starten	Gibt die Sequenzanzahl an, bei der die Übertragung begonnen hat.
CTAS	Tatsächliche Endsequenzanzahl	Gibt die letzte erfolgreich übertragene Sequenzanzahl an. Wenn die tatsächliche Endsequenzanzahl mit der Startsequenzanzahl übereinstimmt und das Übertragungsergebnis nicht erfolgreich war, wurden keine Daten ausgetauscht.

Code	Feld	Beschreibung
RSLT	Übertragungsergebnis	Das Ergebnis des Übertragungsvorgangs (aus Sicht der sendenden Entität): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung verloren CTMO: Verbindungs-Timeout während des Aufbaus oder der Übertragung UNRE: Zielknoten-ID nicht erreichbar CRPT: Übertragung aufgrund des Empfangs beschädigter oder ungültiger Daten beendet

Diese Prüfmeldung bedeutet, dass ein Datenübertragungsvorgang von Knoten zu Knoten abgeschlossen wurde. Wenn das Übertragungsergebnis erfolgreich war, hat der Vorgang Daten von „Start Sequence Count“ nach „Actual End Sequence Count“ übertragen. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und Fehler zu lokalisieren, zu tabellieren und zu analysieren. In Kombination mit Speicherüberwachungsmeldungen kann es auch zum Überprüfen der Replikatanzahl verwendet werden.

CBSB: Objekt senden beginnen

Während des normalen Systembetriebs werden Inhaltsblöcke kontinuierlich zwischen verschiedenen Knoten übertragen, während auf Daten zugegriffen, diese repliziert und gespeichert werden. Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen initiiert wird, wird diese Nachricht von der Quellentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.

Code	Feld	Beschreibung
CTSS	Sequenzzählung starten	Gibt die erste angeforderte Sequenzanzahl an. Bei Erfolg beginnt die Übertragung ab dieser Sequenzzählung.
CTES	Erwartete Endsequenzanzahl	Gibt die zuletzt angeforderte Sequenzzählung an. Bei Erfolg gilt die Übertragung als abgeschlossen, wenn diese Sequenzanzahl empfangen wurde.
RSLT	Übertragungsstartstatus	Status zum Zeitpunkt des Überweisungsbeginns: SUCS: Übertragung erfolgreich gestartet.

Diese Prüfmeldung bedeutet, dass ein Knoten-zu-Knoten-Datenübertragungsvorgang für ein einzelnes Inhaltselement initiiert wurde, das durch seine Inhaltsblockkennung identifiziert wird. Der Vorgang fordert Daten von „Start Sequence Count“ bis „Expected End Sequence Count“ an. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und in Kombination mit Speicherüberwachungsmeldungen die Anzahl der Replikate zu überprüfen.

CBSE: Objekt senden Ende

Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen abgeschlossen ist, wird diese Nachricht von der Quellentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.
CTSS	Sequenzzählung starten	Gibt die Sequenzanzahl an, bei der die Übertragung begonnen hat.

Code	Feld	Beschreibung
CTAS	Tatsächliche Endsequenzanzahl	Gibt die letzte erfolgreich übertragene Sequenzanzahl an. Wenn die tatsächliche Endsequenzanzahl mit der Startsequenzanzahl übereinstimmt und das Übertragungsergebnis nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Übertragungsergebnis	Das Ergebnis des Übertragungsvorgangs (aus Sicht der sendenden Entität): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung verloren CTMO: Verbindungs-Timeout während des Aufbaus oder der Übertragung UNRE: Zielknoten-ID nicht erreichbar CRPT: Übertragung aufgrund des Empfangs beschädigter oder ungültiger Daten beendet

Diese Prüfmeldung bedeutet, dass ein Datenübertragungsvorgang von Knoten zu Knoten abgeschlossen wurde. Wenn das Übertragungsergebnis erfolgreich war, hat der Vorgang Daten von „Start Sequence Count“ nach „Actual End Sequence Count“ übertragen. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und Fehler zu lokalisieren, zu tabellieren und zu analysieren. In Kombination mit Speicherüberwachungsmeldungen kann es auch zum Überprüfen der Replikatanzahl verwendet werden.

CGRR: Cross-Grid-Replikationsanforderung

Diese Nachricht wird generiert, wenn StorageGRID einen Cross-Grid-Replikationsvorgang versucht, um Objekte zwischen Buckets in einer Grid-Föderationsverbindung zu replizieren.

Code	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Bytes. Das CSIZ-Attribut wurde in StorageGRID 11.8 eingeführt. Dies kann dazu führen, dass Cross-Grid-Replikationsanforderungen, die ein Upgrade von StorageGRID 11.7 auf 11.8 umfassen, eine ungenaue Gesamtobjektgröße aufweisen.
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, dem der Bucket gehört, aus dem das Objekt repliziert wird.
GFID	Grid-Föderation-Verbindungs-ID	Die ID der Grid-Föderationsverbindung, die für die Grid-übergreifende Replikation verwendet wird.

Code	Feld	Beschreibung
OPER	CGR-Betrieb	Der Typ des Cross-Grid-Replikationsvorgangs, der versucht wurde: • 0 = Objekt replizieren • 1 = Mehrteiliges Objekt replizieren • 2 = Löschmarkierung replizieren
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, das repliziert wurde.
RSLT	Ergebniscode	Gibt „Erfolgreich“ (SUCS) oder einen allgemeinen Fehler (GERR) zurück.

EBDL: Leeren Bucket löschen

Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, der alle Objekte löscht (und dabei einen Bucket-Leervorgang durchführt).

Code	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Bytes.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
RSLT	Ergebnis des Löschvorgangs	Das Ergebnis eines Ereignisses, Prozesses oder einer Transaktion. Wenn es für eine Nachricht nicht relevant ist, wird NONE statt SUCS verwendet, damit die Nachricht nicht versehentlich gefiltert wird.

EBKR: Leere Bucket-Anforderung

Diese Nachricht zeigt an, dass ein Benutzer eine Anforderung zum Ein- oder Ausschalten des leeren Buckets gesendet hat (d. h. zum Löschen von Bucket-Objekten oder zum Beenden des Löschens von Objekten).

Code	Feld	Beschreibung
BAUEN	Bucket-UUID	Die Bucket-ID.
EBJS	JSON-Konfiguration für leeren Bucket	Enthält das JSON, das die aktuelle Empty Bucket-Konfiguration darstellt.
S3AI	S3-Mandantenkonto-ID	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.

ECMC: Fehlendes Erasure-Coded-Datenfragment

Diese Prüfmeldung zeigt an, dass das System ein fehlendes Erasure-Coded-Datenfragment erkannt hat.

Code	Feld	Beschreibung
VCMC	VCS-ID	Der Name des VCS, das den fehlenden Block enthält.
MCID	Chunk-ID	Die Kennung des fehlenden Erasure-Codierten-Fragments.
RSLT	Ergebnis	Dieses Feld hat den Wert „NONE“. RSLT ist ein obligatorisches Nachrichtenfeld, ist für diese spezielle Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird „NONE“ anstelle von „SUCS“ verwendet.

ECOC: Beschädigtes Erasure-Coded-Datenfragment

Diese Prüfmeldung zeigt an, dass das System ein beschädigtes, löschcodiertes Datenfragment erkannt hat.

Code	Feld	Beschreibung
VCCO	VCS-ID	Der Name des VCS, das den beschädigten Block enthält.
VLID	Datenträger-ID	Das RangeDB-Volume, das das beschädigte Erasure-Coded-Fragment enthält.
CCID	Chunk-ID	Die Kennung des beschädigten Erasure-Code-Fragments.
RSLT	Ergebnis	Dieses Feld hat den Wert „NONE“. RSLT ist ein obligatorisches Nachrichtenfeld, ist für diese spezielle Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird „NONE“ anstelle von „SUCS“ verwendet.

ETAF: Sicherheitsauthentifizierung fehlgeschlagen

Diese Nachricht wird generiert, wenn ein Verbindungsversuch mit Transport Layer Security (TLS) fehlgeschlagen ist.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung, über die die Authentifizierung fehlgeschlagen ist.
RUID	Benutzeridentität	Eine dienstabhängige Kennung, die die Identität des Remotebenutzers darstellt.
RSLT	Ursachencode	Der Grund für das Scheitern: SCNI: Der Aufbau einer sicheren Verbindung ist fehlgeschlagen. CERM: Zertifikat fehlte. CERT: Das Zertifikat war ungültig. CERE: Zertifikat ist abgelaufen. CERR: Zertifikat wurde widerrufen. CSGN: Die Zertifikatssignatur war ungültig. CSGU: Der Zertifikatsunterzeichner war unbekannt. UCRM: Benutzeranmeldeinformationen fehlten. UCRI: Benutzeranmeldeinformationen waren ungültig. UCRU: Benutzeranmeldeinformationen wurden nicht zugelassen. TOUT: Zeitüberschreitung bei der Authentifizierung.

Wenn eine Verbindung zu einem sicheren Dienst hergestellt wird, der TLS verwendet, werden die Anmeldeinformationen der Remote-Entität mithilfe des TLS-Profils und zusätzlicher, in den Dienst integrierter Logik überprüft. Wenn diese Authentifizierung aufgrund ungültiger, unerwarteter oder nicht zulässiger Zertifikate oder Anmeldeinformationen fehlschlägt, wird eine Prüfmeldung protokolliert. Dies ermöglicht Abfragen bei unberechtigten Zugriffsversuchen und anderen sicherheitsrelevanten Verbindungsproblemen.

Die Meldung kann durch eine falsche Konfiguration einer Remote-Entität oder durch Versuche verursacht werden, dem System ungültige oder nicht zulässige Anmeldeinformationen vorzulegen. Diese Prüfmeldung sollte überwacht werden, um Versuche zu erkennen, sich unbefugten Zugriff auf das System zu verschaffen.

GNRG: GNDS-Registrierung

Der CMN-Dienst generiert diese Prüfnachricht, wenn ein Dienst Informationen über sich selbst im StorageGRID System aktualisiert oder registriert hat.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • SUCS: Erfolgreich • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Knoten-ID	Die Knoten-ID des Dienstes, der die Aktualisierungsanforderung initiiert hat.
GNTP	Gerätetyp	Der Gerätetyp des Grid-Knotens (z. B. BLDR für einen LDR-Dienst).
GNDV	Gerätemodellversion	Die Zeichenfolge, die die Gerätemodellversion des Grid-Knotens im DMDL-Paket identifiziert.
GNGP	Gruppe	Die Gruppe, zu der der Grid-Knoten gehört (im Kontext der Link-Kosten und der Rangfolge der Service-Abfragen).
GNIA	IP-Adresse	Die IP-Adresse des Grid-Knotens.

Diese Nachricht wird immer dann generiert, wenn ein Grid-Knoten seinen Eintrag im Grid-Knoten-Paket aktualisiert.

GNUR: GNDS-Abmeldung

Der CMN-Dienst generiert diese Prüfnachricht, wenn ein Dienst nicht registrierte Informationen über sich selbst aus dem StorageGRID System hat.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • SUCS: Erfolgreich • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Knoten-ID	Die Knoten-ID des Dienstes, der die Aktualisierungsanforderung initiiert hat.

GTED: Grid-Aufgabe beendet

Diese Prüfmeldung zeigt an, dass der CMN-Dienst die Verarbeitung der angegebenen Rasteraufgabe abgeschlossen und die Aufgabe in die Verlaufstabelle verschoben hat. Wenn das Ergebnis SUCS, ABRT oder ROLF ist, wird eine entsprechende Prüfmeldung „Grid Task Started“ angezeigt. Die anderen Ergebnisse deuten darauf hin, dass die Verarbeitung dieser Grid-Aufgabe nie begonnen hat.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Grid-Aufgabe über ihren Lebenszyklus. **Hinweis:** Die Aufgaben-ID wird zum Zeitpunkt der Generierung einer Rasteraufgabe zugewiesen, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Rasteraufgabe mehrmals übermittelt wird. In diesem Fall reicht das Feld „Aufgaben-ID“ nicht aus, um die Prüfmeldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.
RSLT	Ergebnis	Das endgültige Statusergebnis der Grid-Aufgabe: • SUCS: Die Rasteraufgabe wurde erfolgreich abgeschlossen. • ABRT: Die Grid-Aufgabe wurde ohne Rollback-Fehler beendet. • ROLF: Die Grid-Aufgabe wurde beendet und konnte den Rollback-Prozess nicht abschließen. • CANC: Die Grid-Aufgabe wurde vom Benutzer abgebrochen, bevor sie gestartet wurde. • EXPR: Die Grid-Aufgabe ist abgelaufen, bevor sie gestartet wurde. • IVLD: Die Rasteraufgabe war ungültig. • AUTH: Die Grid-Aufgabe war nicht autorisiert. • DUPL: Die Rasteraufgabe wurde als Duplikat abgelehnt.

GTST: Grid-Aufgabe gestartet

Diese Prüfmeldung zeigt an, dass der CMN-Dienst mit der Verarbeitung der angegebenen Grid-Aufgabe begonnen hat. Die Prüfnachricht folgt unmittelbar auf die Nachricht „Grid Task Submitted“ für Grid-Aufgaben, die vom internen Grid Task Submission-Dienst initiiert und für die automatische Aktivierung ausgewählt wurden. Für Rasteraufgaben, die in die Tabelle „Ausstehend“ übermittelt werden, wird diese Nachricht generiert, wenn der Benutzer die Rasteraufgabe startet.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Dieses Feld identifiziert eine generierte Rasteraufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über ihren Lebenszyklus. **Hinweis:** Die Aufgaben-ID wird zum Zeitpunkt der Generierung einer Rasteraufgabe zugewiesen, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Rasteraufgabe mehrmals übermittelt wird. In diesem Fall reicht das Feld „Aufgaben-ID“ nicht aus, um die Prüfmeldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis. Dieses Feld hat nur einen Wert: • SUCS: Die Grid-Task wurde erfolgreich gestartet.

GTSU: Grid-Aufgabe übermittelt

Diese Prüfnachricht zeigt an, dass eine Rasteraufgabe an den CMN-Dienst übermittelt wurde.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Identifiziert eine generierte Rasteraufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über ihren Lebenszyklus. **Hinweis:** Die Aufgaben-ID wird zum Zeitpunkt der Generierung einer Rasteraufgabe zugewiesen, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Rasteraufgabe mehrmals übermittelt wird. In diesem Fall reicht das Feld „Aufgaben-ID“ nicht aus, um die Prüfmeldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.
TTYP	Aufgabentyp	Der Typ der Rasteraufgabe.
TWER	Aufgabenversion	Eine Zahl, die die Version der Rasteraufgabe angibt.
TDSC	Aufgabenbeschreibung	Eine für Menschen lesbare Beschreibung der Rasteraufgabe.
Mehrwertsteuer	Gültig nach Zeitstempel	Der früheste Zeitpunkt (UINT64 Mikrosekunden ab 1. Januar 1970 – UNIX-Zeit), zu dem die Grid-Aufgabe gültig ist.
VBTS	Gültig vor Zeitstempel	Der späteste Zeitpunkt (UINT64 Mikrosekunden ab 1. Januar 1970 – UNIX-Zeit), zu dem die Grid-Aufgabe gültig ist.
TSRC	Quelle	Die Quelle der Aufgabe: • TXTB: Die Grid-Aufgabe wurde über das StorageGRID -System als signierter Textblock übermittelt. • GRID: Die Grid-Aufgabe wurde über den internen Grid Task Submission Service übermittelt.
ACTV	Aktivierungstyp	Die Art der Aktivierung: • AUTO: Die Rasteraufgabe wurde zur automatischen Aktivierung übermittelt. • PEND: Die Rasteraufgabe wurde in die ausstehende Tabelle übermittelt. Dies ist die einzige Möglichkeit für die TXTB-Quelle.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Einreichung: • SUCS: Die Rasteraufgabe wurde erfolgreich übermittelt. • FEHLGESCHLAGEN: Die Aufgabe wurde direkt in die Verlaufstabelle verschoben.

IDEL: Von ILM initiiertes Löschen

Diese Nachricht wird generiert, wenn ILM den Löschvorgang eines Objekts startet.

Die IDEL-Nachricht wird in einer der folgenden Situationen generiert:

- **Für Objekte in konformen S3-Buckets**: Diese Nachricht wird generiert, wenn ILM den Prozess des automatischen Löschens eines Objekts startet, weil seine Aufbewahrungsfrist abgelaufen ist (vorausgesetzt, die Einstellung zum automatischen Löschen ist aktiviert und die rechtliche Aufbewahrungsfrist ist deaktiviert).
- **Für Objekte in nicht konformen S3-Buckets**. Diese Nachricht wird generiert, wenn ILM mit dem Löschen eines Objekts beginnt, weil in den aktiven ILM-Richtlinien derzeit keine Platzierungsanweisungen für das Objekt gelten.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die CBID des Objekts.
CMPA	Compliance: Automatisches Löschen	Nur für Objekte in konformen S3-Buckets. 0 (falsch) oder 1 (wahr) gibt an, ob ein konformes Objekt automatisch gelöscht werden soll, wenn seine Aufbewahrungsfrist endet, es sei denn, der Bucket unterliegt einer rechtlichen Sperre.
CMPL	Compliance: Gesetzliche Aufbewahrungspflicht	Nur für Objekte in konformen S3-Buckets. 0 (falsch) oder 1 (wahr), gibt an, ob der Bucket derzeit einer rechtlichen Sperre unterliegt.
CMPR	Compliance: Aufbewahrungsfrist	Nur für Objekte in konformen S3-Buckets. Die Länge der Aufbewahrungsdauer des Objekts in Minuten.
CTME	Compliance: Aufnahmezeit	Nur für Objekte in konformen S3-Buckets. Die Aufnahmezeit des Objekts. Sie können zu diesem Wert die Aufbewahrungsdauer in Minuten hinzufügen, um festzulegen, wann das Objekt aus dem Bucket gelöscht werden kann.
DMRK	Marker-Versions-ID löschen	Die Versions-ID der Löschmarkierung, die beim Löschen eines Objekts aus einem versionierten Bucket erstellt wird. Operationen an Buckets schließen dieses Feld nicht ein.

Code	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.
LOCS	Standorte	Der Speicherort der Objektdaten innerhalb des StorageGRID -Systems. Der Wert für LOCS ist "", wenn das Objekt keine Standorte hat (z. B. wenn es gelöscht wurde). CLEC: für Erasure-Coding-Objekte die Erasure-Coding-Profil-ID und die Erasure-Coding-Gruppen-ID, die auf die Daten des Objekts angewendet wird. CLDI: für replizierte Objekte die LDR-Knoten-ID und die Volume-ID des Objektstandorts. CLNL: ARC-Knoten-ID des Objektstandorts, wenn die Objektdaten archiviert sind.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	• Wenn ein Objekt in einem konformen S3-Bucket automatisch gelöscht wird, weil seine Aufbewahrungsfrist abgelaufen ist, ist dieses Feld leer. • Wenn das Objekt gelöscht wird, weil derzeit keine Platzierungsanweisungen mehr für das Objekt gelten, wird in diesem Feld die menschenlesbare Bezeichnung der letzten ILM-Regel angezeigt, die für das Objekt galt.
SGRP	Site (Gruppe)	Falls vorhanden, wurde das Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das Objekt aufgenommen wurde.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, das gelöscht wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

LKCU: Bereinigung überschriebener Objekte

Diese Meldung wird generiert, wenn StorageGRID ein überschriebenes Objekt entfernt, das zuvor bereinigt werden musste, um Speicherplatz freizugeben. Ein Objekt wird überschrieben, wenn ein S3-Client ein Objekt in einen Pfad schreibt, der bereits ein Objekt enthält. Der Entfernungsprozess erfolgt automatisch und im Hintergrund.

Code	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.
LTYP	Art der Bereinigung	*Nur zur internen Verwendung.*
LUID	Entfernte Objekt-UUID	Die Kennung des Objekts, das entfernt wurde.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
UUID	Universell eindeutige Kennung	Die Kennung des noch vorhandenen Objekts. Dieser Wert ist nur verfügbar, wenn das Objekt nicht gelöscht wurde.

LKDM: Bereinigung durchgesickerter Objekte

Diese Nachricht wird generiert, wenn ein durchgesickerter Block bereinigt oder gelöscht wurde. Ein Chunk kann Teil eines replizierten Objekts oder eines erasure-encoded Objekts sein.

Code	Feld	Beschreibung
CLOC	Chunk-Standort	Der Dateipfad des durchgesickerten Blocks, der gelöscht wurde.

CTYP	Chunk-Typ	Art des Chunks:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

Code	Feld	Beschreibung

LTYP	Lecktyp	Die fünf Arten von Lecks, die erkannt werden können:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Chunk-Erstellungszeit	Zeitpunkt der Erstellung des durchgesickerten Chunks.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts, zu dem der Block gehört.
CBID	Inhaltsblockkennung	CBID des Objekts, zu dem der durchgesickerte Block gehört.
CSIZ	Inhaltsgröße	Die Größe des Blocks in Bytes.

LLST: Standort verloren

Diese Nachricht wird generiert, wenn kein Speicherort für eine Objektkopie (repliziert oder löschcodiert) gefunden werden kann.

Code	Feld	Beschreibung
CBIL	CBID	Das betroffene CBID.
ECPR	Erasure-Coding-Profil	Für löschcodierte Objektdaten. Die ID des verwendeten Erasure-Coding-Profils.
LTYP	Ortstyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für erasure-coded Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten

Code	Feld	Beschreibung
NOID	Quellknoten-ID	Die Knoten-ID, auf der die Standorte verloren gegangen sind.
PCLD	Pfad zum replizierten Objekt	Der vollständige Pfad zum Speicherort der verlorenen Objektdaten auf der Festplatte. Wird nur zurückgegeben, wenn LTYP den Wert CLDI hat (d. h. für replizierte Objekte). Nimmt die Form an `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Ergebnis	Immer KEINE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.
TSRC	Auslösende Quelle	USER: Vom Benutzer ausgelöst SYST: System ausgelöst
UUID	Universell eindeutige ID	Die Kennung des betroffenen Objekts im StorageGRID -System.

MGAU: Management-Audit-Nachricht

Die Kategorie „Verwaltung“ protokolliert Benutzeranforderungen an die Verwaltungs-API. Jede HTTP-Anforderung, die keine GET- oder HEAD-Anforderung an eine gültige API-URI ist, protokolliert eine Antwort, die den Benutzernamen, die IP und den Anforderungstyp an die API enthält. Ungültige API-URIs (wie z. B. /api/v3-authorize) und ungültige Anfragen an gültige API-URIs werden nicht protokolliert.

Code	Feld	Beschreibung
MDIP	Ziel-IP-Adresse	Die IP-Adresse des Servers (Ziel).
MDNA	Domänenname	Der Hostdomänenname.
MPAT	PATH anfordern	Der Anforderungspfad.
MPQP	Abfrageparameter anfordern	Die Abfrageparameter für die Anfrage.

Code	Feld	Beschreibung
MRBD	Anforderungstext	Der Inhalt des Anforderungstexts. Während der Antworttext standardmäßig protokolliert wird, wird der Anforderungstext in bestimmten Fällen protokolliert, wenn der Antworttext leer ist. Da die folgenden Informationen im Antworttext nicht verfügbar sind, werden sie für die folgenden POST-Methoden aus dem Anforderungstext übernommen: • Benutzername und Konto-ID in **POST-Autorisierung** • Neue Subnetzkonfiguration in **POST /grid/grid-networks/update** • Neue NTP-Server in **POST /grid/ntp-servers/update** • Außer Betrieb genommene Server-IDs in **POST /grid/servers/decommission** **Hinweis:** Vertrauliche Informationen werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen maskiert (z. B. ein Passwort).
MRMD	Anforderungsmethode	Die HTTP-Anforderungsmethode: • POST • SETZEN • LÖSCHEN • PATCH
MRSC	Antwortcode	Der Antwortcode.
UVP	Antworttext	Der Inhalt der Antwort (der Antworttext) wird standardmäßig protokolliert. **Hinweis:** Vertrauliche Informationen werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen maskiert (z. B. ein Passwort).
MSIP	Quell-IP-Adresse	Die IP-Adresse des Clients (Quelle).
MUUN	Benutzer-URN	Der URN (Uniform Resource Name) des Benutzers, der die Anfrage gesendet hat.
RSLT	Ergebnis	Gibt „Erfolgreich“ (SUCS) oder den vom Backend gemeldeten Fehler zurück.

OLST: System hat verlorenes Objekt erkannt

Diese Nachricht wird generiert, wenn der DDS-Dienst keine Kopien eines Objekts im StorageGRID -System finden kann.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die CBID des verlorenen Objekts.
NOID	Knoten-ID	Falls verfügbar, der letzte bekannte direkte oder nahegelegene Standort des verlorenen Objekts. Es ist möglich, nur die Knoten-ID ohne Volume-ID zu haben, wenn die Volume-Informationen nicht verfügbar sind.
WEG	S3-Bucket/Schlüssel	Falls verfügbar, der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.
UUID	Universell eindeutige ID	Die Kennung des verlorenen Objekts innerhalb des StorageGRID -Systems.
VOLI	Datenträger-ID	Falls verfügbar, die Volume-ID des Speicherknotens für den letzten bekannten Standort des verlorenen Objekts.

ORLM: Objektregeln erfüllt

Diese Nachricht wird generiert, wenn das Objekt gemäß den ILM-Regeln erfolgreich gespeichert und kopiert wurde.

> ⓘ Die ORLM-Meldung wird nicht generiert, wenn ein Objekt erfolgreich durch die Standardregel „2 Kopien erstellen“ gespeichert wurde und eine andere Regel in der Richtlinie den erweiterten Filter „Objektgröße“ verwendet.

Code	Feld	Beschreibung
BAUEN	Schaufelkopf	Bucket-ID-Feld. Wird für interne Vorgänge verwendet. Erscheint nur, wenn STAT PRGD ist.
CBID	Inhaltsblockkennung	Die CBID des Objekts.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.

Code	Feld	Beschreibung
LOCS	Standorte	Der Speicherort der Objektdaten innerhalb des StorageGRID -Systems. Der Wert für LOCS ist "", wenn das Objekt keine Standorte hat (z. B. wenn es gelöscht wurde). CLEC: für Erasure-Coding-Objekte die Erasure-Coding-Profil-ID und die Erasure-Coding-Gruppen-ID, die auf die Daten des Objekts angewendet wird. CLDI: für replizierte Objekte die LDR-Knoten-ID und die Volume-ID des Objektstandorts. CLNL: ARC-Knoten-ID des Objektstandorts, wenn die Objektdaten archiviert sind.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	Die für Menschen lesbare Bezeichnung für die auf dieses Objekt angewendete ILM-Regel.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
SGCB	Behälter CBID	CBID des Containers für das segmentierte Objekt. Dieser Wert ist nur für segmentierte und mehrteilige Objekte verfügbar.
STAT	Status	Der Status des ILM-Vorgangs. FERTIG: ILM-Vorgänge für das Objekt wurden abgeschlossen. DFER: Das Objekt wurde für eine zukünftige ILM-Neubewertung markiert. PRGD: Das Objekt wurde aus dem StorageGRID -System gelöscht. NLOC: Die Objektdaten sind im StorageGRID -System nicht mehr auffindbar. Dieser Status kann darauf hinweisen, dass alle Kopien der Objektdaten fehlen oder beschädigt sind.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.

Code	Feld	Beschreibung
VSID	Versions-ID	Die Versions-ID eines neuen Objekts, das in einem versionierten Bucket erstellt wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

Die ORLM-Audit-Nachricht kann für ein einzelnes Objekt mehr als einmal ausgegeben werden. Es wird beispielsweise immer dann ausgegeben, wenn eines der folgenden Ereignisse eintritt:

- ILM-Regeln für das Objekt werden dauerhaft erfüllt.
- Die ILM-Regeln für das Objekt werden für diese Epoche erfüllt.
- Das Objekt wurde durch ILM-Regeln gelöscht.
- Der Hintergrundüberprüfungsprozess erkennt, dass eine Kopie der replizierten Objektdaten beschädigt ist. Das StorageGRID -System führt eine ILM-Auswertung durch, um das beschädigte Objekt zu ersetzen.

Ähnliche Informationen

- "Objektaufnahmetransaktionen"
- "Objektlöschtransaktionen"

OVWR: Objektüberschreiben

Diese Nachricht wird generiert, wenn ein externer (vom Client angeforderter) Vorgang dazu führt, dass ein Objekt durch ein anderes Objekt überschrieben wird.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung (neu)	Die CBID für das neue Objekt.
CSIZ	Vorherige Objektgröße	Die Größe des zu überschreibenden Objekts in Bytes.
OCBD	Inhaltsblockkennung (vorherig)	Die CBID für das vorherige Objekt.
UUID	Universell eindeutige ID (neu)	Die Kennung des neuen Objekts innerhalb des StorageGRID -Systems.
OUID	Universell eindeutige ID (vorher)	Die Kennung für das vorherige Objekt innerhalb des StorageGRID -Systems.
WEG	S3-Objektpfad	Der S3-Objektpfad, der sowohl für das vorherige als auch für das neue Objekt verwendet wird

Code	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der Objektüberschreibungstransaktion. Ergebnis ist immer: SUCS: Erfolgreich
SGRP	Site (Gruppe)	Falls vorhanden, wurde das überschriebene Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das überschriebene Objekt aufgenommen wurde.

S3SL: S3-Auswahlanforderung

Diese Nachricht protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Nachricht kann Fehlermeldungs- und Fehlercodedetails enthalten. Die Anfrage war möglicherweise nicht erfolgreich.

Code	Feld	Beschreibung
BYSC	Gescannte Bytes	Anzahl der von Speicherknoten gescannten (empfangenen) Bytes. BYSC und BYPR sind wahrscheinlich unterschiedlich, wenn das Objekt komprimiert ist. Wenn das Objekt komprimiert ist, enthält BYSC die komprimierte Byteanzahl und BYPR die Bytes nach der Dekomprimierung.
BYPR	Verarbeitete Bytes	Anzahl der verarbeiteten Bytes. Gibt an, wie viele Bytes der „gescannten Bytes“ tatsächlich von einem S3 Select-Job verarbeitet oder bearbeitet wurden.
BYRT	Zurückgegebene Bytes	Anzahl der Bytes, die ein S3 Select-Job an den Client zurückgegeben hat.
REPR	Verarbeitete Datensätze	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job von Speicherknoten empfangen hat.
RERT	Zurückgegebene Datensätze	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job an den Client zurückgegeben hat.
JOFI	Auftrag abgeschlossen	Gibt an, ob die Verarbeitung des S3 Select-Jobs abgeschlossen ist oder nicht. Wenn dieser Wert falsch ist, konnte der Auftrag nicht abgeschlossen werden und die Fehlerfelder enthalten wahrscheinlich Daten. Der Kunde hat möglicherweise nur Teilergebnisse oder gar keine Ergebnisse erhalten.
REID	Anforderungs-ID	Kennung für die S3 Select-Anfrage.
EXTM	Ausführungszeit	Die Zeit in Sekunden, die für die Ausführung des S3 Select-Jobs benötigt wurde.

Code	Feld	Beschreibung
ERMG	Fehlermeldung	Fehlermeldung, die der S3 Select-Job generiert hat.
ERTY	Fehlertyp	Fehlertyp, der vom S3 Select-Job generiert wurde.
ERST	Fehler-Stacktrace	Fehler-Stacktrace, den der S3 Select-Job generiert hat.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat.
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen.

SADD: Sicherheitsüberprüfung deaktivieren

Diese Nachricht zeigt an, dass der ursprüngliche Dienst (Knoten-ID) die Protokollierung von Prüfnachrichten deaktiviert hat. Prüfnachrichten werden nicht mehr erfasst oder übermittelt.

Code	Feld	Beschreibung
AETM	Enable-Methode	Die zum Deaktivieren der Überwachung verwendete Methode.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Deaktivieren der Überwachungsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.

Die Meldung impliziert, dass die Protokollierung zuvor aktiviert war, jetzt aber deaktiviert wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemleistung zu verbessern. Nach der Massenaktivität wird die Überwachung wiederhergestellt (SADE) und die Möglichkeit, die Überwachung zu deaktivieren, wird dann dauerhaft blockiert.

SADE: Sicherheitsaudit aktivieren

Diese Nachricht zeigt an, dass der ursprüngliche Dienst (Knoten-ID) die Protokollierung

von Prüfnachrichten wiederhergestellt hat. Prüfnachrichten werden wieder erfasst und übermittelt.

Code	Feld	Beschreibung
AETM	Enable-Methode	Die Methode, die zum Aktivieren der Prüfung verwendet wird.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Aktivieren der Überwachungsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.

Die Meldung impliziert, dass die Protokollierung zuvor deaktiviert war (SADD), jetzt aber wiederhergestellt wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemleistung zu verbessern. Nach der Massenaktivität wird die Überwachung wiederhergestellt und die Möglichkeit zum Deaktivieren der Überwachung dauerhaft blockiert.

SCMT: Objektspeicher-Commit

Grid-Inhalte werden erst verfügbar gemacht oder als gespeichert erkannt, wenn sie festgeschrieben (d. h. dauerhaft gespeichert) wurden. Dauerhaft gespeicherte Inhalte wurden vollständig auf die Festplatte geschrieben und haben die zugehörigen Integritätsprüfungen bestanden. Diese Nachricht wird ausgegeben, wenn ein Inhaltsblock gespeichert wird.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des Inhaltsblocks, der dauerhaft gespeichert wird.
RSLT	Ergebniscode	Status zum Zeitpunkt der Speicherung des Objekts auf der Festplatte: SUCS: Objekt erfolgreich gespeichert.

Diese Meldung bedeutet, dass ein bestimmter Inhaltsblock vollständig gespeichert und überprüft wurde und nun angefordert werden kann. Damit kann der Datenfluss innerhalb des Systems verfolgt werden.

SDEL: S3 LÖSCHEN

Wenn ein S3-Client eine DELETE-Transaktion ausgibt, wird eine Anforderung zum Entfernen des angegebenen Objekts oder Buckets oder zum Entfernen einer Bucket-/Objekt-Unterressource gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
DMRK	Marker-Versions-ID löschen	Die Versions-ID der Löschmarkierung, die beim Löschen eines Objekts aus einem versionierten Bucket erstellt wird. Operationen an Buckets schließen dieses Feld nicht ein.
GFID	Grid Federation-Verbindungs-ID	Die Verbindungs-ID der Grid-Föderationsverbindung, die einer Grid-übergreifenden Replikationslöschanforderung zugeordnet ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation-Quellkonto-ID	Die Konto-ID des Mandanten im Quellraster für eine rasterübergreifende Replikationslöschanforderung. Nur in Prüfprotokollen im Zielraster enthalten.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). `` `x-amz-bypass-governance-retention`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist.
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der DELETE-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich

Code	Feld	Beschreibung
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SGRP	Site (Gruppe)	Falls vorhanden, wurde das Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das Objekt aufgenommen wurde.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.

Code	Feld	Beschreibung
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUDM	Universell eindeutige Kennung für eine Löschmarkierung	Die Kennung einer Löschmarkierung. In den Prüfprotokollmeldungen ist entweder UUDM oder UUID angegeben, wobei UUDM eine Löschmarkierung angibt, die als Ergebnis einer Objektlöschanforderung erstellt wurde, und UUID ein Objekt angibt.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, das gelöscht wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SGET: S3 GET

Wenn ein S3-Client eine GET-Transaktion ausgibt, wird eine Anforderung zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket oder zum Entfernen einer Bucket-/Objekt-Unterressource gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.

Code	Feld	Beschreibung
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
LITÄT	ListObjectsV2	Es wurde eine Antwort im *v2-Format* angefordert. Weitere Einzelheiten finden Sie unter "AWS ListObjectsV2" . Nur für GET-Bucket-Operationen.
NCHD	Anzahl der Kinder	Enthält Schlüssel und allgemeine Präfixe. Nur für GET-Bucket-Operationen.
RANG	Bereichsablesung	Nur für Bereichslesevorgänge. Gibt den Bytebereich an, der von dieser Anforderung gelesen wurde. Der Wert nach dem Schrägstrich (/) gibt die Größe des gesamten Objekts an.
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend.

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
Türkische Republik Nordzypern	Abgeschnitten oder nicht abgeschnitten	Auf „False“ setzen, wenn alle Ergebnisse zurückgegeben wurden. Auf „true“ setzen, wenn weitere Ergebnisse zur Rückgabe verfügbar sind. Nur für GET-Bucket-Operationen.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines angeforderten Objekts. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SHEA: S3 KOPF

Wenn ein S3-Client eine HEAD-Transaktion ausgibt, wird eine Anforderung gestellt, um die Existenz eines Objekts oder Buckets zu überprüfen und die Metadaten zu einem Objekt abzurufen. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des geprüften Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). ``
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines angeforderten Objekts. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SPOS: S3 POST

Wenn ein S3-Client eine POST-Objektanforderung ausgibt, wird diese Nachricht vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). (Für SPOS nicht zu erwarten).
RSLT	Ergebniscode	Ergebnis der RestoreObject-Anforderung. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend. Für einen S3-Auswahlvorgang auf „Auswählen“ einstellen.

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SRCF	Unterressourcenkonfiguration	Informationen wiederherstellen.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines angeforderten Objekts. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SPUT: S3 PUT

Wenn ein S3-Client eine PUT-Transaktion ausgibt, wird eine Anforderung zum Erstellen

eines neuen Objekts oder Buckets oder zum Entfernen einer Bucket-/Objekt-Unterressource gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CMPS	Compliance-Einstellungen	Die beim Erstellen des Buckets verwendeten Compliance-Einstellungen, sofern in der Anfrage vorhanden (auf die ersten 1024 Zeichen gekürzt).
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
GFID	Grid Federation-Verbindungs-ID	Die Verbindungs-ID der Grid-Föderationsverbindung, die einer PUT-Anforderung für die Grid-übergreifende Replikation zugeordnet ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation-Quellkonto-ID	Die Konto-ID des Mandanten im Quellraster für eine PUT-Anforderung zur rasterübergreifenden Replikation. Nur in Prüfprotokollen im Zielraster enthalten.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). `` `x-amz-bypass-governance-retention`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist.
LKEN	Objektsperre aktiviert	Wert des Anforderungsheaders `x-amz-bucket-object-lock-enabled` , falls in der Anfrage vorhanden.

Code	Feld	Beschreibung
LKLH	Objektsperre – Rechtliche Aufbewahrung	Wert des Anforderungsheaders `x-amz-object-lock-legal-hold` , falls in der PutObject-Anforderung vorhanden.
LKMD	Objektsperr-Aufbewahrungsmodus	Wert des Anforderungsheaders `x-amz-object-lock-mode` , falls in der PutObject-Anforderung vorhanden.
LKRU	Objektsperre – Aufbewahrung bis Datum	Wert des Anforderungsheaders `x-amz-object-lock-retain-until-date` , falls in der PutObject-Anforderung vorhanden. Die Werte sind auf einen Zeitraum von 100 Jahren ab dem Datum der Einnahme des Objekts begrenzt.
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.

Code	Feld	Beschreibung
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SRCF	Unterressourcenkonfiguration	Die neue Unterressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
ULID	ID hochladen	Nur in SPUT-Nachrichten für CompleteMultipartUpload-Vorgänge enthalten. Zeigt an, dass alle Teile hochgeladen und zusammengebaut wurden.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID eines neuen Objekts, das in einem versionierten Bucket erstellt wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.
VSST	Versionsstatus	Der neue Versionsstatus eines Buckets. Es werden zwei Zustände verwendet: „aktiviert“ oder „ausgesetzt“. Operationen an Objekten schließen dieses Feld nicht ein.

SREM: Objektspeicher entfernen

Diese Nachricht wird ausgegeben, wenn Inhalte aus dem permanenten Speicher entfernt werden und nicht mehr über reguläre APIs zugänglich sind.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des aus dem permanenten Speicher gelöschten Inhaltsblocks.
RSLT	Ergebniscode	Gibt das Ergebnis der Inhaltsentfernungsvorgänge an. Der einzige definierte Wert ist: SUCS: Inhalt aus dem persistenten Speicher entfernt

Diese Prüfmeldung bedeutet, dass ein bestimmter Inhaltsblock aus einem Knoten gelöscht wurde und nicht mehr direkt angefordert werden kann. Mithilfe der Nachricht kann der Fluss gelöschter Inhalte innerhalb des Systems verfolgt werden.

SUPD: S3-Metadaten aktualisiert

Diese Nachricht wird von der S3-API generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert. Die Meldung wird vom Server ausgegeben, wenn die Aktualisierung der Metadaten erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden, beim Aktualisieren der Compliance-Einstellungen eines Buckets.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). ``

Code	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer: SUCS: erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.

Code	Feld	Beschreibung
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SVRF: Objektspeicherüberprüfung fehlgeschlagen

Diese Meldung wird immer dann ausgegeben, wenn ein Inhaltsblock den Überprüfungsprozess nicht besteht. Jedes Mal, wenn replizierte Objektdaten von der Festplatte gelesen oder auf die Festplatte geschrieben werden, werden mehrere Überprüfungen und Integritätsprüfungen durchgeführt, um sicherzustellen, dass die an den anfordernden Benutzer gesendeten Daten mit den ursprünglich in das System aufgenommenen Daten identisch sind. Wenn eine dieser Prüfungen fehlschlägt, stellt das System die beschädigten replizierten Objektdaten automatisch unter Quarantäne, um zu verhindern, dass sie erneut abgerufen werden.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des Inhaltsblocks, dessen Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	Art des Überprüfungsfehlers: CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen. HMAC: Die Prüfung des Hash-basierten Nachrichtenauthentifizierungscodes (HMAC) ist fehlgeschlagen. EHSH: Unerwarteter Hash für verschlüsselten Inhalt. PHSH: Unerwarteter Hash des Originalinhalts. SEQC: Falsche Datensequenz auf der Festplatte. PERR: Ungültige Struktur der Datenträgerdatei. DERR: Festplattenfehler. FNAM: Ungültiger Dateiname.

Diese Nachricht sollte genau beobachtet werden. Fehler bei der Inhaltsüberprüfung können auf bevorstehende Hardwarefehler hinweisen.

Um festzustellen, welcher Vorgang die Nachricht ausgelöst hat, sehen Sie sich den Wert des AMID-Felds (Modul-ID) an. Beispielsweise gibt ein SVFY-Wert an, dass die Nachricht vom Storage Verifier-Modul generiert wurde, also durch Hintergrundüberprüfung, und STOR gibt an, dass die Nachricht durch Inhaltsabruf ausgelöst wurde.

SVRU: Object Store Verify Unbekannt

Die Speicherkomponente des LDR-Dienstes scannt kontinuierlich alle Kopien der replizierten Objektdaten im Objektspeicher. Diese Meldung wird ausgegeben, wenn eine unbekannte oder unerwartete Kopie replizierter Objektdaten im Objektspeicher erkannt und in das Quarantäneverzeichnis verschoben wird.

Code	Feld	Beschreibung
FPTH	Dateipfad	Der Dateipfad der unerwarteten Objektkopie.
RSLT	Ergebnis	Dieses Feld hat den Wert „NONE“. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird „NONE“ anstelle von „SUCS“ verwendet.

Die Prüfmeldung „SVRU: Object Store Verify Unknown“ sollte genau überwacht werden. Dies bedeutet, dass im Objektspeicher unerwartete Kopien von Objektdaten erkannt wurden. Diese Situation sollte sofort untersucht werden, um festzustellen, wie diese Kopien erstellt wurden, da dies auf bevorstehende Hardwarefehler hinweisen kann.

SYSD: Knotenstopp

Wenn ein Dienst ordnungsgemäß beendet wird, wird diese Meldung generiert, um anzuzeigen, dass das Herunterfahren angefordert wurde. Normalerweise wird diese Nachricht erst nach einem anschließenden Neustart gesendet, da die Warteschlange der Prüfnachrichten vor dem Herunterfahren nicht gelöscht wird. Suchen Sie nach der SYST-Nachricht, die zu Beginn der Herunterfahrsequenz gesendet wurde, wenn der Dienst nicht neu gestartet wurde.

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Die Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren.

Die Meldung gibt nicht an, ob der Hostserver gestoppt wird, sondern nur der Berichtsdienst. Das RSLT eines SYSD kann kein „schmutziges“ Herunterfahren anzeigen, da die Meldung nur bei „sauberen“ Herunterfahren generiert wird.

SYST: Knoten wird gestoppt

Wenn ein Dienst ordnungsgemäß beendet wird, wird diese Meldung generiert, um anzuzeigen, dass das Herunterfahren angefordert wurde und dass der Dienst seine Herunterfahrsequenz eingeleitet hat. Mit SYST kann ermittelt werden, ob das Herunterfahren angefordert wurde, bevor der Dienst neu gestartet wird (im Gegensatz zu SYSD, das normalerweise nach dem Neustart des Dienstes gesendet wird).

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Die Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren.

Die Meldung gibt nicht an, ob der Hostserver gestoppt wird, sondern nur der Berichtsdienst. Der RSLT-Code einer SYST-Nachricht kann kein „schmutziges“ Herunterfahren anzeigen, da die Nachricht nur bei „sauberen“ Herunterfahren generiert wird.

SYSU: Knotenstart

Wenn ein Dienst neu gestartet wird, wird diese Meldung generiert, um anzuzeigen, ob das vorherige Herunterfahren sauber (befohlen) oder ungeordnet (unerwartet) war.

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Die Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren. DSDN: Das System wurde nicht sauber heruntergefahren. VRGN: Das System wurde nach der Serverinstallation (oder Neuinstallation) zum ersten Mal gestartet.

Die Meldung gibt nicht an, ob der Hostserver gestartet wurde, sondern nur, ob der Berichtsdienst gestartet wurde. Diese Nachricht kann verwendet werden, um:

- Erkennen Sie Diskontinuitäten im Prüfpfad.
- Stellen Sie fest, ob ein Dienst während des Betriebs ausfällt (da die verteilte Natur des StorageGRID -Systems diese Ausfälle maskieren kann). Der Server Manager startet einen ausgefallenen Dienst automatisch neu.

WDEL: Schnelles LÖSCHEN

Wenn ein Swift-Client eine DELETE-Transaktion ausgibt, wird eine Anforderung zum Entfernen des angegebenen Objekts oder Containers gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Bytes. Vorgänge an Containern umfassen dieses Feld nicht.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der DELETE-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SGRP	Site (Gruppe)	Falls vorhanden, wurde das Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das Objekt aufgenommen wurde.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.

Code	Feld	Beschreibung
WCON	Schneller Container	Der Name des Swift-Containers.
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.

WGET: Schnelles GET

Wenn ein Swift-Client eine GET-Transaktion ausgibt, wird eine Anforderung zum Abrufen eines Objekts, zum Auflisten der Objekte in einem Container oder zum Auflisten der Container in einem Konto gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer SUCS: erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.

Code	Feld	Beschreibung
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.
WCON	Schneller Container	Der Name des Swift-Containers. Bei Vorgängen mit Konten ist dieses Feld nicht enthalten.
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.

WHEA: Schneller Kopf

Wenn ein Swift-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, um die Existenz eines Kontos, Containers oder Objekts zu überprüfen und alle relevanten Metadaten abzurufen. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Vorgänge an Konten und Containern umfassen dieses Feld nicht.

Code	Feld	Beschreibung
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
RSLT	Ergebniscode	Ergebnis der HEAD-Transaktion. Ergebnis ist immer: SUCS: erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.
WCON	Schneller Container	Der Name des Swift-Containers. Bei Vorgängen mit Konten ist dieses Feld nicht enthalten.
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.

WPUT: Schnelles PUT

Wenn ein Swift-Client eine PUT-Transaktion ausgibt, wird eine Anforderung zum Erstellen eines neuen Objekts oder Containers gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Vorgänge an Containern umfassen dieses Feld nicht.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Ergebnis ist immer: SUCS: erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.
WCON	Schneller Container	Der Name des Swift-Containers.

Code	Feld	Beschreibung
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.

Erweitern eines Rasters

Erweiterungstypen

Sie können die Kapazität oder Funktionen Ihres StorageGRID -Systems erweitern, ohne den Systembetrieb zu unterbrechen.

Mit einer StorageGRID -Erweiterung können Sie Folgendes hinzufügen:

- Speichervolumes zu Speicherknoten
- Neue Grid-Knoten zu einer bestehenden Site
- Eine völlig neue Site

Der Grund für die Erweiterung bestimmt, wie viele neue Knoten jedes Typs Sie hinzufügen müssen und wo sich diese neuen Knoten befinden. Beispielsweise gelten andere Knotenanforderungen, wenn Sie eine Erweiterung durchführen, um die Speicherkapazität zu erhöhen, Metadatenkapazität hinzuzufügen oder Redundanz oder neue Funktionen hinzuzufügen.

Befolgen Sie die Schritte für die Art der Erweiterung, die Sie durchführen:

Speichervolumes hinzufügen

Befolgen Sie die Schritte für"Hinzufügen von Speichervolumes zu Speicherknoten" .

Rasterknoten hinzufügen

1. Befolgen Sie die Schritte für"Hinzufügen von Rasterknoten zu einer vorhandenen Site" .
2. "Aktualisieren der Subnetze" .
3. Grid-Knoten bereitstellen:
   - "Geräte"
   - "VMware"
   - "Linux"

   > ⓘ „Linux“ bezieht sich auf eine Bereitstellung von Red Hat Enterprise Linux, Ubuntu oder Debian. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

4. "Führen Sie die Erweiterung durch" .
5. "Konfigurieren Sie das erweiterte System" .

Neue Site hinzufügen

1. Befolgen Sie die Schritte für"Hinzufügen einer neuen Site" .
2. "Aktualisieren der Subnetze" .
3. Grid-Knoten bereitstellen:
   - "Geräte"
   - "VMware"
   - "Linux"

   > ⓘ „Linux“ bezieht sich auf eine Bereitstellung von Red Hat Enterprise Linux, Ubuntu oder Debian. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

4. "Führen Sie die Erweiterung durch" .
5. "Konfigurieren Sie das erweiterte System" .

StorageGRID Erweiterung planen

Speicherkapazität hinzufügen

Richtlinien zum Hinzufügen von Objektkapazität

Sie können die Objektspeicherkapazität Ihres StorageGRID -Systems erweitern, indem Sie Speichervolumes zu vorhandenen Speicherknoten hinzufügen oder neue Speicherknoten zu vorhandenen Sites hinzufügen. Sie müssen die Speicherkapazität so hinzufügen, dass sie den Anforderungen Ihrer ILM-Richtlinie (Information Lifecycle

Management) entspricht.

Richtlinien zum Hinzufügen von Speichervolumes

Bevor Sie Speichervolumes zu vorhandenen Speicherknoten hinzufügen, lesen Sie die folgenden Richtlinien und Einschränkungen:

- Sie müssen Ihre aktuellen ILM-Regeln prüfen, um festzustellen, wo und wann"Speichervolumes hinzufügen" um den verfügbaren Speicherplatz zu erhöhen für"replizierte Objekte" oder"Erasure-Codierte Objekte" .
- Sie können die Metadatenkapazität Ihres Systems nicht durch Hinzufügen von Speichervolumes erhöhen, da Objektmetadaten nur auf Volume 0 gespeichert werden.
- Jeder softwarebasierte Speicherknoten kann maximal 48 Speichervolumes unterstützen. Wenn Sie darüber hinaus Kapazität hinzufügen müssen, müssen Sie neue Speicherknoten hinzufügen.
- Sie können jedem SG6060-Gerät ein oder zwei Erweiterungsregale hinzufügen. Jedes Erweiterungsregal fügt 16 Speichervolumes hinzu. Wenn beide Erweiterungsfächer installiert sind, kann das SG6060 insgesamt 48 Speichervolumes unterstützen.
- Sie können jedem SG6160-Gerät ein oder zwei Erweiterungsregale hinzufügen. Jedes Erweiterungsregal fügt 60 Speichervolumes hinzu. Wenn beide Erweiterungsregale installiert sind, kann das SG6160 insgesamt 180 Speichervolumes unterstützen.
- Sie können keinem anderen Speichergerät Speichervolumes hinzufügen.
- Sie können die Größe eines vorhandenen Speichervolumens nicht erhöhen.
- Sie können einem Speicherknoten keine Speichervolumes hinzufügen, während Sie gleichzeitig ein Systemupgrade, eine Wiederherstellungsoperation oder eine andere Erweiterung durchführen.

Nachdem Sie sich entschieden haben, Speichervolumes hinzuzufügen und ermittelt haben, welche Speicherknoten Sie erweitern müssen, um Ihre ILM-Richtlinie zu erfüllen, folgen Sie den Anweisungen für Ihren Speicherknotentyp:

- Um ein oder zwei Erweiterungsregale zu einem SG6060-Speichergerät hinzuzufügen, gehen Sie zu "Erweiterungsfach zum bereitgestellten SG6060 hinzufügen" .
- Um ein oder zwei Erweiterungsregale zu einem SG6160-Speichergerät hinzuzufügen, gehen Sie zu "Erweiterungsfach zum bereitgestellten SG6160 hinzufügen"
- Für einen softwarebasierten Knoten folgen Sie den Anweisungen für"Hinzufügen von Speichervolumes zu Speicherknoten" .

Richtlinien zum Hinzufügen von Speicherknoten

Bevor Sie Speicherknoten zu vorhandenen Sites hinzufügen, lesen Sie die folgenden Richtlinien und Einschränkungen:

- Sie müssen Ihre aktuellen ILM-Regeln prüfen, um zu bestimmen, wo und wann Sie Speicherknoten hinzufügen müssen, um den verfügbaren Speicher für"replizierte Objekte" oder"Erasure-Codierte Objekte" .
- Sie sollten in einem einzigen Erweiterungsvorgang nicht mehr als 10 Speicherknoten hinzufügen.
- Sie können Speicherknoten in einem einzigen Erweiterungsvorgang zu mehreren Standorten hinzufügen.
- Sie können Speicherknoten und andere Knotentypen in einem einzigen Erweiterungsvorgang hinzufügen.
- Bevor Sie mit dem Erweiterungsvorgang beginnen, müssen Sie bestätigen, dass alle im Rahmen einer Wiederherstellung durchgeführten Datenreparaturvorgänge abgeschlossen sind. Sehen "Überprüfen Sie

die Datenreparaturaufträge" .

- Wenn Sie vor oder nach einer Erweiterung Speicherknoten entfernen müssen, sollten Sie in einem einzigen Vorgang zum Außerbetriebsetzen von Knoten nicht mehr als 10 Speicherknoten außer Betrieb nehmen.

Richtlinien für den ADC-Dienst auf Speicherknoten

Beim Konfigurieren der Erweiterung müssen Sie auswählen, ob der Dienst „Administrative Domain Controller“ (ADC) auf jedem neuen Speicherknoten enthalten sein soll. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Diensten.

- Das StorageGRID -System erfordert eine"Quorum der ADC-Dienste" an jedem Standort und jederzeit verfügbar zu sein.
- Mindestens drei Speicherknoten an jedem Standort müssen den ADC-Dienst enthalten.
- Es wird nicht empfohlen, den ADC-Dienst zu jedem Speicherknoten hinzuzufügen. Die Einbeziehung zu vieler ADC-Dienste kann aufgrund der erhöhten Kommunikationsmenge zwischen den Knoten zu Verlangsamungen führen.
- Ein einzelnes Grid sollte nicht mehr als 48 Speicherknoten mit dem ADC-Dienst haben. Dies entspricht 16 Standorten mit jeweils drei ADC-Diensten.
- Wenn Sie die Einstellung **ADC-Dienst** für einen neuen Knoten auswählen, sollten Sie im Allgemeinen **Automatisch** auswählen. Wählen Sie **Ja** nur, wenn der neue Knoten einen anderen Speicherknoten ersetzt, der den ADC-Dienst enthält. Da Sie einen Speicherknoten nicht außer Betrieb nehmen können, wenn zu wenige ADC-Dienste übrig bleiben, wird dadurch sichergestellt, dass ein neuer ADC-Dienst verfügbar ist, bevor der alte Dienst entfernt wird.
- Sie können den ADC-Dienst nach der Bereitstellung nicht mehr zu einem Knoten hinzufügen.

Speicherkapazität für replizierte Objekte hinzufügen

Wenn die Richtlinie für das Information Lifecycle Management (ILM) Ihrer Bereitstellung eine Regel zum Erstellen replizierter Kopien von Objekten enthält, müssen Sie überlegen, wie viel Speicher Sie hinzufügen und wo Sie die neuen Speichervolumes oder Speicherknoten hinzufügen.

Hinweise dazu, wo zusätzlicher Speicher hinzugefügt werden kann, finden Sie in den ILM-Regeln zum Erstellen replizierter Kopien. Wenn durch ILM-Regeln zwei oder mehr Objektkopien erstellt werden, planen Sie, an jedem Standort, an dem Objektkopien erstellt werden, zusätzlichen Speicher hinzuzufügen. Ein einfaches Beispiel: Wenn Sie ein Grid mit zwei Sites haben und eine ILM-Regel, die an jeder Site eine Objektkopie erstellt, müssen Sie"Speicher hinzufügen" zu jedem Standort, um die Gesamtobjektkapazität des Netzes zu erhöhen. Informationen zur Objektreplikation finden Sie unter"Was ist Replikation?" .

Aus Leistungsgründen sollten Sie versuchen, die Speicherkapazität und Rechenleistung zwischen den Standorten auszugleichen. Für dieses Beispiel sollten Sie also jedem Standort die gleiche Anzahl an Speicherknoten oder zusätzliche Speichervolumes hinzufügen.

Wenn Sie über eine komplexere ILM-Richtlinie verfügen, die Regeln enthält, die Objekte basierend auf Kriterien wie dem Bucket-Namen an verschiedenen Speicherorten platzieren, oder Regeln, die Objektspeicherorte im Laufe der Zeit ändern, ist Ihre Analyse, wo Speicher für die Erweiterung erforderlich ist, ähnlich, aber komplexer.

Durch die Aufzeichnung der Geschwindigkeit, mit der die gesamte Speicherkapazität verbraucht wird, können Sie besser einschätzen, wie viel Speicher Sie bei der Erweiterung hinzufügen müssen und wann der

zusätzliche Speicherplatz benötigt wird. Mit dem Grid Manager können Sie"Monitor- und Diagrammspeicherkapazität" .

Denken Sie bei der Planung des Zeitpunkts einer Erweiterung daran, wie lange die Beschaffung und Installation von zusätzlichem Speicher dauern könnte.

Speicherkapazität für Erasure-Coded-Objekte hinzufügen

Wenn Ihre ILM-Richtlinie eine Regel zum Erstellen von Erasure-Coded-Kopien enthält, müssen Sie planen, wo und wann neuer Speicher hinzugefügt werden soll. Die Menge des hinzugefügten Speichers und der Zeitpunkt der Hinzufügung können sich auf die nutzbare Speicherkapazität des Netzes auswirken.

Der erste Schritt bei der Planung einer Speichererweiterung besteht darin, die Regeln in Ihrer ILM-Richtlinie zu untersuchen, die Erasure-Coded-Objekte erstellen. Da StorageGRID für jedes Erasure-Codierte-Objekt *k+m* Fragmente erstellt und jedes Fragment auf einem anderen Speicherknoten speichert, müssen Sie sicherstellen, dass nach der Erweiterung mindestens *k+m* Speicherknoten Platz für neue Erasure-Codierte-Daten haben. Wenn das Erasure-Coding-Profil Schutz vor Site-Verlust bietet, müssen Sie jedem Site Speicher hinzufügen. Sehen"Was sind Erasure-Coding-Schemata?" für Informationen zu Erasure-Coding-Profilen.

Die Anzahl der hinzuzufügenden Knoten hängt auch davon ab, wie voll die vorhandenen Knoten sind, wenn Sie die Erweiterung durchführen.

Allgemeine Empfehlung zum Hinzufügen von Speicherkapazität für Erasure-Coded-Objekte

Wenn Sie detaillierte Berechnungen vermeiden möchten, können Sie zwei Speicherknoten pro Site hinzufügen, wenn die vorhandenen Speicherknoten 70 % ihrer Kapazität erreichen.

Diese allgemeine Empfehlung liefert angemessene Ergebnisse für eine breite Palette von Erasure-Coding-Schemata sowohl für Einzelstandort-Grids als auch für Grids, bei denen Erasure Coding Schutz vor Standortverlust bietet.

Um die Faktoren, die zu dieser Empfehlung geführt haben, besser zu verstehen oder einen präziseren Plan für Ihre Site zu entwickeln, lesen Sie"Überlegungen zum Neuausgleich von Erasure-Coded-Daten" . Wenden Sie sich an Ihren NetApp Professional Services-Berater, um eine individuelle, auf Ihre Situation optimierte Empfehlung zu erhalten.

Überlegungen zum Neuausgleich von Erasure-Coded-Daten

Wenn Sie eine Erweiterung durchführen, um Speicherknoten hinzuzufügen, und ILM-Regeln zum Löschen von Codedaten verwenden, müssen Sie möglicherweise das Neuausgleichsverfahren für die Löschcodierung (EC) durchführen, wenn Sie nicht genügend Speicherknoten für das von Ihnen verwendete Löschcodierungsschema hinzufügen können.

Nachdem Sie diese Überlegungen überprüft haben, führen Sie die Erweiterung durch und gehen Sie dann zu"Neuausgleich von erasure-coded Daten nach dem Hinzufügen von Speicherknoten" um die Prozedur auszuführen.

Was ist EC-Rebalancing?

EC-Rebalancing ist ein StorageGRID -Verfahren, das nach einer Storage Node-Erweiterung erforderlich sein kann. Das Verfahren wird als Befehlszeilenskript vom primären Admin-Knoten aus ausgeführt. Wenn Sie das

EC-Neuausgleichsverfahren ausführen, verteilt StorageGRID Erasure-Coded-Fragmente unter den vorhandenen und den neu hinzugefügten Speicherknoten an einem Standort neu.

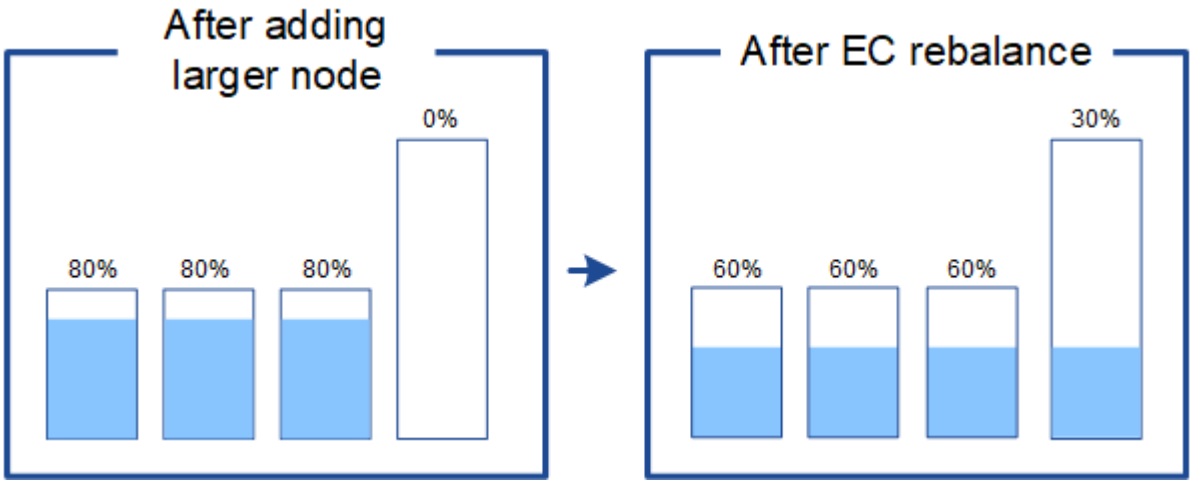
Das Verfahren zur Neugewichtung der EG:

- Verschiebt nur löschcodierte Objektdaten. Es werden keine replizierten Objektdaten verschoben.
- Verteilt die Daten innerhalb einer Site neu. Es werden keine Daten zwischen Standorten verschoben.
- Verteilt Daten auf alle Speicherknoten an einem Standort neu. Es werden keine Daten innerhalb von Speichervolumes neu verteilt.
- Berücksichtigt bei der Bestimmung, wohin die löschcodierten Daten verschoben werden sollen, nicht die replizierte Datennutzung auf jedem Speicherknoten.
- Verteilt löschcodierte Daten gleichmäßig zwischen Speicherknoten, ohne die relativen Kapazitäten der einzelnen Knoten zu berücksichtigen.
- Verteilt keine erasure-coded Daten an Speicherknoten, die zu mehr als 80 % voll sind.
- Kann die Leistung von ILM-Operationen und S3-Client-Operationen während der Ausführung beeinträchtigen. Für die Neuverteilung der Erasure-Coding-Fragmente sind zusätzliche Ressourcen erforderlich.

Wenn der EC-Neuausgleichsvorgang abgeschlossen ist:

- Löschcodierte Daten werden von Speicherknoten mit weniger verfügbarem Speicherplatz auf Speicherknoten mit mehr verfügbarem Speicherplatz verschoben.
- Der Datenschutz von Erasure-Coded-Objekten bleibt unverändert.
- Die Werte für „Verwendet (%)“ können zwischen Speicherknoten aus zwei Gründen unterschiedlich sein:
  - Replizierte Objektkopien belegen weiterhin Speicherplatz auf den vorhandenen Knoten – das EC-Neuausgleichsverfahren verschiebt keine replizierten Daten.
  - Knoten mit größerer Kapazität sind relativ weniger voll als Knoten mit kleinerer Kapazität, obwohl alle Knoten am Ende ungefähr die gleiche Menge an Erasure-Codierten Daten enthalten.

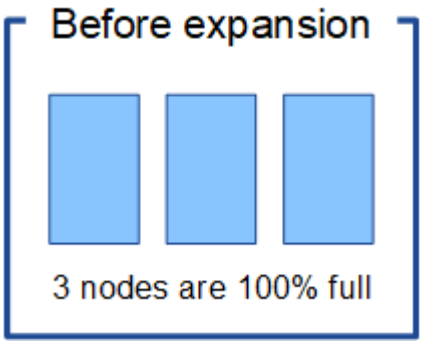
    Nehmen wir beispielsweise an, dass drei 200-TB-Knoten jeweils zu 80 % gefüllt sind (200 × 0,8 = 160 TB auf jedem Knoten oder 480 TB für die Site). Wenn Sie einen 400-TB-Knoten hinzufügen und das Neuausgleichsverfahren ausführen, verfügen alle Knoten nun über ungefähr die gleiche Menge an Erasure-Code-Daten (480/4 = 120 TB). Allerdings ist der Wert für „Verwendet (%)“ für den größeren Knoten geringer als der Wert für „Verwendet (%)“ für die kleineren Knoten.



Wann sollten Erasure-Codierte Daten neu ausgeglichen werden?

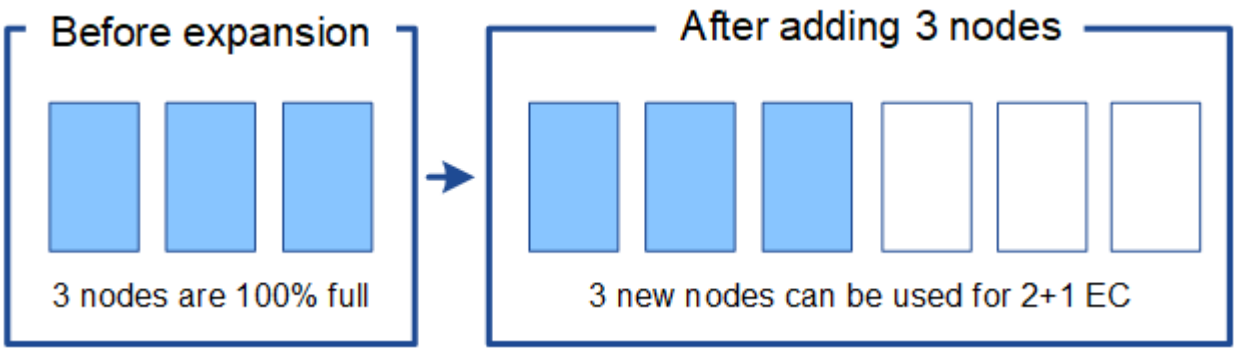
Stellen Sie sich folgendes Szenario vor:

- StorageGRID wird an einem einzelnen Standort ausgeführt, der drei Speicherknoten enthält.
- Die ILM-Richtlinie verwendet eine 2+1-Erasure-Coding-Regel für alle Objekte, die größer als 1,0 MB sind, und eine 2-Kopien-Replikationsregel für kleinere Objekte.
- Alle Speicherknoten sind vollständig belegt. Die Warnung **Niedriger Objektspeicher** wurde mit dem Schweregrad „Schwer“ ausgelöst.



Eine Neuverteilung ist nicht erforderlich, wenn Sie genügend Knoten hinzufügen

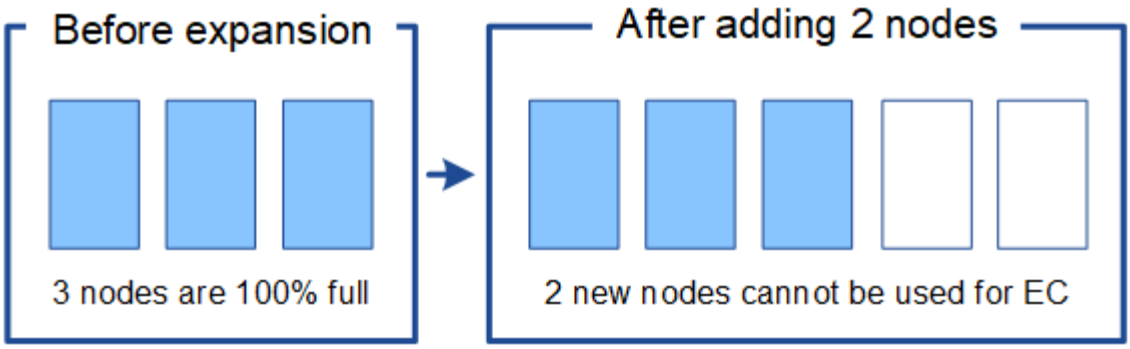
Um zu verstehen, wann keine EC-Neuverteilung erforderlich ist, nehmen wir an, Sie haben drei (oder mehr) neue Speicherknoten hinzugefügt. In diesem Fall müssen Sie keine EC-Neugewichtung durchführen. Die ursprünglichen Speicherknoten bleiben voll, aber neue Objekte verwenden jetzt die drei neuen Knoten für 2+1-Löschcodierung – die beiden Datenfragmente und das eine Paritätsfragment können jeweils auf einem anderen Knoten gespeichert werden.



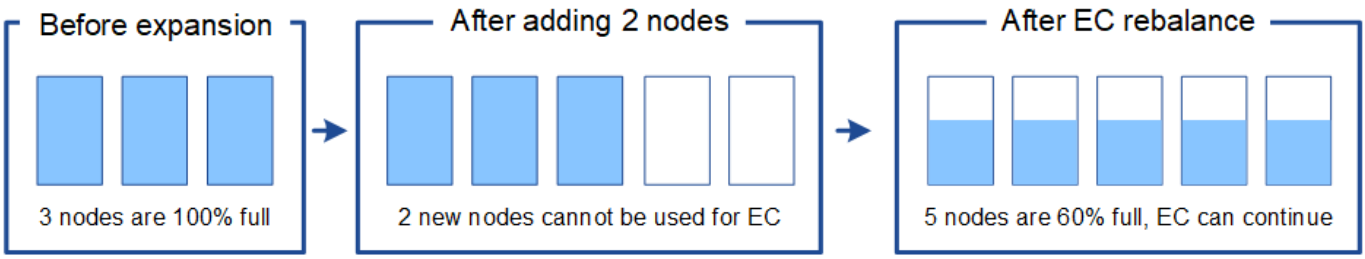
> Obwohl Sie in diesem Fall das EC-Neuausgleichsverfahren ausführen können, wird durch das Verschieben der vorhandenen Erasure-Coded-Daten die Leistung des Grids vorübergehend verringert, was sich auf den Clientbetrieb auswirken kann.

Eine Neuverteilung ist erforderlich, wenn Sie nicht genügend Knoten hinzufügen können

Um zu verstehen, wann eine EC-Neuausrichtung erforderlich ist, nehmen Sie an, dass Sie nur zwei statt drei Speicherknoten hinzufügen können. Da für das 2+1-Schema mindestens drei Speicherknoten über freien Speicherplatz verfügen müssen, können die leeren Knoten nicht für neue erasure-coded Daten verwendet werden.



Um die neuen Speicherknoten zu nutzen, sollten Sie das EC-Neuausgleichsverfahren ausführen. Wenn dieser Vorgang ausgeführt wird, verteilt StorageGRID vorhandene erasure-coded Daten und Paritätsfragmente auf alle Speicherknoten am Standort neu. In diesem Beispiel sind nach Abschluss des EC-Neuausgleichsvorgangs alle fünf Knoten nur noch zu 60 % gefüllt und Objekte können weiterhin in das 2+1-Erasure-Coding-Schema auf allen Speicherknoten aufgenommen werden.



Empfehlungen zur Neuausrichtung der EG

NetApp erfordert eine EC-Neuausrichtung, wenn *alle* der folgenden Aussagen zutreffen:

- Sie verwenden Erasure Coding für Ihre Objektdaten.
- Für einen oder mehrere Speicherknoten an einem Standort wurde die Warnung „Wenig Objektspeicher“ ausgelöst, die darauf hinweist, dass die Knoten zu 80 % oder mehr belegt sind.
- Sie können nicht genügend neue Speicherknoten für das verwendete Erasure-Coding-Schema hinzufügen. Sehen "Speicherkapazität für Erasure-Coded-Objekte hinzufügen" .
- Ihre S3-Clients können eine geringere Leistung bei ihren Schreib- und Lesevorgängen tolerieren, während das EC-Neuausgleichsverfahren ausgeführt wird.

Sie können das EC-Neuausgleichsverfahren optional ausführen, wenn Sie es vorziehen, dass die Speicherknoten auf einem ähnlichen Niveau gefüllt werden und Ihre S3-Clients eine geringere Leistung für ihre Schreib- und Lesevorgänge tolerieren können, während das EC-Neuausgleichsverfahren ausgeführt wird.

Wie das EC-Neuausgleichsverfahren mit anderen Wartungsaufgaben interagiert

Sie können bestimmte Wartungsvorgänge nicht gleichzeitig mit dem EC-Neuausgleichsverfahren durchführen.

Verfahren	Während des EC-Neuausgleichsverfahrens zulässig?
Zusätzliche Verfahren zur Neugewichtung der EG	NEIN. Sie können jeweils nur einen EC-Neuausgleichsvorgang ausführen.

Verfahren	Während des EC-Neuausgleichsverfahrens zulässig?
Außerbetriebnahmeverfahren EC-Datenreparaturauftrag	NEIN. • Während der EC-Neuausgleich läuft, können Sie keinen Außerbetriebnahmevorgang oder keine EC-Datenreparatur starten. • Sie können den EC-Neuausgleichsvorgang nicht starten, während ein Verfahren zur Außerbetriebnahme eines Speicherknotens oder eine EC-Datenreparatur ausgeführt wird.
Erweiterungsverfahren	NEIN. Wenn Sie in einer Erweiterung neue Speicherknoten hinzufügen müssen, führen Sie nach dem Hinzufügen aller neuen Knoten das EC-Neuausgleichsverfahren aus.
Upgrade-Verfahren	NEIN. Wenn Sie die StorageGRID -Software aktualisieren müssen, führen Sie den Aktualisierungsvorgang vor oder nach dem Ausführen des EC-Neuausgleichsverfahrens durch. Bei Bedarf können Sie den EC-Neuausgleichsvorgang beenden, um ein Software-Upgrade durchzuführen.
Verfahren zum Klonen von Appliance-Knoten	NEIN. Wenn Sie einen Appliance-Speicherknoten klonen müssen, führen Sie nach dem Hinzufügen des neuen Knotens das EC-Neuausgleichsverfahren aus.
Hotfix-Verfahren	Ja. Sie können einen StorageGRID Hotfix anwenden, während der EC-Neuausgleichsvorgang ausgeführt wird.
Andere Wartungsverfahren	NEIN. Sie müssen das EC-Neuausgleichsverfahren beenden, bevor Sie andere Wartungsvorgänge ausführen.

Wie das EC-Neuausgleichsverfahren mit ILM interagiert

Vermeiden Sie während der Ausführung des EC-Neuausgleichsverfahrens ILM-Änderungen, die den Speicherort vorhandener Erasure-Coded-Objekte ändern könnten. Beginnen Sie beispielsweise nicht mit der Verwendung einer ILM-Regel, die ein anderes Erasure-Coding-Profil hat. Wenn Sie solche ILM-Änderungen vornehmen müssen, sollten Sie das EC-Neuausgleichsverfahren beenden.

Metadatenkapazität hinzufügen

Um sicherzustellen, dass ausreichend Speicherplatz für Objektmetadaten zur Verfügung steht, müssen Sie möglicherweise einen Erweiterungsvorgang durchführen, um an jedem

Standort neue Speicherknoten hinzuzufügen.

StorageGRID reserviert Speicherplatz für Objektmetadaten auf Volume 0 jedes Speicherknotens. An jedem Standort werden drei Kopien aller Objektmetadaten verwaltet, gleichmäßig verteilt auf alle Speicherknoten.

Mit dem Grid Manager können Sie die Metadatenkapazität von Speicherknoten überwachen und abschätzen, wie schnell die Metadatenkapazität verbraucht wird. Darüber hinaus wird für einen Speicherknoten die Warnung **Geringer Metadatenspeicher** ausgelöst, wenn der verwendete Metadatenspeicher bestimmte Schwellenwerte erreicht.

Beachten Sie, dass die Objektmetadatenkapazität eines Grids je nach Verwendung des Grids möglicherweise schneller verbraucht wird als seine Objektspeicherkapazität. Wenn Sie beispielsweise normalerweise eine große Anzahl kleiner Objekte aufnehmen oder Objekten große Mengen an Benutzermetadaten oder Tags hinzufügen, müssen Sie möglicherweise Speicherknoten hinzufügen, um die Metadatenkapazität zu erhöhen, obwohl noch ausreichend Objektspeicherkapazität vorhanden ist.

Weitere Informationen finden Sie unter:

- "Verwalten des Objektmetadatenspeichers"
- "Überwachen Sie die Objektmetadatenkapazität für jeden Speicherknoten"

Richtlinien zur Erhöhung der Metadatenkapazität

Bevor Sie Speicherknoten hinzufügen, um die Metadatenkapazität zu erhöhen, lesen Sie die folgenden Richtlinien und Einschränkungen:

- Vorausgesetzt, es steht ausreichend Objektspeicherkapazität zur Verfügung, erhöht mehr Speicherplatz für Objektmetadaten die Anzahl der Objekte, die Sie in Ihrem StorageGRID System speichern können.
- Sie können die Metadatenkapazität eines Grids erhöhen, indem Sie jedem Standort einen oder mehrere Speicherknoten hinzufügen.
- Der tatsächliche Speicherplatz, der für Objektmetadaten auf einem bestimmten Speicherknoten reserviert ist, hängt von der Speicheroption „Reservierter Speicherplatz für Metadaten“ (systemweite Einstellung), der dem Knoten zugewiesenen RAM-Menge und der Größe des Volumes 0 des Knotens ab.
- Sie können die Metadatenkapazität nicht erhöhen, indem Sie Speichervolumes zu vorhandenen Speicherknoten hinzufügen, da Metadaten nur auf Volume 0 gespeichert werden.
- Sie können die Metadatenkapazität nicht durch Hinzufügen einer neuen Site erhöhen.
- StorageGRID speichert an jedem Standort drei Kopien aller Objektmetadaten. Aus diesem Grund ist die Metadatenkapazität Ihres Systems durch die Metadatenkapazität Ihrer kleinsten Site begrenzt.
- Wenn Sie die Metadatenkapazität erweitern, sollten Sie jeder Site die gleiche Anzahl von Speicherknoten hinzufügen.

Für reine Metadaten-Speicherknoten gelten bestimmte Hardwareanforderungen:

- Bei Verwendung von StorageGRID -Geräten können reine Metadatenknoten nur auf SGF6112-Geräten mit zwölf 1,9-TB- oder zwölf 3,8-TB-Laufwerken konfiguriert werden.
- Bei der Verwendung softwarebasierter Knoten müssen die Knotenressourcen, die nur Metadaten enthalten, mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:
  - Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
    - 128 GB RAM

        - 8-Kern-CPU
        - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)
    - Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).
- Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

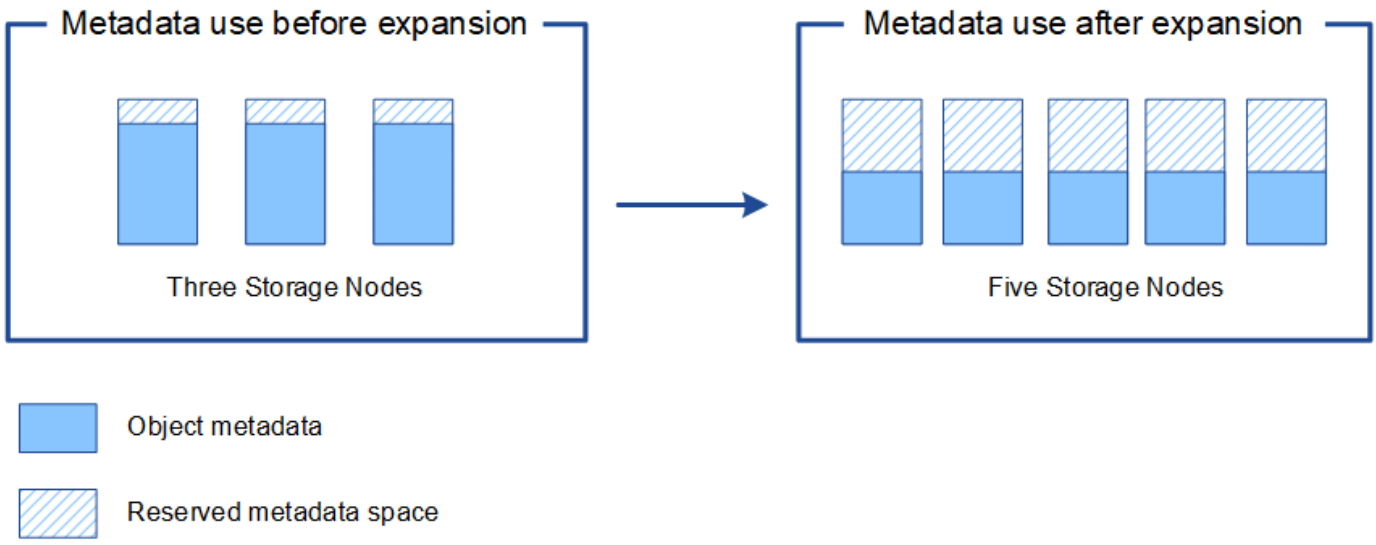
Siehe die"Beschreibung, was Metadata Reserved Space ist" .

So werden Metadaten neu verteilt, wenn Sie Speicherknoten hinzufügen

Wenn Sie in einer Erweiterung Speicherknoten hinzufügen, verteilt StorageGRID die vorhandenen Objektmetadaten an die neuen Knoten an jedem Standort neu, wodurch die Gesamtmetadatenkapazität des Grids erhöht wird. Es ist keine Benutzeraktion erforderlich.

Die folgende Abbildung zeigt, wie StorageGRID Objektmetadaten neu verteilt, wenn Sie Storage Nodes in einer Erweiterung hinzufügen. Die linke Seite der Abbildung stellt Volume 0 von drei Speicherknoten vor einer Erweiterung dar. Metadaten belegen einen relativ großen Teil des verfügbaren Metadatenspeichers jedes Knotens und die Warnung **Geringer Metadatenspeicher** wurde ausgelöst.

Die rechte Seite der Abbildung zeigt, wie die vorhandenen Metadaten neu verteilt werden, nachdem der Site zwei Speicherknoten hinzugefügt wurden. Die Menge der Metadaten auf jedem Knoten hat abgenommen, die Warnung „Geringer Metadatenspeicher“ wird nicht mehr ausgelöst und der für Metadaten verfügbare Speicherplatz hat zugenommen.



Fügen Sie Grid-Knoten hinzu, um Ihrem System Funktionen hinzuzufügen

Sie können einem StorageGRID -System Redundanz oder zusätzliche Funktionen hinzufügen, indem Sie vorhandenen Sites neue Grid-Knoten hinzufügen.

Sie können beispielsweise Gateway-Knoten zur Verwendung in einer Hochverfügbarkeitsgruppe (HA) hinzufügen oder einen Admin-Knoten an einem Remote-Standort hinzufügen, um die Überwachung mithilfe eines lokalen Knotens zu ermöglichen.

Sie können in einem einzigen Erweiterungsvorgang einen oder mehrere der folgenden Knotentypen zu einer oder mehreren vorhandenen Sites hinzufügen:

- Nicht-primäre Admin-Knoten
- Speicherknoten
- Gateway-Knoten

Beachten Sie beim Hinzufügen von Rasterknoten die folgenden Einschränkungen:

- Der primäre Admin-Knoten wird während der Erstinstallation bereitgestellt. Sie können während einer Erweiterung keinen primären Admin-Knoten hinzufügen.
- Sie können Speicherknoten und andere Knotentypen in derselben Erweiterung hinzufügen.
- Beim Hinzufügen von Speicherknoten müssen Sie die Anzahl und den Standort der neuen Knoten sorgfältig planen. Sehen "Richtlinien zum Hinzufügen von Objektkapazität" .
- Wenn die Option **Neuen Knotenstandard festlegen** auf der Registerkarte „Nicht vertrauenswürdige Client-Netzwerke“ der Seite „Firewall-Steuerung“ auf „Nicht vertrauenswürdig“ gesetzt ist, müssen Client-Anwendungen, die über das Client-Netzwerk eine Verbindung zu Erweiterungsknoten herstellen, die Verbindung über einen Endpunktport des Lastenausgleichs herstellen (**KONFIGURATION** > **Sicherheit** > **Firewall-Steuerung**). Siehe die Anweisungen zu"Ändern Sie die Sicherheitseinstellungen für den neuen Knoten" und zu"Konfigurieren Sie Load Balancer-Endpunkte" .

Hinzufügen einer neuen Site

Sie können Ihr StorageGRID -System erweitern, indem Sie eine neue Site hinzufügen.

Richtlinien zum Hinzufügen einer Site

Überprüfen Sie vor dem Hinzufügen einer Site die folgenden Anforderungen und Einschränkungen:

- Sie können pro Erweiterungsvorgang nur eine Site hinzufügen.
- Sie können einer vorhandenen Site im Rahmen derselben Erweiterung keine Rasterknoten hinzufügen.
- Alle Sites müssen mindestens drei Speicherknoten enthalten.
- Durch das Hinzufügen einer neuen Site wird nicht automatisch die Anzahl der Objekte erhöht, die Sie speichern können. Die Gesamtobjektkapazität eines Grids hängt von der Menge des verfügbaren Speichers, der ILM-Richtlinie und der Metadatenkapazität an jedem Standort ab.
- Bei der Dimensionierung einer neuen Site müssen Sie sicherstellen, dass sie über genügend Metadatenkapazität verfügt.

  StorageGRID speichert an jedem Standort eine Kopie aller Objektmetadaten. Wenn Sie eine neue Site hinzufügen, müssen Sie sicherstellen, dass sie über genügend Metadatenkapazität für die vorhandenen Objektmetadaten und über genügend Metadatenkapazität für Wachstum verfügt.

  Weitere Informationen finden Sie unter:

  - "Verwalten des Objektmetadatenspeichers"
  - "Überwachen Sie die Objektmetadatenkapazität für jeden Speicherknoten"
- Sie müssen die verfügbare Netzwerkbandbreite zwischen den Standorten und die Netzwerklatenz berücksichtigen. Metadatenaktualisierungen werden kontinuierlich zwischen Sites repliziert, auch wenn alle Objekte nur an der Site gespeichert werden, an der sie aufgenommen werden.

- Da Ihr StorageGRID -System während der Erweiterung betriebsbereit bleibt, müssen Sie die ILM-Regeln überprüfen, bevor Sie mit dem Erweiterungsvorgang beginnen. Sie müssen sicherstellen, dass Objektkopien erst nach Abschluss des Erweiterungsvorgangs auf der neuen Site gespeichert werden.

  Stellen Sie beispielsweise vor Beginn der Erweiterung fest, ob irgendwelche Regeln den Standardspeicherpool (Alle Speicherknoten) verwenden. Wenn dies der Fall ist, müssen Sie einen neuen Speicherpool erstellen, der die vorhandenen Speicherknoten enthält, und Ihre ILM-Regeln aktualisieren, um den neuen Speicherpool zu verwenden. Andernfalls werden Objekte an den neuen Standort kopiert, sobald der erste Knoten an diesem Standort aktiv wird.

  Weitere Informationen zum Ändern von ILM beim Hinzufügen einer neuen Site finden Sie im"Beispiel für die Änderung einer ILM-Richtlinie" .

Benötigte Materialien zusammenstellen

Bevor Sie eine Erweiterung durchführen, sammeln Sie die Materialien und installieren und konfigurieren Sie alle neuen Hardware- und Netzwerkkomponenten.

Artikel	Hinweise
StorageGRID -Installationsarchiv	Wenn Sie neue Grid-Knoten oder eine neue Site hinzufügen, müssen Sie das StorageGRID -Installationsarchiv herunterladen und extrahieren. Sie müssen dieselbe Version verwenden, die derzeit im Grid ausgeführt wird. Einzelheiten finden Sie in der Anleitung fürHerunterladen und Extrahieren der StorageGRID -Installationsdateien . **Hinweis:** Sie müssen keine Dateien herunterladen, wenn Sie vorhandenen Speicherknoten neue Speichervolumes hinzufügen oder ein neues StorageGRID Gerät installieren.
Service-Laptop	Der Service-Laptop verfügt über folgende Ausstattung: • Netzwerkanschluss • SSH-Client (z. B. PuTTY) • "Unterstützte Webbrowser"
`Passwords.txt`Datei	Enthält die Passwörter, die für den Zugriff auf Grid-Knoten über die Befehlszeile erforderlich sind. Im Wiederherstellungspaket enthalten.
Bereitstellungspassphrase	Die Passphrase wird bei der Erstinstallation des StorageGRID -Systems erstellt und dokumentiert. Die Bereitstellungspassphrase ist nicht in der `Passwords.txt` Datei.

Artikel	Hinweise
StorageGRID -Dokumentation	• "StorageGRID verwalten" • "Versionshinweise" • Installationsanweisungen für Ihre Plattform ◦ "Installieren Sie StorageGRID unter Red Hat Enterprise Linux" ◦ "Installieren Sie StorageGRID unter Ubuntu oder Debian" ◦ "Installieren Sie StorageGRID auf VMware"
Aktuelle Dokumentation für Ihre Plattform	Informationen zu unterstützten Versionen finden Sie im "Interoperabilitätsmatrix-Tool (IMT)" .

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

[[Installationsdateien herunterladen und extrahieren]]

Bevor Sie neue Grid-Knoten oder eine neue Site hinzufügen können, müssen Sie das entsprechende StorageGRID Installationsarchiv herunterladen und die Dateien extrahieren.

Informationen zu diesem Vorgang

Sie müssen Erweiterungsvorgänge mit der Version von StorageGRID durchführen, die derzeit im Grid ausgeführt wird.

Schritte

1. Gehe zu "NetApp Downloads: StorageGRID" .
2. Wählen Sie die Version von StorageGRID aus, die derzeit im Grid ausgeführt wird.
3. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Ihr NetApp -Konto an .
4. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.
5. Wählen Sie in der Spalte **Install StorageGRID** der Download-Seite die `.tgz` oder `.zip` Datei für Ihre Plattform.

   Die in der Installationsarchivdatei angezeigte Version muss mit der Version der aktuell installierten Software übereinstimmen.

   Verwenden Sie die `.zip` Datei, wenn Sie Windows auf dem Service-Laptop ausführen.

Plattform	Installationsarchiv
Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu oder Debian oder Appliances	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

Plattform	Installationsarchiv
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`
OpenStack/anderer Hypervisor	Um eine vorhandene Bereitstellung auf OpenStack zu erweitern, müssen Sie eine virtuelle Maschine bereitstellen, auf der eine der oben aufgeführten unterstützten Linux-Distributionen ausgeführt wird, und die entsprechenden Anweisungen für Linux befolgen.

6. Laden Sie die Archivdatei herunter und extrahieren Sie sie.
7. Führen Sie die entsprechenden Schritte für Ihre Plattform aus, um die benötigten Dateien basierend auf Ihrer Plattform, der geplanten Grid-Topologie und der Art und Weise auszuwählen, wie Sie Ihr StorageGRID System erweitern möchten.

   Die im Schritt für jede Plattform aufgeführten Pfade beziehen sich auf das von der Archivdatei installierte Verzeichnis der obersten Ebene.

8. Wenn Sie ein Red Hat Enterprise Linux-System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet.
	RPM-Paket zum Installieren der StorageGRID -Knotenimages auf Ihren RHEL-Hosts.
	RPM-Paket zum Installieren des StorageGRID Hostdienstes auf Ihren RHEL-Hosts.
Bereitstellungsskripttool	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.

Pfad und Dateiname	Beschreibung
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Beispiel für eine Ansible-Rolle und ein Playbook zum Konfigurieren von RHEL-Hosts für die Bereitstellung von StorageGRID Containern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

1. Wenn Sie ein Ubuntu- oder Debian-System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine nicht für die Produktion NetApp -Lizenzdatei, die Sie für Tests und Proof-of-Concept-Bereitstellungen verwenden können.
	DEB-Paket zum Installieren der StorageGRID -Knotenimages auf Ubuntu- oder Debian-Hosts.

Pfad und Dateiname	Beschreibung
	MD5-Prüfsumme für die Datei `/debs/storagegrid-webscale-images-version-SHA.deb` .
	DEB-Paket zum Installieren des StorageGRID -Hostdienstes auf Ubuntu- oder Debian-Hosts.
Bereitstellungsskripttool	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Beispiel für eine Ansible-Rolle und ein Playbook zum Konfigurieren von Ubuntu- oder Debian-Hosts für die Bereitstellung von StorageGRID Containern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.

Pfad und Dateiname	Beschreibung
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

1. Wenn Sie ein VMware-System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet.
	Die Festplattendatei der virtuellen Maschine, die als Vorlage zum Erstellen virtueller Grid-Knotenmaschinen verwendet wird.
	Die Open Virtualization Format-Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen des primären Admin-Knotens.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen nicht primärer Admin-Knoten.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Gateway-Knoten.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Speicherknoten auf Basis virtueller Maschinen.
Bereitstellungsskripttool	Beschreibung
	Ein Bash-Shell-Skript zur Automatisierung der Bereitstellung virtueller Grid-Knoten.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `deploy-vsphere-ovftool.sh` Skript.

Pfad und Dateiname	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On (SSO) aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

1. Wenn Sie ein auf StorageGRID -Geräten basierendes System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	DEB-Paket zum Installieren der StorageGRID -Knotenimages auf Ihren Geräten.

Pfad und Dateiname	Beschreibung
	MD5-Prüfsumme für die Datei `/debs/storagegridwebscale-images-version-SHA.deb` .

Für die Installation der Appliance sind diese Dateien nur erforderlich, wenn Sie Netzwerkverkehr vermeiden müssen. Das Gerät kann die erforderlichen Dateien vom primären Admin-Knoten herunterladen.

Überprüfen der Hardware und des Netzwerks

Bevor Sie mit der Erweiterung Ihres StorageGRID -Systems beginnen, stellen Sie Folgendes sicher:

- Die zur Unterstützung der neuen Grid-Knoten oder des neuen Standorts erforderliche Hardware wurde installiert und konfiguriert.
- Alle neuen Knoten verfügen über bidirektionale Kommunikationspfade zu allen vorhandenen und neuen Knoten (eine Voraussetzung für das Grid-Netzwerk). Stellen Sie insbesondere sicher, dass die folgenden TCP-Ports zwischen den neuen Knoten, die Sie in der Erweiterung hinzufügen, und dem primären Admin-Knoten geöffnet sind:
  - 1055
  - 7443
  - 8011
  - 10342

  Sehen "Interne Grid-Knoten-Kommunikation" .
- Der primäre Admin-Knoten kann mit allen Erweiterungsservern kommunizieren, die das StorageGRID -System hosten sollen.
- Wenn einer der neuen Knoten eine Grid-Netzwerk-IP-Adresse in einem bisher nicht verwendeten Subnetz hat, haben Sie bereits"das neue Subnetz hinzugefügt" zur Grid-Network-Subnetzliste. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und den Vorgang erneut starten.
- Sie verwenden keine Netzwerkadressübersetzung (NAT) im Grid-Netzwerk zwischen Grid-Knoten oder zwischen StorageGRID Sites. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt geroutet werden können. Die Verwendung von NAT zum Überbrücken des Grid-Netzwerks über ein öffentliches Netzwerksegment wird nur unterstützt, wenn Sie eine Tunnelanwendung verwenden, die für alle Knoten im Grid transparent ist, d. h. die Grid-Knoten benötigen keine Kenntnis der öffentlichen IP-Adressen.

  Diese NAT-Einschränkung gilt speziell für Grid-Knoten und das Grid-Netzwerk. Bei Bedarf können Sie NAT zwischen externen Clients und Grid-Knoten verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway-Knoten bereitzustellen.

Speichervolumes hinzufügen

Speichervolumes zu Speicherknoten hinzufügen

Sie können die Speicherkapazität von Speicherknoten erweitern, die unter der maximal

unterstützten Anzahl von Volumes liegen. Möglicherweise müssen Sie Speichervolumes zu mehr als einem Speicherknoten hinzufügen, um die ILM-Anforderungen für replizierte oder löschcodierte Kopien zu erfüllen.

Bevor Sie beginnen

Bevor Sie Speichervolumes hinzufügen, überprüfen Sie die"Richtlinien zum Hinzufügen von Objektkapazität" um sicherzustellen, dass Sie wissen, wo Sie Volumes hinzufügen müssen, um die Anforderungen Ihrer ILM-Richtlinie zu erfüllen.

> Diese Anweisungen gelten nur für softwarebasierte Speicherknoten. Sehen "Erweiterungsfach zum bereitgestellten SG6060 hinzufügen" oder "Erweiterungsfach zum bereitgestellten SG6160 hinzufügen" um zu erfahren, wie Sie durch die Installation von Erweiterungsregalen Speichervolumes zum SG6060 oder SG6160 hinzufügen. Andere Appliance-Speicherknoten können nicht erweitert werden.

Informationen zu diesem Vorgang

Der zugrunde liegende Speicher eines Speicherknotens ist in Speichervolumes unterteilt. Speichervolumes sind blockbasierte Speichergeräte, die vom StorageGRID -System formatiert und zum Speichern von Objekten bereitgestellt werden. Jeder Speicherknoten kann bis zu 48 Speichervolumes unterstützen, die im Grid Manager als *Objektspeicher* bezeichnet werden.

> Objektmetadaten werden immer im Objektspeicher 0 gespeichert.

Jeder Objektspeicher wird auf einem Datenträger bereitgestellt, der seiner ID entspricht. Beispielsweise entspricht der Objektspeicher mit der ID 0000 dem `/var/local/rangedb/0` Einhängepunkt.

Bevor Sie neue Speichervolumes hinzufügen, verwenden Sie den Grid Manager, um die aktuellen Objektspeicher für jeden Speicherknoten sowie die entsprechenden Bereitstellungspunkte anzuzeigen. Sie können diese Informationen beim Hinzufügen von Speichervolumes verwenden.

Schritte

1. Wählen Sie **NODES** > ***site*** > ***Storage Node*** > **Storage**.
2. Scrollen Sie nach unten, um die Menge des verfügbaren Speichers für jedes Volume und jeden Objektspeicher anzuzeigen.

   Bei Appliance-Speicherknoten entspricht der weltweite Name für jede Festplatte der weltweiten Volume-Kennung (WWID), die angezeigt wird, wenn Sie die Standard-Volume-Eigenschaften in SANtricity OS anzeigen (der Verwaltungssoftware, die mit dem Speichercontroller der Appliance verbunden ist).

   Um Ihnen die Interpretation der Lese- und Schreibstatistiken für die Datenträger in Bezug auf Volume-Mount-Punkte zu erleichtern, entspricht der erste Teil des in der Spalte **Name** der Tabelle „Datenträgergeräte“ angezeigten Namens (also *sdc*, *sdd*, *sde* usw.) dem in der Spalte **Gerät** der Tabelle „Volumes“ angezeigten Wert.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. Befolgen Sie die Anweisungen für Ihre Plattform, um dem Speicherknoten neue Speichervolumes hinzuzufügen.
   - "VMware: Speichervolumes zum Speicherknoten hinzufügen"
   - "Linux: Direkt angeschlossene oder SAN-Volumes zum Speicherknoten hinzufügen"

VMware: Speichervolumes zum Speicherknoten hinzufügen

Wenn ein Speicherknoten weniger als 16 Speichervolumes umfasst, können Sie seine Kapazität erhöhen, indem Sie mithilfe von VMware vSphere Volumes hinzufügen.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anweisungen zur Installation von StorageGRID für VMware-Bereitstellungen.
  - "Installieren Sie StorageGRID auf VMware"
- Sie haben die `Passwords.txt` Datei.
- Du hast"spezifische Zugriffsberechtigungen" .

> Versuchen Sie nicht, einem Speicherknoten Speichervolumes hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein anderes Erweiterungsverfahren aktiv ist.

Informationen zu diesem Vorgang

Der Speicherknoten ist für kurze Zeit nicht verfügbar, wenn Sie Speichervolumes hinzufügen. Sie sollten dieses Verfahren jeweils nur auf einem Speicherknoten durchführen, um eine Beeinträchtigung der Client-orientierten Grid-Dienste zu vermeiden.

Schritte

1. Installieren Sie bei Bedarf neue Speicherhardware und erstellen Sie neue VMware-Datenspeicher.
2. Fügen Sie der virtuellen Maschine eine oder mehrere Festplatten zur Verwendung als Speicher (Objektspeicher) hinzu.
   a. Öffnen Sie den VMware vSphere-Client.
   b. Bearbeiten Sie die Einstellungen der virtuellen Maschine, um eine oder mehrere zusätzliche Festplatten hinzuzufügen.

   Die Festplatten sind typischerweise als Virtual Machine Disks (VMDKs) konfiguriert. VMDKs werden häufiger verwendet und sind einfacher zu verwalten, während RDMs möglicherweise eine bessere Leistung für Workloads bieten, die größere Objektgrößen verwenden (z. B. größer als 100 MB). Weitere Informationen zum Hinzufügen von Festplatten zu virtuellen Maschinen finden Sie in der VMware vSphere-Dokumentation.
3. Starten Sie die virtuelle Maschine neu, indem Sie die Option **Gastbetriebssystem neu starten** im VMware vSphere-Client verwenden oder indem Sie in einer SSH-Sitzung mit der virtuellen Maschine den folgenden Befehl eingeben:`sudo reboot`

   > Verwenden Sie nicht **Ausschalten** oder **Zurücksetzen**, um die virtuelle Maschine neu zu starten.
4. Konfigurieren Sie den neuen Speicher für die Verwendung durch den Speicherknoten:

a. Melden Sie sich beim Grid-Knoten an:

   i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

   ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

   iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

   iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

b. Konfigurieren Sie die neuen Speichervolumes:

```
sudo add_rangedbs.rb
```

   Dieses Skript findet alle neuen Speichervolumes und fordert Sie auf, sie zu formatieren.

c. Geben Sie **y** ein, um die Formatierung zu akzeptieren.

d. Wenn eines der Volumes zuvor formatiert wurde, entscheiden Sie, ob Sie es neu formatieren möchten.

   - Geben Sie **y** ein, um neu zu formatieren.
   - Geben Sie **n** ein, um die Neuformatierung zu überspringen.

Der `setup_rangedbs.sh` Skript wird automatisch ausgeführt.

5. Überprüfen Sie, ob die Dienste ordnungsgemäß gestartet werden:

   a. Zeigen Sie eine Liste mit dem Status aller Dienste auf dem Server an:

```
sudo storagegrid-status
```

   Der Status wird automatisch aktualisiert.

   a. Warten Sie, bis alle Dienste ausgeführt oder überprüft wurden.

   b. Verlassen Sie den Statusbildschirm:

```
Ctrl+C
```

6. Überprüfen Sie, ob der Speicherknoten online ist:

   a. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .

   b. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.

   c. Wählen Sie ***site*** > ***Storage Node*** > **LDR** > **Storage**.

   d. Wählen Sie die Registerkarte **Konfiguration** und dann die Registerkarte **Haupt**.

   e. Wenn die Dropdown-Liste **Speicherstatus – Gewünscht** auf „Schreibgeschützt“ oder „Offline“ eingestellt ist, wählen Sie „Online“ aus.

   f. Wählen Sie **Änderungen übernehmen**.

7. So zeigen Sie die neuen Objektspeicher an:

   a. Wählen Sie **NODES** > ***site*** > ***Storage Node*** > **Storage**.

   b. Sehen Sie sich die Details in der Tabelle **Objektspeicher** an.

Ergebnis

Sie können die erweiterte Kapazität der Storage Nodes zum Speichern von Objektdaten nutzen.

Linux: Direkt angeschlossene oder SAN-Volumes zum Speicherknoten hinzufügen

Wenn ein Speicherknoten weniger als 48 Speichervolumes umfasst, können Sie seine Kapazität erhöhen, indem Sie neue Blockspeichergeräte hinzufügen, diese für die Linux-Hosts sichtbar machen und die neuen Blockgerätezuordnungen zur StorageGRID -Konfigurationsdatei hinzufügen, die für den Speicherknoten verwendet wird.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anweisungen zur Installation von StorageGRID für Ihre Linux-Plattform.
  - "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
  - "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- Sie haben die `Passwords.txt` Datei.
- Du hast"spezifische Zugriffsberechtigungen" .

> Versuchen Sie nicht, einem Speicherknoten Speichervolumes hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein anderes Erweiterungsverfahren aktiv ist.

Informationen zu diesem Vorgang

Der Speicherknoten ist für kurze Zeit nicht verfügbar, wenn Sie Speichervolumes hinzufügen. Sie sollten dieses Verfahren jeweils nur auf einem Speicherknoten durchführen, um eine Beeinträchtigung der Client-orientierten Grid-Dienste zu vermeiden.

Schritte

1. Installieren Sie die neue Speicherhardware.

   Weitere Informationen finden Sie in der Dokumentation Ihres Hardwareanbieters.

2. Erstellen Sie neue Blockspeichervolumes der gewünschten Größe.
   - Schließen Sie die neuen Laufwerke an und aktualisieren Sie die RAID-Controller-Konfiguration nach Bedarf oder weisen Sie die neuen SAN-LUNs auf den gemeinsam genutzten Speicher-Arrays zu und ermöglichen Sie dem Linux-Host den Zugriff darauf.
   - Verwenden Sie dasselbe persistente Benennungsschema, das Sie für die Speichervolumes auf dem vorhandenen Speicherknoten verwendet haben.
   - Wenn Sie die StorageGRID Knotenmigrationsfunktion verwenden, machen Sie die neuen Volumes für andere Linux-Hosts sichtbar, die Migrationsziele für diesen Speicherknoten sind. Weitere Informationen finden Sie in den Anweisungen zur Installation von StorageGRID für Ihre Linux-Plattform.
3. Melden Sie sich beim Linux-Host, der den Speicherknoten unterstützt, als Root oder mit einem Konto mit Sudo-Berechtigung an.
4. Bestätigen Sie, dass die neuen Speichervolumes auf dem Linux-Host sichtbar sind.

   Möglicherweise müssen Sie erneut nach Geräten suchen.

5. Führen Sie den folgenden Befehl aus, um den Speicherknoten vorübergehend zu deaktivieren:

   ```
   sudo storagegrid node stop <node-name>
   ```

6. Bearbeiten Sie mit einem Texteditor wie vim oder pico die Knotenkonfigurationsdatei für den

Speicherknoten, die Sie unter finden. `/etc/storagegrid/nodes/<node-name>.conf` .

7. Suchen Sie den Abschnitt der Knotenkonfigurationsdatei, der die vorhandenen Objektspeicher-Blockgerätezuordnungen enthält.

   Im Beispiel `BLOCK_DEVICE_RANGEDB_00` Zu `BLOCK_DEVICE_RANGEDB_03` sind die vorhandenen Objektspeicher-Blockgerätezuordnungen.

   ```
   NODE_TYPE = VM_Storage_Node
   ADMIN_IP = 10.1.0.2
   BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
   BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
   BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
   BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
   BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
   GRID_NETWORK_TARGET = bond0.1001
   ADMIN_NETWORK_TARGET = bond0.1002
   CLIENT_NETWORK_TARGET = bond0.1003
   GRID_NETWORK_IP = 10.1.0.3
   GRID_NETWORK_MASK = 255.255.255.0
   GRID_NETWORK_GATEWAY = 10.1.0.1
   ```

8. Fügen Sie neue Objektspeicher-Blockgerätezuordnungen hinzu, die den Blockspeichervolumes entsprechen, die Sie für diesen Speicherknoten hinzugefügt haben.

   Beginnen Sie unbedingt mit dem nächsten `BLOCK_DEVICE_RANGEDB_nn` . Lassen Sie keine Lücke.

   - Basierend auf dem obigen Beispiel beginnen Sie bei `BLOCK_DEVICE_RANGEDB_04` .
   - Im folgenden Beispiel wurden dem Knoten vier neue Blockspeichervolumes hinzugefügt: `BLOCK_DEVICE_RANGEDB_04` Zu `BLOCK_DEVICE_RANGEDB_07` .

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. Führen Sie den folgenden Befehl aus, um Ihre Änderungen an der Knotenkonfigurationsdatei für den Speicherknoten zu validieren:

   ```
   sudo storagegrid node validate <node-name>
   ```

   Beheben Sie alle Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

   > Wenn Sie einen Fehler ähnlich dem folgenden beobachten, bedeutet dies, dass die Knotenkonfigurationsdatei versucht, das von `<node-name>` für `<PURPOSE>` zu den gegebenen `<path-name>` im Linux-Dateisystem, aber an diesem Speicherort gibt es keine gültige spezielle Blockgerätedatei (oder keinen Softlink zu einer speziellen Blockgerätedatei).
   >
   > ```
   > Checking configuration file for node <node-name>…
   > ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
   > <path-name> is not a valid block device
   > ```
   >
   > Überprüfen Sie, ob Sie die richtige `<path-name>` .

10. Führen Sie den folgenden Befehl aus, um den Knoten mit den neuen Blockgerätezuordnungen neu zu starten:

    ```
    sudo storagegrid node start <node-name>
    ```

11. Melden Sie sich als Administrator am Speicherknoten an und verwenden Sie dabei das Passwort, das in der `Passwords.txt` Datei.
12. Überprüfen Sie, ob die Dienste ordnungsgemäß gestartet werden:
    a. Zeigen Sie eine Liste des Status aller Dienste auf dem Server an:

```
sudo storagegrid-status
```

Der Status wird automatisch aktualisiert.

b. Warten Sie, bis alle Dienste ausgeführt oder überprüft wurden.

c. Verlassen Sie den Statusbildschirm:

```
Ctrl+C
```

13. Konfigurieren Sie den neuen Speicher für die Verwendung durch den Speicherknoten:

a. Konfigurieren Sie die neuen Speichervolumes:

```
sudo add_rangedbs.rb
```

Dieses Skript findet alle neuen Speichervolumes und fordert Sie auf, sie zu formatieren.

b. Geben Sie **y** ein, um die Speichervolumes zu formatieren.

c. Wenn eines der Volumes zuvor formatiert wurde, entscheiden Sie, ob Sie es neu formatieren möchten.

- Geben Sie **y** ein, um neu zu formatieren.
- Geben Sie **n** ein, um die Neuformatierung zu überspringen.

Der `setup_rangedbs.sh` Skript wird automatisch ausgeführt.

14. Überprüfen Sie, ob der Speicherstatus des Speicherknotens „Online“ lautet:

a. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .

b. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.

c. Wählen Sie ***site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Wählen Sie die Registerkarte **Konfiguration** und dann die Registerkarte **Haupt**.

e. Wenn die Dropdown-Liste **Speicherstatus – Gewünscht** auf „Schreibgeschützt“ oder „Offline“ eingestellt ist, wählen Sie „Online“ aus.

f. Klicken Sie auf **Änderungen übernehmen**.

15. So zeigen Sie die neuen Objektspeicher an:

a. Wählen Sie **NODES** > ***site*** > ***Storage Node*** > **Storage**.

b. Sehen Sie sich die Details in der Tabelle **Objektspeicher** an.

Ergebnis

Sie können jetzt die erweiterte Kapazität der Storage Nodes zum Speichern von Objektdaten nutzen.

Rasterknoten oder Site hinzufügen

Fügen Sie Rasterknoten zu einer vorhandenen Site hinzu oder fügen Sie eine neue Site hinzu

Befolgen Sie diese Vorgehensweise, um Rasterknoten zu vorhandenen Sites hinzuzufügen oder eine neue Site hinzuzufügen. Sie können jeweils nur eine Art der Erweiterung durchführen.

Bevor Sie beginnen

- Sie haben die"Root-Zugriff oder Wartungsberechtigung" .
- Alle vorhandenen Knoten im Grid sind an allen Standorten aktiv und betriebsbereit.
- Alle vorherigen Erweiterungs-, Upgrade-, Außerbetriebnahme- oder Wiederherstellungsverfahren sind abgeschlossen.

> Sie können keine Erweiterung starten, während eine andere Erweiterung, ein Upgrade, eine Wiederherstellung oder ein aktives Außerbetriebnahmeverfahren läuft. Bei Bedarf können Sie jedoch einen Außerbetriebnahmevorgang unterbrechen, um eine Erweiterung zu starten.

Schritte

1. "Subnetze für Grid-Netzwerke aktualisieren" .
2. "Neue Grid-Knoten bereitstellen" .
3. "Erweiterung durchführen" .

Subnetze für Grid-Netzwerke aktualisieren

Wenn Sie Grid-Knoten oder einen neuen Standort in einer Erweiterung hinzufügen, müssen Sie möglicherweise Subnetze zum Grid-Netzwerk aktualisieren oder hinzufügen.

StorageGRID verwaltet eine Liste der Netzwerk-Subnetze, die zur Kommunikation zwischen Grid-Knoten im Grid-Netzwerk (eth0) verwendet werden. Diese Einträge umfassen die von jedem Standort in Ihrem StorageGRID -System für das Grid-Netzwerk verwendeten Subnetze sowie alle für NTP, DNS, LDAP oder andere externe Server verwendeten Subnetze, auf die über das Grid-Netzwerk-Gateway zugegriffen wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben die Bereitstellungspassphrase.
- Sie verfügen über die Netzwerkadressen der Subnetze, die Sie konfigurieren möchten, in CIDR-Notation.

Informationen zu diesem Vorgang

Wenn einer der neuen Knoten eine Grid-Netzwerk-IP-Adresse in einem bisher nicht verwendeten Subnetz hat, müssen Sie das neue Subnetz vor Beginn der Erweiterung zur Grid-Netzwerk-Subnetzliste hinzufügen. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und den Vorgang erneut starten.

Verwenden Sie keine Subnetze, die die folgenden IPv4-Adressen für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens enthalten:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Verwenden Sie beispielsweise nicht die folgenden Subnetzbereiche für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens:

- 192.168.130.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.130.101 und 192.168.130.102 enthält
- 192.168.131.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.131.101 und 192.168.131.102 enthält
- 198.51.100.0/24, da dieser Subnetzbereich die IP-Adressen 198.51.100.2 und 198.51.100.4 enthält

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **Grid-Netzwerk**.
2. Wählen Sie **Weiteres Subnetz hinzufügen**, um ein neues Subnetz in CIDR-Notation hinzuzufügen.

   Geben Sie beispielsweise `10.96.104.0/22` .
3. Geben Sie die Bereitstellungspassphrase ein und wählen Sie **Speichern**.
4. Warten Sie, bis die Änderungen übernommen wurden, und laden Sie dann ein neues Wiederherstellungspaket herunter.
   a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
   b. Geben Sie die **Bereitstellungspassphrase** ein.

Die Datei des Wiederherstellungspakets muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können. Es wird auch verwendet, um den primären Admin-Knoten wiederherzustellen.

Die von Ihnen angegebenen Subnetze werden automatisch für Ihr StorageGRID -System konfiguriert.

Neue Grid-Knoten bereitstellen

Die Schritte zum Bereitstellen neuer Grid-Knoten in einer Erweiterung sind dieselben wie die Schritte, die bei der Erstinstallation des Grids verwendet wurden. Sie müssen alle neuen Grid-Knoten bereitstellen, bevor Sie die Erweiterung durchführen können.

Wenn Sie ein Raster erweitern, müssen die hinzugefügten Knoten nicht mit den vorhandenen Knotentypen übereinstimmen. Sie können VMware-Knoten, Linux-Container-basierte Knoten oder Appliance-Knoten

hinzufügen.

VMware: Grid-Knoten bereitstellen

Sie müssen für jeden VMware-Knoten, den Sie der Erweiterung hinzufügen möchten, eine virtuelle Maschine in VMware vSphere bereitstellen.

Schritte

1. "Stellen Sie den neuen Knoten als virtuelle Maschine bereit"und verbinden Sie es mit einem oder mehreren StorageGRID -Netzwerken.

   Wenn Sie den Knoten bereitstellen, können Sie optional Knotenports neu zuordnen oder die CPU- oder Speichereinstellungen erhöhen.

2. Nachdem Sie alle neuen VMware-Knoten bereitgestellt haben,"Führen Sie den Erweiterungsvorgang durch" .

Linux: Grid-Knoten bereitstellen

Sie können Grid-Knoten auf neuen oder vorhandenen Linux-Hosts bereitstellen. Wenn Sie zusätzliche Linux-Hosts benötigen, um die CPU-, RAM- und Speicheranforderungen der StorageGRID -Knoten zu unterstützen, die Sie Ihrem Grid hinzufügen möchten, bereiten Sie diese auf die gleiche Weise vor, wie Sie die Hosts bei der Erstinstallation vorbereitet haben. Anschließend stellen Sie die Erweiterungsknoten auf die gleiche Weise bereit, wie Sie während der Installation Grid-Knoten bereitgestellt haben.

Bevor Sie beginnen

- Sie verfügen über die Anweisungen zur Installation von StorageGRID für Ihre Linux-Version und haben die Hardware- und Speicheranforderungen überprüft.
  - "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
  - "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- Wenn Sie planen, neue Grid-Knoten auf vorhandenen Hosts bereitzustellen, haben Sie sichergestellt, dass die vorhandenen Hosts über genügend CPU-, RAM- und Speicherkapazität für die zusätzlichen Knoten verfügen.
- Sie haben einen Plan zur Minimierung von Fehlerdomänen. Sie sollten beispielsweise nicht alle Gateway-Knoten auf einem einzigen physischen Host bereitstellen.

  > Führen Sie bei einer Produktionsbereitstellung nicht mehr als einen Speicherknoten auf einem einzelnen physischen oder virtuellen Host aus. Durch die Verwendung eines dedizierten Hosts für jeden Speicherknoten wird eine isolierte Fehlerdomäne bereitgestellt.

- Wenn der StorageGRID Knoten Speicher verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass für das Volume keine FabricPool -Tiering-Richtlinie aktiviert ist. Das Deaktivieren der FabricPool Tiering-Funktion für Volumes, die mit StorageGRID -Knoten verwendet werden, vereinfacht die Fehlerbehebung und Speichervorgänge.

Schritte

1. Wenn Sie neue Hosts hinzufügen, greifen Sie auf die Installationsanweisungen zum Bereitstellen von StorageGRID -Knoten zu.
2. Um die neuen Hosts bereitzustellen, befolgen Sie die Anweisungen zum Vorbereiten der Hosts.
3. Um Knotenkonfigurationsdateien zu erstellen und die StorageGRID Konfiguration zu validieren, befolgen Sie die Anweisungen zum Bereitstellen von Grid-Knoten.

4. Wenn Sie einem neuen Linux-Host Knoten hinzufügen, starten Sie den StorageGRID Hostdienst.
5. Wenn Sie einem vorhandenen Linux-Host Knoten hinzufügen, starten Sie die neuen Knoten mithilfe der CLI des StorageGrid-Hostdienstes:`sudo storagegrid node start [<node name\>]`

Nach Abschluss

Nachdem Sie alle neuen Grid-Knoten bereitgestellt haben, können Sie"führen Sie die Erweiterung durch" .

Appliances: Bereitstellen von Speicher-, Gateway- oder nicht primären Admin-Knoten

Um die StorageGRID -Software auf einem Appliance-Knoten zu installieren, verwenden Sie den StorageGRID Appliance Installer, der auf der Appliance enthalten ist. Bei einer Erweiterung fungiert jedes Speichergerät als einzelner Speicherknoten und jedes Servicegerät als einzelner Gateway-Knoten oder nicht-primärer Admin-Knoten. Jedes Gerät kann eine Verbindung zum Grid-Netzwerk, zum Admin-Netzwerk und zum Client-Netzwerk herstellen.

Bevor Sie beginnen

- Das Gerät wurde in einem Rack oder Schrank installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Sie haben die "Hardware einrichten" Schritte.

  Das Einrichten der Appliance-Hardware umfasst die erforderlichen Schritte zum Konfigurieren von StorageGRID -Verbindungen (Netzwerkverbindungen und IP-Adressen) sowie die optionalen Schritte zum Aktivieren der Knotenverschlüsselung, Ändern des RAID-Modus und Neuzuordnung von Netzwerkports.

- Alle auf der IP-Konfigurationsseite des StorageGRID Appliance Installer aufgeführten Grid-Netzwerk-Subnetze wurden in der Grid-Netzwerk-Subnetzliste auf dem primären Admin-Knoten definiert.
- Die StorageGRID Appliance Installer-Firmware auf dem Ersatzgerät ist mit der StorageGRID -Softwareversion kompatibel, die derzeit auf Ihrem Grid ausgeführt wird. Wenn die Versionen nicht kompatibel sind, müssen Sie die Firmware des StorageGRID Appliance Installer aktualisieren.
- Sie verfügen über einen Dienstlaptop mit"unterstützter Webbrowser" .
- Sie kennen eine der dem Compute-Controller des Geräts zugewiesenen IP-Adressen. Sie können die IP-Adresse für jedes angeschlossene StorageGRID Netzwerk verwenden.

Informationen zu diesem Vorgang

Der Prozess der Installation von StorageGRID auf einem Appliance-Knoten umfasst die folgenden Phasen:

- Sie geben die IP-Adresse des primären Admin-Knotens und den Namen des Appliance-Knotens an oder bestätigen diese.
- Sie starten die Installation und warten, während die Volumes konfiguriert und die Software installiert wird.

  Während der Installationsaufgaben der Appliance wird die Installation angehalten. Um die Installation fortzusetzen, melden Sie sich beim Grid Manager an, genehmigen Sie alle Grid-Knoten und schließen Sie den StorageGRID -Installationsprozess ab.

> Wenn Sie mehrere Appliance-Knoten gleichzeitig bereitstellen müssen, können Sie den Installationsprozess automatisieren, indem Sie den `configure-sga.py` Appliance-Installationsskript.

Schritte

1. Öffnen Sie einen Browser und geben Sie eine der IP-Adressen für den Compute-Controller des Geräts ein.

`https://Controller_IP:8443`

Die Startseite des StorageGRID Appliance-Installationsprogramms wird angezeigt.

2. Legen Sie im Abschnitt „Verbindung zum **Primären Admin-Knoten**“ fest, ob Sie die IP-Adresse für den primären Admin-Knoten angeben müssen.

   Wenn Sie zuvor andere Knoten in diesem Rechenzentrum installiert haben, kann der StorageGRID Appliance Installer diese IP-Adresse automatisch erkennen, vorausgesetzt, der primäre Admin-Knoten oder mindestens ein anderer Grid-Knoten mit konfigurierter ADMIN_IP ist im selben Subnetz vorhanden.

3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	a. Deaktivieren Sie das Kontrollkästchen **Admin-Knotenerkennung aktivieren**. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie auf **Speichern**. d. Warten Sie, bis der Verbindungsstatus für die neue IP-Adresse bereit ist.
Automatische Erkennung aller verbundenen primären Admin-Knoten	a. Aktivieren Sie das Kontrollkästchen **Admin-Knotenerkennung aktivieren**. b. Warten Sie, bis die Liste der erkannten IP-Adressen angezeigt wird. c. Wählen Sie den primären Admin-Knoten für das Grid aus, in dem dieser Appliance-Speicherknoten bereitgestellt wird. d. Klicken Sie auf **Speichern**. e. Warten Sie, bis der Verbindungsstatus für die neue IP-Adresse bereit ist.

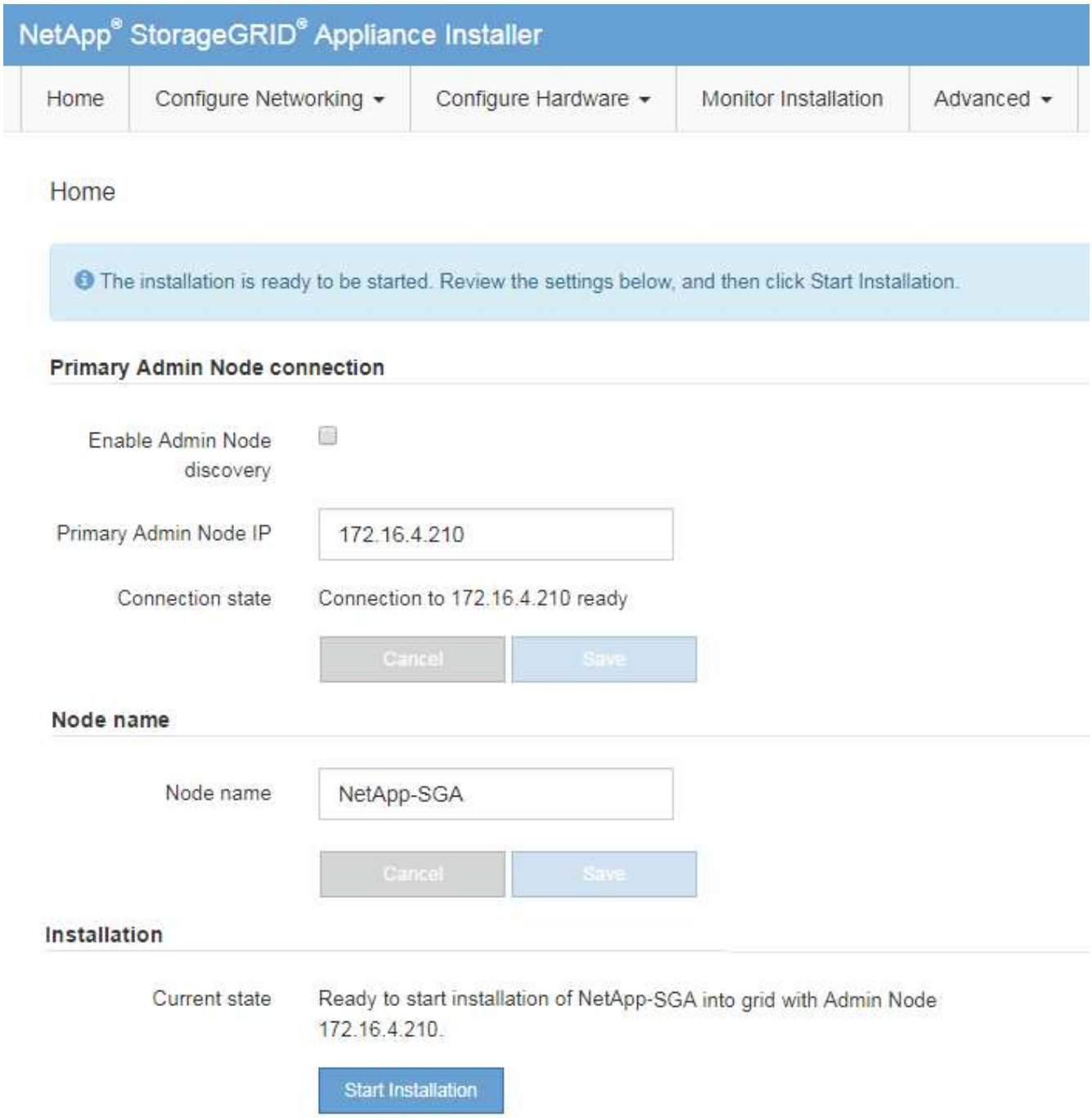
4. Geben Sie im Feld **Knotenname** den Namen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und wählen Sie **Speichern**.

   Der Knotenname wird diesem Appliance-Knoten im StorageGRID -System zugewiesen. Es wird auf der Knotenseite (Registerkarte „Übersicht“) im Grid Manager angezeigt. Bei Bedarf können Sie den Namen ändern, wenn Sie den Knoten genehmigen.

5. Bestätigen Sie im Abschnitt **Installation**, dass der aktuelle Status „Bereit zum Starten der Installation von *Knotenname* im Grid mit dem primären Admin-Knoten *admin_ip*“ lautet und dass die Schaltfläche **Installation starten** aktiviert ist.

   Wenn die Schaltfläche **Installation starten** nicht aktiviert ist, müssen Sie möglicherweise die Netzwerkkonfiguration oder die Porteinstellungen ändern. Anweisungen hierzu finden Sie in der Wartungsanleitung Ihres Geräts.

6. Wählen Sie auf der Startseite des StorageGRID Appliance Installer die Option **Installation starten**.



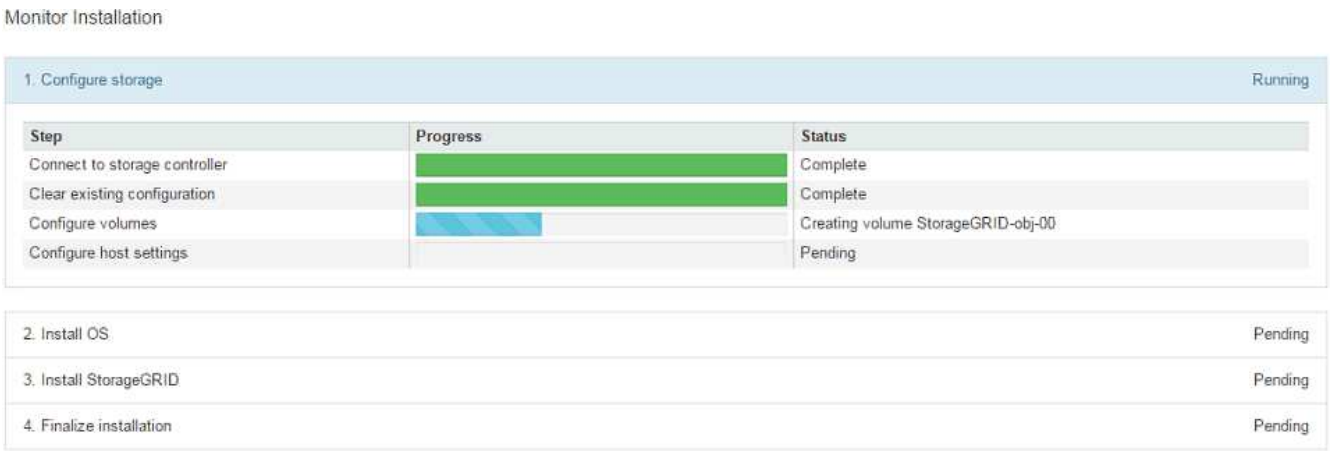
Der aktuelle Status ändert sich in „Installation läuft“ und die Seite „Monitorinstallation“ wird angezeigt.

7. Wenn Ihre Erweiterung mehrere Appliance-Knoten umfasst, wiederholen Sie die vorherigen Schritte für jede Appliance.

> Wenn Sie mehrere Appliance-Speicherknoten gleichzeitig bereitstellen müssen, können Sie den Installationsprozess mithilfe des Appliance-Installationsskripts configure-sga.py automatisieren.

8. Wenn Sie manuell auf die Seite „Monitorinstallation“ zugreifen müssen, wählen Sie in der Menüleiste „Monitorinstallation“ aus.

   Auf der Seite „Installation überwachen“ wird der Installationsfortschritt angezeigt.



Die blaue Statusleiste zeigt an, welche Aufgabe gerade ausgeführt wird. Grüne Statusbalken zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.

> Das Installationsprogramm stellt sicher, dass Aufgaben, die bei einer vorherigen Installation abgeschlossen wurden, nicht erneut ausgeführt werden. Wenn Sie eine Installation erneut ausführen, werden alle Aufgaben, die nicht erneut ausgeführt werden müssen, mit einer grünen Statusleiste und dem Status „Übersprungen“ angezeigt.

9. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

   1. Gerät konfigurieren

   Während dieser Phase findet einer der folgenden Prozesse statt:

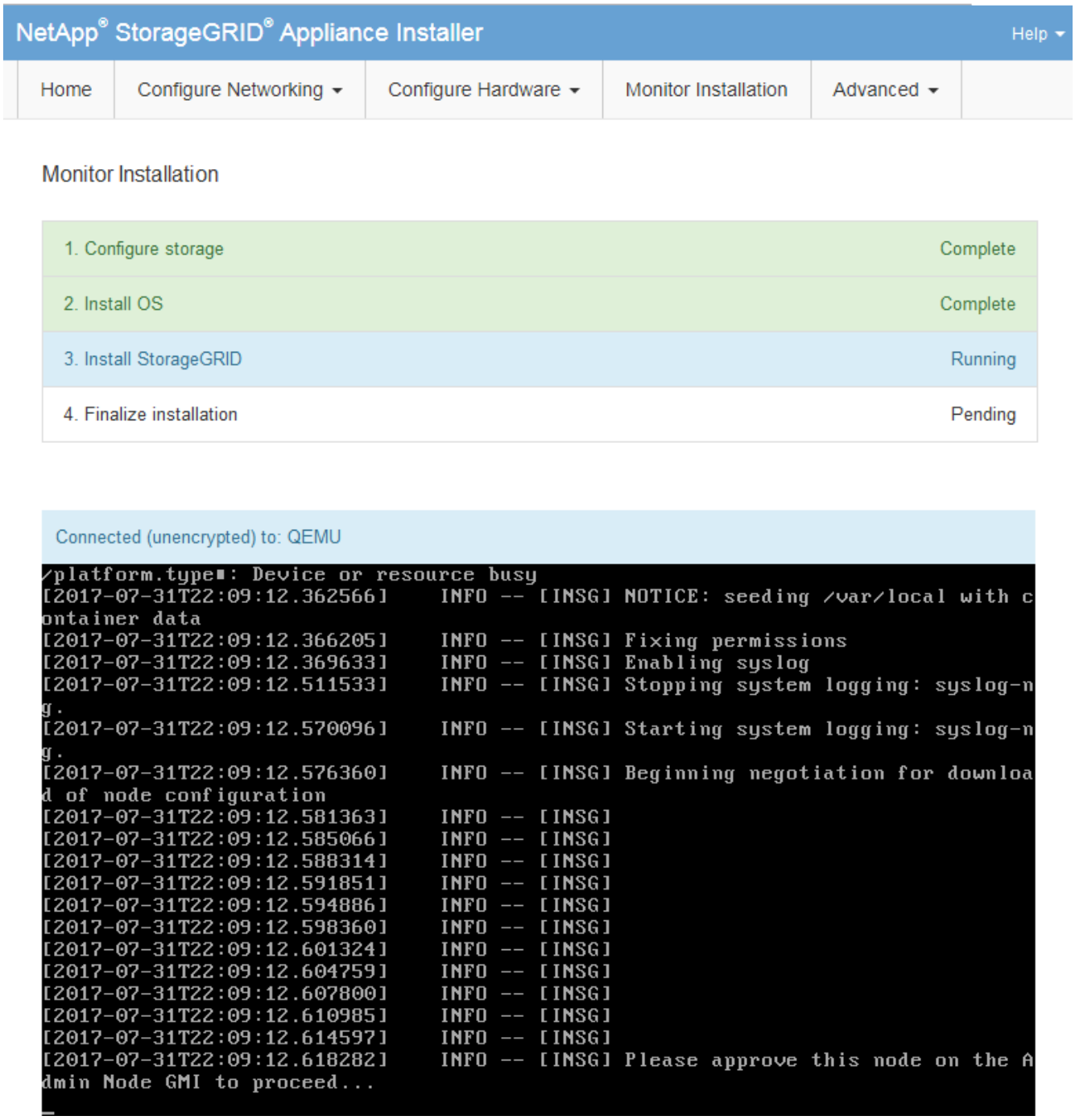
   - Bei einem Speichergerät stellt das Installationsprogramm eine Verbindung zum Speichercontroller her, löscht alle vorhandenen Konfigurationen, kommuniziert mit SANtricity OS, um Volumes zu konfigurieren, und konfiguriert die Hosteinstellungen.
   - Bei einer Service-Appliance löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken im Compute-Controller und konfiguriert die Host-Einstellungen.

   2. Betriebssystem installieren

   Während dieser Phase kopiert das Installationsprogramm das Basis-Betriebssystem-Image für StorageGRID auf das Gerät.

10. Überwachen Sie den Installationsfortschritt weiter, bis im Konsolenfenster eine Meldung angezeigt wird, in der Sie aufgefordert werden, den Knoten mithilfe des Grid Managers zu genehmigen.

> Warten Sie, bis alle Knoten, die Sie in dieser Erweiterung hinzugefügt haben, zur Genehmigung bereit sind, bevor Sie zum Grid Manager gehen, um die Knoten zu genehmigen.



Erweiterung durchführen

Wenn Sie die Erweiterung durchführen, werden die neuen Grid-Knoten zu Ihrer vorhandenen StorageGRID Bereitstellung hinzugefügt.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die Bereitstellungspassphrase.
- Sie haben alle Grid-Knoten bereitgestellt, die in dieser Erweiterung hinzugefügt werden.
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .

- Wenn Sie Speicherknoten hinzufügen, haben Sie bestätigt, dass alle im Rahmen einer Wiederherstellung durchgeführten Datenreparaturvorgänge abgeschlossen sind. Sehen "Überprüfen Sie die Datenreparaturaufträge" .
- Wenn Sie Speicherknoten hinzufügen und diesen Knoten eine benutzerdefinierte Speicherklasse zuweisen möchten, haben Sie bereits"erstellt die benutzerdefinierte Speicherklasse" . Sie verfügen außerdem entweder über die Root-Zugriffsberechtigung oder sowohl über die Wartungs- als auch über die ILM-Berechtigung.
- Wenn Sie eine neue Site hinzufügen, haben Sie die ILM-Regeln überprüft und aktualisiert. Sie müssen sicherstellen, dass Objektkopien erst nach Abschluss der Erweiterung auf der neuen Site gespeichert werden. Wenn beispielsweise eine Regel den Standardspeicherpool (**Alle Speicherknoten**) verwendet, müssen Sie"Erstellen Sie einen neuen Speicherpool" das nur die vorhandenen Speicherknoten enthält und"ILM-Regeln aktualisieren" und die ILM-Richtlinie zur Verwendung dieses neuen Speicherpools. Andernfalls werden Objekte an den neuen Standort kopiert, sobald der erste Knoten an diesem Standort aktiv wird.

Informationen zu diesem Vorgang

Die Durchführung der Erweiterung umfasst die folgenden Hauptaufgaben des Benutzers:

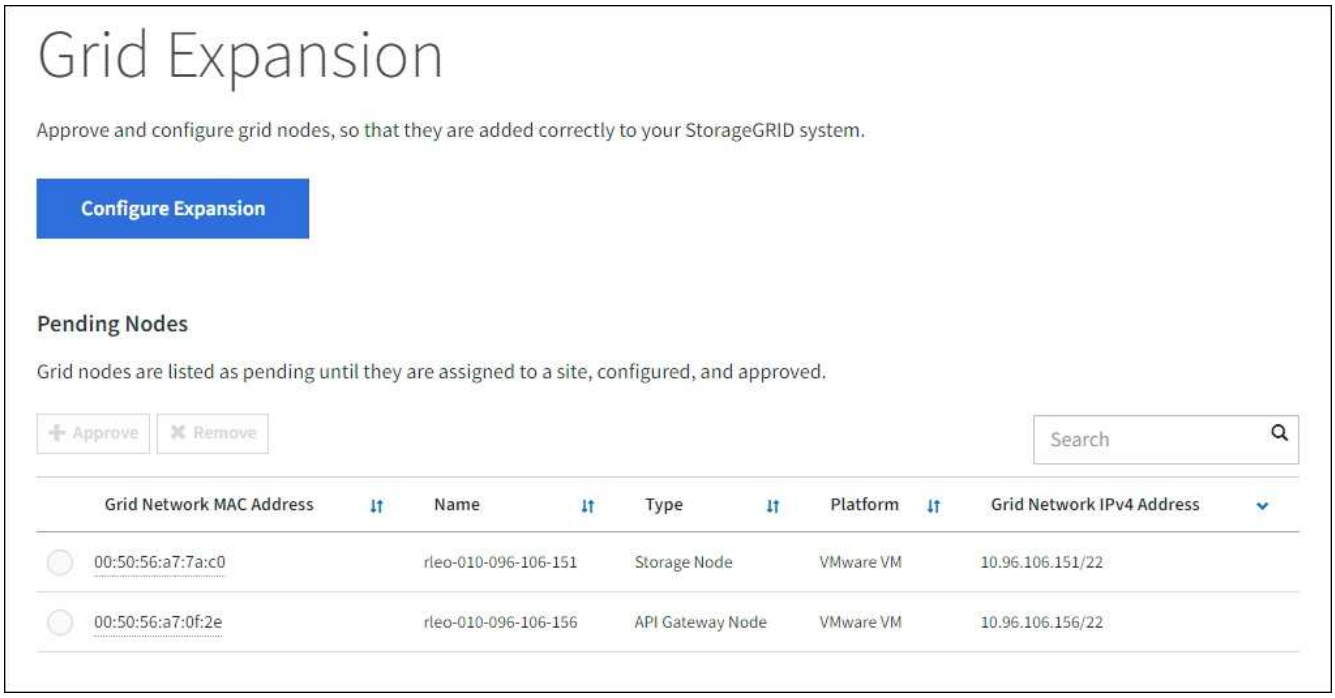
1. Konfigurieren Sie die Erweiterung.
2. Starten Sie die Erweiterung.
3. Laden Sie eine neue Wiederherstellungspaketdatei herunter.
4. Überwachen Sie die Erweiterungsschritte und -phasen, bis alle neuen Knoten installiert und konfiguriert sind und alle Dienste gestartet wurden.

> Die Ausführung einiger Erweiterungsschritte und -phasen in einem großen Grid kann eine beträchtliche Zeit in Anspruch nehmen. Beispielsweise kann das Streamen von Cassandra auf einen neuen Speicherknoten nur wenige Minuten dauern, wenn die Cassandra-Datenbank leer ist. Wenn die Cassandra-Datenbank jedoch eine große Menge an Objektmetadaten enthält, kann dieser Schritt mehrere Stunden oder länger dauern. Starten Sie während der Phasen „Erweitern des Cassandra-Clusters“ oder „Starten von Cassandra und Streamen von Daten“ keine Speicherknoten neu.

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Erweiterung**.

   Die Seite „Netzerweiterung“ wird angezeigt. Im Abschnitt „Ausstehende Knoten“ werden die Knoten aufgelistet, die zum Hinzufügen bereit sind.

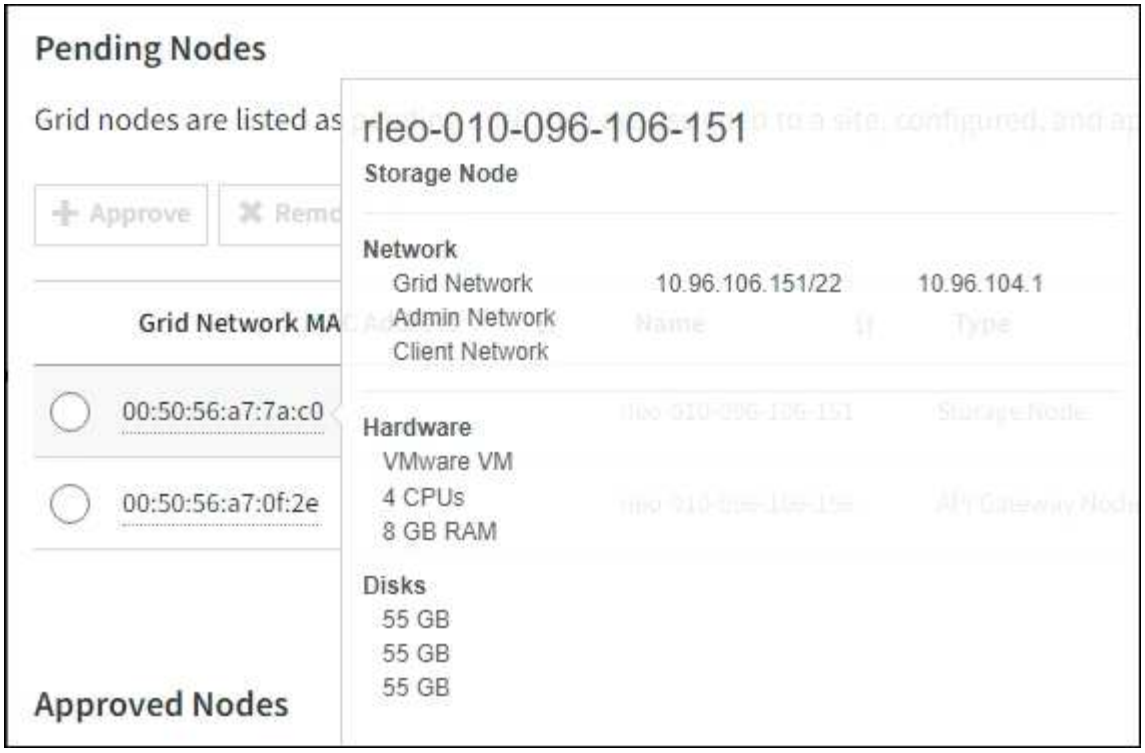


2. Wählen Sie **Erweiterung konfigurieren**.

   Das Dialogfeld „Site-Auswahl“ wird angezeigt.

3. Wählen Sie den Typ der Erweiterung aus, die Sie starten:
   - Wenn Sie eine neue Site hinzufügen, wählen Sie **Neu** und geben Sie den Namen der neuen Site ein.
   - Wenn Sie einer vorhandenen Site einen oder mehrere Knoten hinzufügen, wählen Sie **Vorhanden** aus.
4. Wählen Sie **Speichern**.
5. Überprüfen Sie die Liste **Ausstehende Knoten** und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

   Bei Bedarf können Sie Ihren Cursor über die **Grid-Netzwerk-MAC-Adresse** eines Knotens positionieren, um Details zu diesem Knoten anzuzeigen.



Wenn ein Knoten fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

6. Genehmigen Sie aus der Liste der ausstehenden Knoten die Knoten, die Sie dieser Erweiterung hinzufügen möchten.
   a. Wählen Sie das Optionsfeld neben dem ersten ausstehenden Rasterknoten aus, den Sie genehmigen möchten.
   b. Wählen Sie **Genehmigen**.

      Das Konfigurationsformular für Rasterknoten wird angezeigt.

   c. Passen Sie bei Bedarf die allgemeinen Einstellungen an:

Feld	Beschreibung
Website	Der Name der Site, mit der der Rasterknoten verknüpft wird. Wenn Sie mehrere Knoten hinzufügen, achten Sie darauf, für jeden Knoten die richtige Site auszuwählen. Wenn Sie eine neue Site hinzufügen, werden alle Knoten zur neuen Site hinzugefügt.
Name	Der Systemname für den Knoten. Systemnamen sind für interne StorageGRID -Vorgänge erforderlich und können nicht geändert werden.

Feld	Beschreibung
Speichertyp (nur Speicherknoten)	• **Daten und Metadaten** („kombiniert“): Objektdaten- und Metadaten-Speicherknoten • **Nur Daten**: Speicherknoten, der nur Objektdaten enthält (keine Metadaten) • **Nur Metadaten**: Speicherknoten, der nur Metadaten enthält (keine Objektdaten)
NTP-Rolle	Die Network Time Protocol (NTP)-Rolle des Grid-Knotens: • Wählen Sie **Automatisch** (Standard), um dem Knoten automatisch die NTP-Rolle zuzuweisen. Die primäre Rolle wird Admin-Knoten, Speicherknoten mit ADC-Diensten, Gateway-Knoten und allen Grid-Knoten mit nicht statischen IP-Adressen zugewiesen. Die Client-Rolle wird allen anderen Grid-Knoten zugewiesen. • Wählen Sie **Primär** aus, um dem Knoten manuell die primäre NTP-Rolle zuzuweisen. Mindestens zwei Knoten an jedem Standort sollten die primäre Rolle haben, um redundanten Systemzugriff auf externe Zeitquellen bereitzustellen. • Wählen Sie **Client** aus, um dem Knoten manuell die Client-NTP-Rolle zuzuweisen.
ADC-Dienst (kombinierte oder reine Metadaten-Speicherknoten)	Ob dieser Speicherknoten den Administrative Domain Controller (ADC)-Dienst ausführen wird. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Diensten. Mindestens drei Speicherknoten an jedem Standort müssen den ADC-Dienst enthalten. Sie können den ADC-Dienst nach der Bereitstellung nicht mehr zu einem Knoten hinzufügen. • Wählen Sie **Ja**, wenn der Speicherknoten, den Sie ersetzen, den ADC-Dienst enthält. Da Sie einen Speicherknoten nicht außer Betrieb nehmen können, wenn zu wenige ADC-Dienste übrig bleiben, wird dadurch sichergestellt, dass ein neuer ADC-Dienst verfügbar ist, bevor der alte Dienst entfernt wird. • Wählen Sie **Automatisch**, damit das System ermittelt, ob dieser Knoten den ADC-Dienst benötigt. Erfahren Sie mehr über die"ADC-Quorum" .
Speicherqualität (kombinierte oder reine Datenspeicherknoten)	Verwenden Sie die **Standard**-Speicherklasse oder wählen Sie die benutzerdefinierte Speicherklasse aus, die Sie diesem neuen Knoten zuweisen möchten. Speicherklassen werden von ILM-Speicherpools verwendet, Ihre Auswahl kann sich also darauf auswirken, welche Objekte auf dem Speicherknoten platziert werden.

d. Ändern Sie nach Bedarf die Einstellungen für das Grid-Netzwerk, das Admin-Netzwerk und das Client-

Netzwerk.

- **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Netzwerkschnittstelle. Beispiel: 172.16.10.100/24

> Wenn Sie beim Genehmigen von Knoten feststellen, dass Knoten im Grid-Netzwerk doppelte IP-Adressen haben, müssen Sie die Erweiterung abbrechen, die virtuellen Maschinen oder Appliances mit einer nicht doppelten IP erneut bereitstellen und die Erweiterung neu starten.

- **Gateway**: Das Standard-Gateway des Grid-Knotens. Beispiel: 172.16.10.1
- **Subnetze (CIDR)**: Ein oder mehrere Subnetze für das Admin-Netzwerk.

e. Wählen Sie **Speichern**.

Der genehmigte Rasterknoten wird in die Liste „Genehmigte Knoten“ verschoben.

- Um die Eigenschaften eines genehmigten Rasterknotens zu ändern, wählen Sie dessen Optionsfeld aus und wählen Sie **Bearbeiten**.
- Um einen genehmigten Rasterknoten zurück in die Liste „Ausstehende Knoten“ zu verschieben, wählen Sie das entsprechende Optionsfeld aus und wählen Sie „Zurücksetzen“.
- Um einen genehmigten Grid-Knoten dauerhaft zu entfernen, schalten Sie den Knoten aus. Wählen Sie dann das Optionsfeld und wählen Sie **Entfernen**.

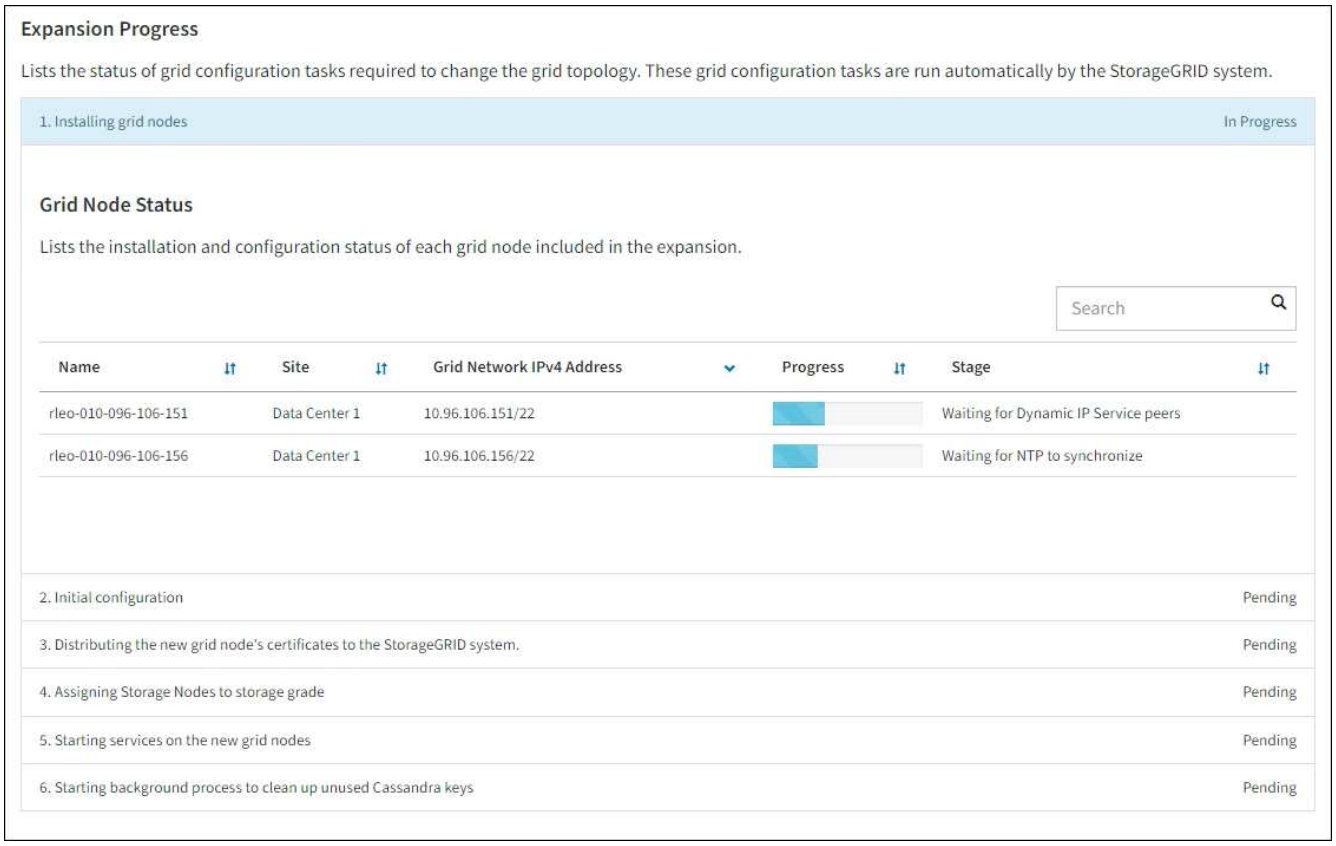
f. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

> Wenn möglich, sollten Sie alle ausstehenden Rasternotizen genehmigen und eine einzelne Erweiterung durchführen. Wenn Sie mehrere kleine Erweiterungen durchführen, ist mehr Zeit erforderlich.

7. Wenn Sie alle Grid-Knoten genehmigt haben, geben Sie die **Bereitstellungspassphrase** ein und wählen Sie **Erweitern**.

Nach einigen Minuten wird diese Seite aktualisiert und zeigt den Status des Erweiterungsvorgangs an. Wenn Aufgaben ausgeführt werden, die einzelne Grid-Knoten betreffen, wird im Abschnitt „Grid-Knotenstatus“ der aktuelle Status für jeden Grid-Knoten aufgelistet.

> Während des Schritts „Grid-Knoten installieren“ für ein neues Gerät zeigt das StorageGRID Appliance Installer den Übergang der Installation von Phase 3 zu Phase 4, „Installation abschließen“. Wenn Phase 4 abgeschlossen ist, wird der Controller neu gestartet.



Eine Site-Erweiterung umfasst eine zusätzliche Aufgabe zum Konfigurieren von Cassandra für die neue Site.

8. Sobald der Link **Wiederherstellungspaket herunterladen** angezeigt wird, laden Sie die Wiederherstellungspaketdatei herunter.

   Sie müssen so schnell wie möglich eine aktualisierte Kopie der Wiederherstellungspaketdatei herunterladen, nachdem Sie Änderungen an der Netztopologie am StorageGRID -System vorgenommen haben. Mit der Wiederherstellungspaketdatei können Sie das System wiederherstellen, wenn ein Fehler auftritt.

   a. Wählen Sie den Download-Link.
   b. Geben Sie die Bereitstellungspassphrase ein und wählen Sie **Download starten**.
   c. Wenn der Download abgeschlossen ist, öffnen Sie die `.zip` Datei und bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich der `Passwords.txt` Datei.
   d. Kopieren Sie die heruntergeladene Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.

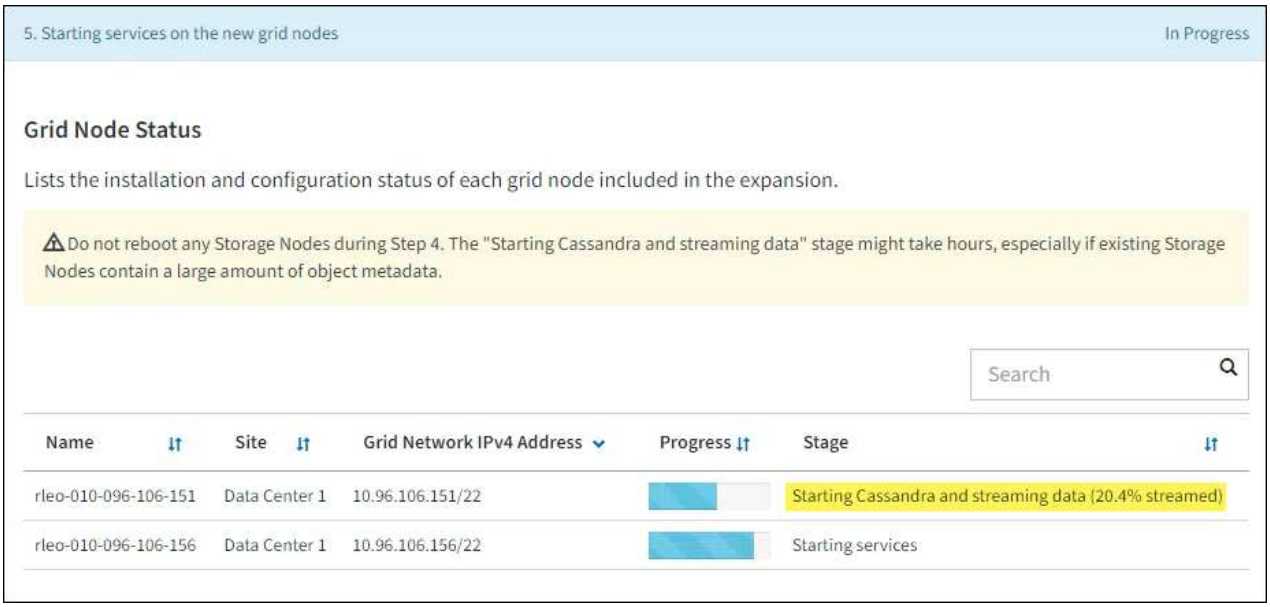
   Die Datei des Wiederherstellungspakets muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

9. Wenn Sie Speicherknoten zu einer vorhandenen Site hinzufügen oder eine Site hinzufügen, überwachen Sie die Cassandra-Phasen, die auftreten, wenn Dienste auf den neuen Grid-Knoten gestartet werden.

Starten Sie während der Phasen „Erweitern des Cassandra-Clusters“ oder „Starten von Cassandra und Streamen von Daten“ keine Speicherknoten neu. Die Ausführung dieser Schritte kann für jeden neuen Speicherknoten mehrere Stunden dauern, insbesondere wenn vorhandene Speicherknoten eine große Menge an Objektmetadaten enthalten.

Hinzufügen von Speicherknoten

Wenn Sie einer vorhandenen Site Speicherknoten hinzufügen, überprüfen Sie den Prozentsatz, der in der Statusmeldung „Cassandra wird gestartet und Daten werden gestreamt“ angezeigt wird.



Dieser Prozentsatz schätzt, wie vollständig der Cassandra-Streaming-Vorgang ist, basierend auf der Gesamtmenge der verfügbaren Cassandra-Daten und der Menge, die bereits auf den neuen Knoten geschrieben wurde.

Site hinzufügen

Wenn Sie eine neue Site hinzufügen, verwenden Sie `nodetool status` um den Fortschritt des Cassandra-Streamings zu überwachen und zu sehen, wie viele Metadaten während der Phase „Erweitern des Cassandra-Clusters“ auf die neue Site kopiert wurden. Die gesamte Datenlast auf der neuen Site sollte etwa 20 % der Gesamtdatenlast einer aktuellen Site betragen.

10. Überwachen Sie die Erweiterung weiter, bis alle Aufgaben abgeschlossen sind und die Schaltfläche **Erweiterung konfigurieren** erneut angezeigt wird.

Nach Abschluss

Führen Sie je nachdem, welche Arten von Grid-Knoten Sie hinzugefügt haben, zusätzliche Integrations- und Konfigurationsschritte durch. Sehen "Konfigurationsschritte nach der Erweiterung" .

Erweitertes System konfigurieren

Konfigurationsschritte nach der Erweiterung

Nach Abschluss einer Erweiterung müssen Sie zusätzliche Integrations- und Konfigurationsschritte durchführen.

Informationen zu diesem Vorgang

Sie müssen die unten aufgeführten Konfigurationsaufgaben für die Grid-Knoten oder Sites abschließen, die Sie Ihrer Erweiterung hinzufügen. Einige Aufgaben sind möglicherweise optional, je nachdem, welche Optionen Sie bei der Installation und Verwaltung Ihres Systems ausgewählt haben und wie Sie die während der Erweiterung hinzugefügten Knoten und Sites konfigurieren möchten.

Schritte

1. Wenn Sie eine Site hinzugefügt haben:
   - "Erstellen eines Speicherpools"für den Standort und jede Speicherklasse, die Sie für die neuen Speicherknoten ausgewählt haben.
   - Bestätigen Sie, dass die ILM-Richtlinie die neuen Anforderungen erfüllt. Wenn Regeländerungen erforderlich sind,"neue Regeln erstellen" Und"Aktualisieren Sie die ILM-Richtlinie" . Wenn die Regeln bereits richtig sind,"eine neue Richtlinie aktivieren" ohne Regeländerungen, um sicherzustellen, dass StorageGRID die neuen Knoten verwendet.
   - Stellen Sie sicher, dass von dieser Site aus auf die Network Time Protocol (NTP)-Server zugegriffen werden kann. Sehen "NTP-Server verwalten" .

     Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.

2. Wenn Sie einer vorhandenen Site einen oder mehrere Speicherknoten hinzugefügt haben:
   - "Anzeigen von Speicherpooldetails"um zu bestätigen, dass jeder von Ihnen hinzugefügte Knoten in den erwarteten Speicherpools enthalten ist und in den erwarteten ILM-Regeln verwendet wird.
   - Bestätigen Sie, dass die ILM-Richtlinie die neuen Anforderungen erfüllt. Wenn Regeländerungen erforderlich sind,"neue Regeln erstellen" Und"Aktualisieren Sie die ILM-Richtlinie" . Wenn die Regeln bereits richtig sind,"eine neue Richtlinie aktivieren" ohne Regeländerungen, um sicherzustellen, dass StorageGRID die neuen Knoten verwendet.
   - "Überprüfen Sie, ob der Speicherknoten aktiv ist"und in der Lage, Gegenstände zu verschlucken.
   - Wenn Sie nicht die empfohlene Anzahl an Speicherknoten hinzufügen konnten, gleichen Sie die Erasure-Coded-Daten neu aus. Sehen "Neuausgleich von erasure-coded Daten nach dem Hinzufügen von Speicherknoten" .
3. Wenn Sie einen Gateway-Knoten hinzugefügt haben:
   - Wenn Hochverfügbarkeitsgruppen (HA) für Clientverbindungen verwendet werden, fügen Sie den Gateway-Knoten optional zu einer HA-Gruppe hinzu. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Sehen "Konfigurieren von Hochverfügbarkeitsgruppen" .
4. Wenn Sie einen Admin-Knoten hinzugefügt haben:
   a. Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, erstellen Sie eine Vertrauensstellung der vertrauenden Seite für den neuen Admin-Knoten. Sie können sich erst beim Knoten anmelden, wenn Sie diese Vertrauensstellung der vertrauenden Seite erstellt haben. Sehen "Konfigurieren der einmaligen Anmeldung" .
   b. Wenn Sie den Load Balancer-Dienst auf Admin-Knoten verwenden möchten, fügen Sie den neuen Admin-Knoten optional einer HA-Gruppe hinzu. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Sehen "Konfigurieren von Hochverfügbarkeitsgruppen" .

c. Kopieren Sie optional die Admin-Knoten-Datenbank vom primären Admin-Knoten auf den Erweiterungs-Admin-Knoten, wenn Sie die Attribut- und Prüfinformationen auf jedem Admin-Knoten konsistent halten möchten. Sehen "Kopieren Sie die Admin-Knoten-Datenbank" .

d. Kopieren Sie optional die Prometheus-Datenbank vom primären Admin-Knoten auf den Erweiterungs-Admin-Knoten, wenn Sie die historischen Metriken auf jedem Admin-Knoten konsistent halten möchten. Sehen "Prometheus-Metriken kopieren" .

e. Kopieren Sie optional die vorhandenen Prüfprotokolle vom primären Admin-Knoten auf den Erweiterungs-Admin-Knoten, wenn Sie die historischen Protokollinformationen auf jedem Admin-Knoten konsistent halten möchten. Sehen "Audit-Protokolle kopieren" .

5. Um zu überprüfen, ob Erweiterungsknoten mit einem nicht vertrauenswürdigen Client-Netzwerk hinzugefügt wurden, oder um zu ändern, ob das Client-Netzwerk eines Knotens nicht vertrauenswürdig oder vertrauenswürdig ist, gehen Sie zu **KONFIGURATION** > **Sicherheit** > **Firewall-Steuerung**.

   Wenn das Client-Netzwerk auf dem Erweiterungsknoten nicht vertrauenswürdig ist, müssen Verbindungen zum Knoten im Client-Netzwerk über einen Load Balancer-Endpunkt hergestellt werden. Sehen"Konfigurieren von Load Balancer-Endpunkten" Und"Verwalten von Firewall-Steuerelementen" .

6. Konfigurieren Sie den DNS.

   Wenn Sie die DNS-Einstellungen für jeden Grid-Knoten separat angegeben haben, müssen Sie für die neuen Knoten benutzerdefinierte DNS-Einstellungen pro Knoten hinzufügen. Sehen "DNS-Konfiguration für einzelnen Grid-Knoten ändern" .

Um einen ordnungsgemäßen Betrieb sicherzustellen, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, ist es möglich, dass aufgrund bekannter Betriebssystembeschränkungen auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie"Passen Sie die DNS-Serverliste an" für einzelne Knoten (normalerweise alle Knoten an einem Standort), einen anderen Satz von bis zu drei DNS-Servern zu verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein isolierter Standort die FQDNs für externe Ziele auflösen kann.

Überprüfen Sie, ob der Speicherknoten aktiv ist

Nachdem ein Erweiterungsvorgang zum Hinzufügen neuer Speicherknoten abgeschlossen ist, sollte das StorageGRID -System automatisch mit der Verwendung der neuen Speicherknoten beginnen. Sie müssen das StorageGRID -System verwenden, um zu überprüfen, ob der neue Speicherknoten aktiv ist.

Schritte

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Wählen Sie **KNOTEN** > ***Erweiterungsspeicherknoten*** > **Speicher**.
3. Positionieren Sie den Cursor über dem Diagramm **Benutzter Speicher – Objektdaten**, um den Wert für **Benutzt** anzuzeigen. Dabei handelt es sich um die Menge des insgesamt nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
4. Überprüfen Sie, ob der Wert von **Verwendet** zunimmt, wenn Sie den Cursor im Diagramm nach rechts bewegen.

Admin-Knoten-Datenbank kopieren

Wenn Sie Admin-Knoten über ein Erweiterungsverfahren hinzufügen, können Sie optional die Datenbank vom primären Admin-Knoten auf den neuen Admin-Knoten kopieren. Durch das Kopieren der Datenbank können Sie historische Informationen zu Attributen, Warnungen und Alarmen behalten.

Bevor Sie beginnen

- Sie haben die erforderlichen Erweiterungsschritte zum Hinzufügen eines Admin-Knotens abgeschlossen.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Der Aktivierungsprozess der StorageGRID -Software erstellt eine leere Datenbank für den NMS-Dienst auf dem Erweiterungs-Admin-Knoten. Wenn der NMS-Dienst auf dem Erweiterungs-Admin-Knoten startet, zeichnet er Informationen für Server und Dienste auf, die derzeit Teil des Systems sind oder später hinzugefügt werden. Diese Admin-Knoten-Datenbank enthält die folgenden Informationen:

- Alarmverlauf
- Historische Attributdaten, die in Diagrammen im Legacy-Stil auf der Seite „Knoten“ verwendet werden

Um sicherzustellen, dass die Admin-Knoten-Datenbank zwischen den Knoten konsistent ist, können Sie die Datenbank vom primären Admin-Knoten auf den Erweiterungs-Admin-Knoten kopieren.

> ⓘ Das Kopieren der Datenbank vom primären Admin-Knoten (dem*Quell-Admin-Knoten*) auf einen Erweiterungs-Admin-Knoten kann mehrere Stunden dauern. Während dieser Zeit ist der Grid Manager nicht erreichbar.

Führen Sie diese Schritte aus, um den MI-Dienst und den Management-API-Dienst sowohl auf dem primären Admin-Knoten als auch auf dem Erweiterungs-Admin-Knoten zu stoppen, bevor Sie die Datenbank kopieren.

Schritte

1. Führen Sie die folgenden Schritte auf dem primären Admin-Knoten aus:
   a. Melden Sie sich beim Admin-Knoten an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   b. Führen Sie den folgenden Befehl aus: `recover-access-points`
   c. Geben Sie die Bereitstellungspassphrase ein.
   d. Beenden Sie den MI-Dienst: `service mi stop`
   e. Stoppen Sie den Dienst Management Application Program Interface (mgmt-api): `service mgmt-api stop`
2. Führen Sie die folgenden Schritte auf dem Erweiterungsadministratorknoten aus:

a. Melden Sie sich beim Erweiterungsadministratorknoten an:

   i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

   ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

   iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

   iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

b. Beenden Sie den MI-Dienst: `service mi stop`

c. Stoppen Sie den mgmt-api-Dienst: `service mgmt-api stop`

d. Fügen Sie dem SSH-Agenten den privaten SSH-Schlüssel hinzu. Eingeben:`ssh-add`

e. Geben Sie das SSH-Zugriffskennwort ein, das im `Passwords.txt` Datei.

f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten zum Erweiterungs-Admin-Knoten: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Bestätigen Sie bei der entsprechenden Aufforderung, dass Sie die MI-Datenbank auf dem Erweiterungsadministratorknoten überschreiben möchten.

   Die Datenbank und ihre historischen Daten werden in den Erweiterungs-Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den Erweiterungs-Admin-Knoten.

h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel aus dem SSH-Agenten. Eingeben:`ssh-add -D`

3. Starten Sie die Dienste auf dem primären Admin-Knoten neu: `service servermanager start`

Prometheus-Metriken kopieren

Nachdem Sie einen neuen Admin-Knoten hinzugefügt haben, können Sie optional die von Prometheus verwalteten historischen Metriken vom primären Admin-Knoten auf den neuen Admin-Knoten kopieren. Durch das Kopieren der Metriken wird sichergestellt, dass die historischen Metriken zwischen den Admin-Knoten konsistent sind.

Bevor Sie beginnen

- Der neue Admin-Knoten ist installiert und läuft.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Wenn Sie einen Admin-Knoten hinzufügen, erstellt der Softwareinstallationsprozess eine neue Prometheus-Datenbank. Sie können die historischen Metriken zwischen den Knoten konsistent halten, indem Sie die Prometheus-Datenbank vom primären Admin-Knoten (dem *Quell-Admin-Knoten*) auf den neuen Admin-Knoten kopieren.

> Das Kopieren der Prometheus-Datenbank kann eine Stunde oder länger dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während die Dienste auf dem Quell-Admin-Knoten gestoppt sind.

Schritte

1. Melden Sie sich beim Quelladministratorknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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.
2. Stoppen Sie den Prometheus-Dienst vom Quell-Admin-Knoten aus: `service prometheus stop`
3. Führen Sie auf dem neuen Admin-Knoten die folgenden Schritte aus:
   a. Melden Sie sich beim neuen Admin-Knoten an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   b. Stoppen Sie den Prometheus-Dienst: `service prometheus stop`
   c. Fügen Sie dem SSH-Agenten den privaten SSH-Schlüssel hinzu. Eingeben:`ssh-add`
   d. Geben Sie das SSH-Zugriffskennwort ein, das im `Passwords.txt` Datei.
   e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Knoten auf den neuen Admin-Knoten: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Drücken Sie bei der entsprechenden Aufforderung die Eingabetaste, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem neuen Admin-Knoten löschen möchten.

      Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den neuen Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den neuen Admin-Knoten. Es erscheint folgender Status:

```
Database cloned, starting services
```

   a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel aus dem SSH-Agenten. Eingeben:

```
ssh-add -D
```

4. Starten Sie den Prometheus-Dienst auf dem Quell-Admin-Knoten neu.

```
service prometheus start
```

Audit-Protokolle kopieren

Wenn Sie über ein Erweiterungsverfahren einen neuen Admin-Knoten hinzufügen, protokolliert sein AMS-Dienst nur Ereignisse und Aktionen, die nach dem Beitritt zum System auftreten. Bei Bedarf können Sie Audit-Protokolle von einem zuvor installierten Admin-Knoten auf den neuen Erweiterungs-Admin-Knoten kopieren, sodass dieser mit dem Rest des StorageGRID -Systems synchronisiert ist.

Bevor Sie beginnen

- Sie haben die erforderlichen Erweiterungsschritte zum Hinzufügen eines Admin-Knotens abgeschlossen.
- Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Um historische Audit-Meldungen auf einem neuen Admin-Knoten verfügbar zu machen, müssen Sie die Audit-Protokolldateien manuell von einem vorhandenen Admin-Knoten auf den Erweiterungs-Admin-Knoten kopieren.

> Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf den Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn einer der folgenden Punkte zutrifft:
>
> - Sie haben einen externen Syslog-Server konfiguriert und Prüfprotokolle werden jetzt an den Syslog-Server statt an Admin-Knoten gesendet.
> - Sie haben ausdrücklich angegeben, dass Prüfmeldungen nur auf den lokalen Knoten gespeichert werden sollen, die sie generiert haben.
>
> Sehen"Konfigurieren von Überwachungsmeldungen und Protokollzielen" für Details.

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. Stoppen Sie den AMS-Dienst, um zu verhindern, dass er eine neue Datei erstellt: `service ams stop`
3. Navigieren Sie zum Audit-Exportverzeichnis:

   ```
   cd /var/local/log
   ```

4. Benennen Sie die Quelle um `audit.log` Datei, um sicherzustellen, dass die Datei auf dem Erweiterungs-Admin-Knoten, auf den Sie sie kopieren, nicht überschrieben wird:

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```

5. Kopieren Sie alle Audit-Protokolldateien an den Zielspeicherort auf dem Erweiterungsadministratorknoten:

   ```
   scp -p * IP_address:/var/local/log
   ```

6. Wenn Sie nach der Passphrase für `/root/.ssh/id_rsa` , geben Sie das SSH-Zugriffskennwort für den primären Admin-Knoten ein, der in der `Passwords.txt` Datei.
7. Wiederherstellen des Originals `audit.log` Datei:

```
mv new_name.txt audit.log
```

8. Starten Sie den AMS-Dienst:

```
service ams start
```

9. Vom Server abmelden:

```
exit
```

10. Melden Sie sich beim Erweiterungsadministratorknoten an:
    a. Geben Sie den folgenden Befehl ein: `ssh admin@expansion_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 `#` .

11. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen für die Audit-Protokolldateien:

```
cd /var/local/log

chown ams-user:bycast *
```

12. Vom Server abmelden:

```
exit
```

Neuausgleich von erasure-coded Daten nach dem Hinzufügen von Speicherknoten

Nachdem Sie Speicherknoten hinzugefügt haben, können Sie das Erasure-Coding-(EC)-Neuausgleichsverfahren verwenden, um Erasure-Coding-Fragmente zwischen den vorhandenen und neuen Speicherknoten neu zu verteilen.

Bevor Sie beginnen

- Sie haben die Erweiterungsschritte zum Hinzufügen der neuen Speicherknoten abgeschlossen.
- Sie haben die"Überlegungen zum Neuausgleich von Erasure-Codierten Daten" .
- Sie verstehen, dass replizierte Objektdaten durch dieses Verfahren nicht verschoben werden und dass das EC-Neuausgleichsverfahren bei der Bestimmung, wohin Erasure-Coded-Daten verschoben werden sollen, die Nutzung der replizierten Daten auf jedem Speicherknoten nicht berücksichtigt.
- Sie haben die `Passwords.txt` Datei.

Was passiert, wenn diese Prozedur ausgeführt wird?

Bevor Sie mit dem Verfahren beginnen, beachten Sie Folgendes:

- Der EC-Neuausgleichsvorgang wird nicht gestartet, wenn ein oder mehrere Volumes offline (nicht gemountet) sind oder wenn sie online (gemountet) sind, sich aber in einem Fehlerzustand befinden.
- Das EC-Neuausgleichsverfahren reserviert vorübergehend eine große Menge an Speicherplatz.

Möglicherweise werden Speicherwarnungen ausgelöst, die jedoch nach Abschluss der Neuverteilung behoben werden. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Neuausgleichsvorgang fehl. Speicherreservierungen werden freigegeben, wenn der EC-Neuausgleichsvorgang abgeschlossen ist, unabhängig davon, ob der Vorgang fehlgeschlagen oder erfolgreich war.

- Wenn ein Volume offline geht, während der EC-Neuausgleichsvorgang läuft, wird der Neuausgleichsvorgang beendet. Alle bereits verschobenen Datenfragmente verbleiben an ihren neuen Speicherorten und es gehen keine Daten verloren.

  Sie können den Vorgang erneut ausführen, nachdem alle Volumes wieder online sind.

- Wenn das EC-Neuausgleichsverfahren ausgeführt wird, kann die Leistung von ILM-Vorgängen und S3-Client-Vorgängen beeinträchtigt werden.

> ⓘ S3-API-Operationen zum Hochladen von Objekten (oder Objektteilen) können während des EC-Neuausgleichsvorgangs fehlschlagen, wenn ihre Ausführung mehr als 24 Stunden dauert. PUT-Vorgänge mit langer Dauer schlagen fehl, wenn die anwendbare ILM-Regel bei der Aufnahme eine ausgewogene oder strikte Platzierung verwendet. Der folgende Fehler wird gemeldet: `500 Internal Server Error.`

- Während dieses Vorgangs ist die Speicherkapazität aller Knoten auf 80 % begrenzt. Knoten, die dieses Limit überschreiten, aber immer noch unterhalb der Zieldatenpartition speichern, werden von Folgendem ausgeschlossen:
  - Der Site-Ungleichgewichtswert
  - Alle Bedingungen für die Auftragserfüllung

> ⓘ Die Zieldatenpartition wird berechnet, indem die Gesamtdaten für eine Site durch die Anzahl der Knoten geteilt werden.

- **Bedingungen für die Auftragserfüllung**. Der EC-Neuausgleichsvorgang gilt als abgeschlossen, wenn eine der folgenden Bedingungen zutrifft:
  - Es können keine weiteren Erasure-Coded-Daten verschoben werden.
  - Die Daten in allen Knoten liegen innerhalb einer 5 %igen Abweichung von der Zieldatenpartition.
  - Das Verfahren läuft seit 30 Tagen.

Schritte

1. Überprüfen Sie die aktuellen Objektspeicherdetails für die Site, die Sie neu ausbalancieren möchten.
   a. Wählen Sie **NODES**.
   b. Wählen Sie den ersten Speicherknoten am Standort aus.
   c. Wählen Sie die Registerkarte **Speicher**.
   d. Positionieren Sie den Cursor über dem Diagramm „Verwendeter Speicher – Objektdaten“, um die aktuelle Menge der replizierten Daten und der löschcodierten Daten auf dem Speicherknoten anzuzeigen.
   e. Wiederholen Sie diese Schritte, um die anderen Speicherknoten am Standort anzuzeigen.
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. Starten Sie den Vorgang:

`rebalance-data start --site "*site-name*"

Geben Sie für „*site-name*“ die erste Site an, an der Sie einen oder mehrere neue Speicherknoten hinzugefügt haben. Beifügen `site-name` in Anführungszeichen.

Das EC-Neuausgleichsverfahren wird gestartet und eine Job-ID wird zurückgegeben.

4. Kopieren Sie die Job-ID.
5. Überwachen Sie den Status des EC-Neuausgleichsverfahrens.

◦ So zeigen Sie den Status eines einzelnen EC-Neuausgleichsverfahrens an:

`rebalance-data status --job-id *job-id*`

Für *`job-id`* Geben Sie die ID an, die beim Starten des Verfahrens zurückgegeben wurde.

◦ So zeigen Sie den Status des aktuellen EC-Neuausgleichsverfahrens und aller zuvor abgeschlossenen Verfahren an:

`rebalance-data status`

So erhalten Sie Hilfe zum Befehl „rebalance-data“:

`rebalance-data --help`

6. Führen Sie je nach zurückgegebenem Status weitere Schritte aus:

◦ Wenn `State` Ist `In progress` , der EC-Neuausgleichsvorgang läuft noch. Sie sollten den Vorgang regelmäßig überwachen, bis er abgeschlossen ist.

Verwenden Sie die `Site Imbalance` Wert, um zu beurteilen, wie unausgewogen die Nutzung von Erasure-Code-Daten über die Speicherknoten am Standort hinweg ist. Dieser Wert kann zwischen 1,0 und 0 liegen, wobei 0 bedeutet, dass die Datennutzung durch Erasure Coding über alle Speicherknoten am Standort hinweg vollständig ausgeglichen ist.

Der EC-Neuausgleichsjob gilt als abgeschlossen und wird beendet, wenn die Daten in allen Knoten innerhalb einer Abweichung von 5 % von der Zieldatenpartition liegen.

◦ Wenn `State` Ist `Success` , optionalObjektspeicher überprüfen um die aktualisierten Details für die Site anzuzeigen.

Löschcodierte Daten sollten jetzt gleichmäßiger auf die Speicherknoten am Standort verteilt sein.

◦ Wenn `State` Ist `Failure` :

i. Bestätigen Sie, dass alle Speicherknoten am Standort mit dem Netz verbunden sind.

ii. Suchen Sie nach Warnungen, die diese Speicherknoten beeinträchtigen könnten, und beheben Sie diese.

iii. Starten Sie den EC-Neuausgleichsvorgang neu:

```
rebalance-data start --job-id job-id
```

iv. Status anzeigendes neuen Verfahrens. Wenn `State` ist immer noch `Failure` , wenden Sie sich an den technischen Support.

7. Wenn das EC-Neuausgleichsverfahren zu viel Last erzeugt (z. B. sind Aufnahmevorgänge betroffen), unterbrechen Sie das Verfahren.

```
rebalance-data pause --job-id job-id
```

8. Wenn Sie den EC-Neuausgleichsvorgang beenden müssen (z. B. um ein StorageGRID -Software-Upgrade durchzuführen), geben Sie Folgendes ein:

```
rebalance-data terminate --job-id job-id
```

> Wenn Sie einen EC-Neuausgleichsvorgang beenden, verbleiben alle bereits verschobenen Datenfragmente an ihren neuen Speicherorten. Die Daten werden nicht an den ursprünglichen Speicherort zurückverschoben.

9. Wenn Sie Erasure Coding an mehr als einem Standort verwenden, führen Sie dieses Verfahren für alle anderen betroffenen Standorte aus.

Fehlerbehebung bei der Erweiterung

Wenn während des Grid-Erweiterungsprozesses Fehler auftreten, die Sie nicht beheben können, oder wenn eine Grid-Aufgabe fehlschlägt, sammeln Sie die Protokolldateien und wenden Sie sich an den technischen Support.

Bevor Sie sich an den technischen Support wenden, sammeln Sie die erforderlichen Protokolldateien, um die Fehlerbehebung zu unterstützen.

Schritte

1. Stellen Sie eine Verbindung zum Erweiterungsknoten her, bei dem Fehler aufgetreten sind:

   a. Geben Sie den folgenden Befehl ein:`ssh -p 8022 admin@grid_node_IP`

   > Port 8022 ist der SSH-Port des Basisbetriebssystems, während Port 22 der SSH-Port der Container-Engine ist, auf der StorageGRID ausgeführt wird.

   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.

   Nachdem Sie sich als Root angemeldet haben, ändert sich die Eingabeaufforderung von `$` Zu `#` .

2. Rufen Sie je nach dem Stadium, in dem sich die Installation befindet, eines der folgenden Protokolle ab, die auf dem Grid-Knoten verfügbar sind:

Plattform	Protokolle
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf`(für jeden ausgefallenen Knoten) • `/var/log/storagegrid/nodes/<node-name>.log`(für jeden ausgefallenen Knoten; existiert möglicherweise nicht)

Warten Sie ein StorageGRID -System

Netzwartung

Zu den Grid-Wartungsaufgaben gehören die Außerbetriebnahme eines Knotens oder Standorts, die Umbenennung eines Grids, Knotens oder Standorts und die Wartung von Netzwerken. Sie können auch Host- und Middleware-Prozeduren sowie Grid-Knoten-Prozeduren durchführen.

> ⓘ In diesen Anweisungen bezieht sich „Linux“ auf eine Bereitstellung von Red Hat® Enterprise Linux®, Ubuntu® oder Debian®. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Bevor Sie beginnen

- Sie verfügen über umfassende Kenntnisse des StorageGRID -Systems.
- Sie haben die Topologie Ihres StorageGRID -Systems überprüft und verstehen die Grid-Konfiguration.
- Sie verstehen, dass Sie alle Anweisungen genau befolgen und alle Warnungen beachten müssen.
- Sie verstehen, dass nicht beschriebene Wartungsverfahren nicht unterstützt werden oder die Inanspruchnahme eines Dienstes erfordern.

Wartungsverfahren für Geräte

Informationen zu Hardwareverfahren finden Sie im "Wartungsanweisungen für Ihr StorageGRID -Gerät" .

Wiederherstellungspaket herunterladen

Mit der Wiederherstellungspaketdatei können Sie das StorageGRID -System wiederherstellen, wenn ein Fehler auftritt.

Bevor Sie beginnen

- Vom primären Admin-Knoten aus werden Sie beim Grid Manager mit einem"unterstützter Webbrowser" .
- Sie haben die Bereitstellungspassphrase.
- Du hast"spezifische Zugriffsberechtigungen" .

Laden Sie die aktuelle Wiederherstellungspaketdatei herunter, bevor Sie Änderungen an der Netztopologie des StorageGRID -Systems vornehmen oder bevor Sie die Software aktualisieren. Laden Sie dann eine neue Kopie des Wiederherstellungspakets herunter, nachdem Sie Änderungen an der Netztopologie vorgenommen oder die Software aktualisiert haben.

Schritte

1. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
2. Geben Sie die Bereitstellungspassphrase ein und wählen Sie **Download starten**.

   Der Download beginnt sofort.

3. Wenn der Download abgeschlossen ist, öffnen Sie die `.zip` Datei und bestätigen Sie, dass Sie auf den

Inhalt zugreifen können, einschließlich der `Passwords.txt` Datei.

4. Kopieren Sie die heruntergeladene 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.

Knoten oder Site außer Betrieb nehmen

Knoten oder Site außer Betrieb nehmen

Sie können ein Außerbetriebnahmeverfahren durchführen, um Grid-Knoten oder einen gesamten Standort dauerhaft aus dem StorageGRID -System zu entfernen.

Um einen Grid-Knoten oder eine Site zu entfernen, führen Sie eines der folgenden Außerbetriebnahmeverfahren durch:

- Führen Sie einen"Außerbetriebnahme von Netzknoten" um einen oder mehrere Knoten zu entfernen, die sich an einem oder mehreren Standorten befinden können. Die Knoten, die Sie entfernen, können online und mit dem StorageGRID -System verbunden sein oder offline und getrennt.
- Führen Sie einen"Stilllegung des Standorts" um eine Site zu entfernen. Sie führen eine **Außerbetriebnahme der verbundenen Site** durch, wenn alle Knoten mit StorageGRID verbunden sind. Sie führen eine **Außerbetriebnahme einer getrennten Site** durch, wenn alle Knoten von StorageGRID getrennt sind. Wenn die Site eine Mischung aus verbundenen und getrennten Knoten enthält, müssen Sie alle Offline-Knoten wieder online bringen.

> Bevor Sie eine getrennte Site-Außerbetriebnahme durchführen, wenden Sie sich an Ihren NetApp Kundenbetreuer. NetApp überprüft Ihre Anforderungen, bevor alle Schritte im Assistenten „Site außer Betrieb nehmen“ aktiviert werden. Sie sollten nicht versuchen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie glauben, dass es möglich sein könnte, die Site wiederherzustellen oder Objektdaten von der Site wiederherzustellen.

Knoten außer Betrieb nehmen

Außerbetriebnahme von Netzknoten

Mit dem Verfahren zur Knoten-Außerbetriebnahme können Sie einen oder mehrere Grid-Knoten an einem oder mehreren Standorten entfernen. Sie können den primären Admin-Knoten nicht außer Betrieb nehmen.

Wann sollte ein Knoten außer Betrieb genommen werden?

Verwenden Sie das Verfahren zur Außerbetriebnahme von Knoten, wenn einer der folgenden Punkte zutrifft:

- Sie haben in einer Erweiterung einen größeren Speicherknoten hinzugefügt und möchten einen oder mehrere kleinere Speicherknoten entfernen, dabei aber gleichzeitig Objekte beibehalten.

Wenn Sie ein älteres Gerät durch ein neueres Gerät ersetzen möchten, bedenken Sie "Klonen des Appliance-Knotens" anstatt bei einer Erweiterung ein neues Gerät hinzuzufügen und das alte Gerät anschließend außer Betrieb zu nehmen.

- Sie benötigen insgesamt weniger Speicherplatz.
- Sie benötigen keinen Gateway-Knoten mehr.
- Sie benötigen keinen nicht primären Admin-Knoten mehr.
- Ihr Grid enthält einen getrennten Knoten, den Sie nicht wiederherstellen oder wieder online bringen können.
- Ihr Raster enthält einen Archivknoten.

So wird ein Knoten außer Betrieb genommen

Sie können verbundene oder getrennte Netzknoten außer Betrieb nehmen.

Außerbetriebnahme verbundener Knoten

Im Allgemeinen sollten Sie Grid-Knoten nur dann außer Betrieb nehmen, wenn sie mit dem StorageGRID -System verbunden sind und nur, wenn alle Knoten in einem normalen Zustand sind (grüne Symbole auf den Seiten **NODES** und auf der Seite **Decommission Nodes**).

Anweisungen hierzu finden Sie unter"Angeschlossene Netzknoten außer Betrieb nehmen" .

Getrennte Knoten außer Betrieb nehmen

In einigen Fällen müssen Sie möglicherweise einen Grid-Knoten außer Betrieb nehmen, der derzeit nicht mit dem Grid verbunden ist (einen Knoten, dessen Zustand unbekannt oder administrativ ausgefallen ist).

Anweisungen hierzu finden Sie unter"Abgeschaltete Netzknoten außer Betrieb nehmen" .

Was ist vor der Außerbetriebnahme eines Knotens zu beachten?

Bevor Sie eines der Verfahren durchführen, überprüfen Sie die Überlegungen für jeden Knotentyp:

- "Überlegungen zur Außerbetriebnahme von Admin- oder Gateway-Knoten"
- "Überlegungen zur Außerbetriebnahme von Speicherknoten"

Überlegungen zur Außerbetriebnahme von Admin- oder Gateway-Knoten

Überprüfen Sie die Überlegungen zur Außerbetriebnahme eines Admin-Knotens oder Gateway-Knotens.

Überlegungen zum Admin-Knoten

- Sie können den primären Admin-Knoten nicht außer Betrieb nehmen.
- Sie können einen Admin-Knoten nicht außer Betrieb nehmen, wenn eine seiner Netzwerkschnittstellen Teil einer Hochverfügbarkeitsgruppe (HA) ist. Sie müssen zuerst die Netzwerkschnittstellen aus der HA-Gruppe entfernen. Siehe die Anweisungen für"Verwalten von HA-Gruppen" .
- Bei Bedarf können Sie ILM-Richtlinien sicher ändern, während Sie einen Admin-Knoten außer Betrieb nehmen.
- Wenn Sie einen Admin-Knoten außer Betrieb nehmen und Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, müssen Sie daran denken, die Vertrauensstellung der vertrauenden Seite des Knotens

aus Active Directory Federation Services (AD FS) zu entfernen.

- Wenn Sie"Netzverbund" , stellen Sie sicher, dass die IP-Adresse des Knotens, den Sie außer Betrieb nehmen, nicht für eine Grid-Föderation-Verbindung angegeben wurde.
- Wenn Sie einen getrennten Admin-Knoten außer Betrieb nehmen, gehen die Prüfprotokolle dieses Knotens verloren. Diese Protokolle sollten jedoch auch auf dem primären Admin-Knoten vorhanden sein.

Überlegungen zum Gateway-Knoten

- Sie können einen Gateway-Knoten nicht außer Betrieb nehmen, wenn eine seiner Netzwerkschnittstellen Teil einer Hochverfügbarkeitsgruppe (HA) ist. Sie müssen zuerst die Netzwerkschnittstellen aus der HA-Gruppe entfernen. Siehe die Anweisungen für"Verwalten von HA-Gruppen" .
- Bei Bedarf können Sie ILM-Richtlinien sicher ändern, während Sie einen Gateway-Knoten außer Betrieb nehmen.
- Wenn Sie"Netzverbund" , stellen Sie sicher, dass die IP-Adresse des Knotens, den Sie außer Betrieb nehmen, nicht für eine Grid-Föderation-Verbindung angegeben wurde.
- Sie können einen Gateway-Knoten sicher außer Betrieb nehmen, während er getrennt ist.

Überlegungen zu Speicherknoten

Überlegungen zur Außerbetriebnahme von Speicherknoten

Überlegen Sie vor der Außerbetriebnahme eines Speicherknotens, ob Sie den Knoten stattdessen klonen können. Wenn Sie sich dann für die Außerbetriebnahme des Knotens entscheiden, überprüfen Sie, wie StorageGRID während des Außerbetriebnahmevorgangs Objekte und Metadaten verwaltet.

Wann sollte ein Knoten geklont werden, anstatt ihn außer Betrieb zu nehmen?

Wenn Sie einen älteren Appliance-Speicherknoten durch eine neuere oder größere Appliance ersetzen möchten, sollten Sie das Klonen des Appliance-Knotens in Betracht ziehen, anstatt bei einer Erweiterung eine neue Appliance hinzuzufügen und die alte Appliance dann außer Betrieb zu nehmen.

Durch das Klonen von Appliance-Knoten können Sie einen vorhandenen Appliance-Knoten problemlos durch eine kompatible Appliance am selben StorageGRID Standort ersetzen. Der Klonvorgang überträgt alle Daten auf das neue Gerät, nimmt das neue Gerät in Betrieb und belässt das alte Gerät in einem Zustand vor der Installation.

Sie können einen Appliance-Knoten klonen, wenn Sie Folgendes benötigen:

- Ersetzen Sie ein Gerät, das das Ende seiner Lebensdauer erreicht.
- Aktualisieren Sie einen vorhandenen Knoten, um die Vorteile der verbesserten Appliance-Technologie zu nutzen.
- Erhöhen Sie die Grid-Speicherkapazität, ohne die Anzahl der Speicherknoten in Ihrem StorageGRID -System zu ändern.
- Verbessern Sie die Speichereffizienz, beispielsweise durch Ändern des RAID-Modus.

Sehen "Klonen von Appliance-Knoten" für Details.

Überlegungen zu verbundenen Speicherknoten

Überprüfen Sie die Überlegungen zur Außerbetriebnahme eines verbundenen Speicherknotens.

- Sie sollten in einem einzigen Verfahren zur Knoten-Außerbetriebnahme nicht mehr als 10 Speicherknoten außer Betrieb nehmen.
- Das System muss jederzeit genügend Speicherknoten enthalten, um die betrieblichen Anforderungen zu erfüllen, einschließlich der"ADC-Quorum" und die aktive"ILM-Richtlinie" . Um diese Einschränkung zu erfüllen, müssen Sie möglicherweise in einem Erweiterungsvorgang einen neuen Speicherknoten hinzufügen, bevor Sie einen vorhandenen Speicherknoten außer Betrieb nehmen können.

  Seien Sie vorsichtig, wenn Sie Speicherknoten in einem Grid außer Betrieb nehmen, das softwarebasierte Knoten enthält, die nur Metadaten enthalten. Wenn Sie alle Knoten außer Betrieb nehmen, die zum Speichern von *sowohl* Objekten als auch Metadaten konfiguriert sind, wird die Möglichkeit zum Speichern von Objekten aus dem Raster entfernt. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

- Wenn Sie einen Speicherknoten entfernen, werden große Mengen an Objektdaten über das Netzwerk übertragen. Obwohl diese Übertragungen den normalen Systembetrieb nicht beeinträchtigen sollten, können sie sich auf die Gesamtmenge der vom StorageGRID -System verbrauchten Netzwerkbandbreite auswirken.
- Aufgaben im Zusammenhang mit der Außerbetriebnahme von Speicherknoten haben eine niedrigere Priorität als Aufgaben im Zusammenhang mit dem normalen Systembetrieb. Dies bedeutet, dass die Außerbetriebnahme den normalen Betrieb des StorageGRID Systems nicht beeinträchtigt und nicht für einen Zeitraum der Systeminaktivität geplant werden muss. Da die Außerbetriebnahme im Hintergrund erfolgt, lässt sich nur schwer abschätzen, wie lange der Vorgang dauern wird. Im Allgemeinen wird die Außerbetriebnahme schneller abgeschlossen, wenn das System ruhig ist oder wenn jeweils nur ein Speicherknoten entfernt wird.
- Die Außerbetriebnahme eines Speicherknotens kann Tage oder Wochen dauern. Planen Sie diesen Vorgang entsprechend. Obwohl der Außerbetriebnahmeprozess so konzipiert ist, dass er den Systembetrieb nicht beeinträchtigt, kann er andere Verfahren einschränken. Generell sollten Sie alle geplanten Systemupgrades oder -erweiterungen durchführen, bevor Sie Grid-Knoten entfernen.
- Wenn Sie während der Entfernung von Storage Nodes eine weitere Wartung durchführen müssen, können Sie"das Außerbetriebnahmeverfahren unterbrechen" und setzen Sie es fort, nachdem der andere Vorgang abgeschlossen ist.

  > Die Schaltfläche **Pause** ist nur aktiviert, wenn die Phasen der ILM-Auswertung oder der Außerbetriebnahme von Erasure-Coded-Daten erreicht sind. Die ILM-Auswertung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt.

- Sie können auf keinem Grid-Knoten Datenreparaturvorgänge ausführen, während eine Außerbetriebnahmeaufgabe ausgeführt wird.
- Sie sollten keine Änderungen an einer ILM-Richtlinie vornehmen, während ein Speicherknoten außer Betrieb genommen wird.
- Um Daten dauerhaft und sicher zu entfernen, müssen Sie die Laufwerke des Speicherknotens nach Abschluss des Außerbetriebnahmevorgangs löschen.

Überlegungen zu getrennten Speicherknoten

Überprüfen Sie die Überlegungen zur Außerbetriebnahme eines getrennten Speicherknotens.

- Nehmen Sie einen getrennten Knoten niemals außer Betrieb, es sei denn, Sie sind sicher, dass er nicht online gebracht oder wiederhergestellt werden kann.

> Führen Sie dieses Verfahren nicht durch, wenn Sie glauben, dass es möglich sein könnte, Objektdaten vom Knoten wiederherzustellen. Wenden Sie sich stattdessen an den technischen Support, um festzustellen, ob eine Knotenwiederherstellung möglich ist.

- Wenn Sie einen getrennten Speicherknoten außer Betrieb nehmen, verwendet StorageGRID Daten von anderen Speicherknoten, um die Objektdaten und Metadaten zu rekonstruieren, die sich auf dem getrennten Knoten befanden.
- Wenn Sie mehr als einen getrennten Speicherknoten außer Betrieb nehmen, kann es zu Datenverlust kommen. Das System ist möglicherweise nicht in der Lage, Daten zu rekonstruieren, wenn nicht genügend Objektkopien, Erasure-Coded-Fragmente oder Objektmetadaten verfügbar bleiben. Wenn Sie Speicherknoten in einem Grid mit softwarebasierten Knoten, die nur Metadaten speichern, außer Betrieb nehmen, wird durch die Außerbetriebnahme aller Knoten, die zum Speichern von Objekten und Metadaten konfiguriert sind, der gesamte Objektspeicher aus dem Grid entfernt. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

> Wenn Sie über mehr als einen getrennten Speicherknoten verfügen, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu bestimmen.

- Wenn Sie einen getrennten Speicherknoten außer Betrieb nehmen, startet StorageGRID am Ende des Außerbetriebnahmeprozesses Datenreparaturjobs. Diese Jobs versuchen, die Objektdaten und Metadaten zu rekonstruieren, die auf dem getrennten Knoten gespeichert waren.
- Wenn Sie einen getrennten Speicherknoten außer Betrieb nehmen, ist der Außerbetriebnahmevorgang relativ schnell abgeschlossen. Die Ausführung der Datenreparaturjobs kann jedoch Tage oder Wochen dauern und wird durch das Außerbetriebnahmeverfahren nicht überwacht. Sie müssen diese Jobs manuell überwachen und bei Bedarf neu starten. Sehen "Überprüfen Sie die Datenreparaturaufträge" .
- Wenn Sie einen getrennten Speicherknoten außer Betrieb nehmen, der die einzige Kopie eines Objekts enthält, geht das Objekt verloren. Die Datenreparaturjobs können Objekte nur rekonstruieren und wiederherstellen, wenn auf den aktuell verbundenen Speicherknoten mindestens eine replizierte Kopie oder genügend Erasure-Coded-Fragmente vorhanden sind.

Was ist das ADC-Quorum?

Möglicherweise können Sie bestimmte Speicherknoten an einem Standort nicht außer Betrieb nehmen, wenn nach der Außerbetriebnahme zu wenige Administrative Domain Controller (ADC)-Dienste übrig bleiben.

Der ADC-Dienst, der auf einigen Speicherknoten zu finden ist, verwaltet Informationen zur Netztopologie und stellt Konfigurationsdienste für das Netz bereit. Das StorageGRID -System erfordert, dass an jedem Standort und jederzeit ein Quorum an ADC-Diensten verfügbar ist.

Sie können einen Speicherknoten nicht außer Betrieb nehmen, wenn das Entfernen des Knotens dazu führen würde, dass das ADC-Quorum nicht mehr erfüllt wird. Um das ADC-Quorum während einer Außerbetriebnahme zu erfüllen, müssen mindestens drei Speicherknoten an jedem Standort über den ADC-Dienst verfügen. Wenn ein Standort über mehr als drei Speicherknoten mit dem ADC-Dienst verfügt, muss nach der Außerbetriebnahme eine einfache Mehrheit dieser Knoten verfügbar bleiben: `((0.5 * Storage Nodes with ADC) + 1)`

Seien Sie vorsichtig, wenn Sie Speicherknoten in einem Grid außer Betrieb nehmen, das softwarebasierte Knoten enthält, die nur Metadaten enthalten. Wenn Sie alle Knoten außer Betrieb nehmen, die zum Speichern von *sowohl* Objekten als auch Metadaten konfiguriert sind, wird die Möglichkeit zum Speichern von Objekten aus dem Raster entfernt. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

Angenommen, eine Site umfasst derzeit sechs Speicherknoten mit ADC-Diensten und Sie möchten drei Speicherknoten außer Betrieb nehmen. Aufgrund der ADC-Quorumsanforderung müssen Sie die folgenden zwei Außerbetriebnahmeverfahren durchführen:

- Beim ersten Außerbetriebnahmevorgang müssen Sie sicherstellen, dass vier Speicherknoten mit ADC-Diensten verfügbar bleiben: `((0.5 * 6) + 1)` . Dies bedeutet, dass Sie zunächst nur zwei Speicherknoten außer Betrieb nehmen können.
- Im zweiten Außerbetriebnahmeverfahren können Sie den dritten Speicherknoten entfernen, da das ADC-Quorum jetzt nur noch erfordert, dass drei ADC-Dienste verfügbar bleiben: `((0.5 * 4) + 1)` .

Wenn Sie einen Speicherknoten außer Betrieb nehmen müssen, dies aber aufgrund der ADC-Quorum-Anforderung nicht möglich ist, fügen Sie einen neuen Speicherknoten in einem"Erweiterung" und geben Sie an, dass es einen ADC-Dienst haben soll. Nehmen Sie dann den vorhandenen Speicherknoten außer Betrieb.

Überprüfen der ILM-Richtlinie und Speicherkonfiguration

Wenn Sie planen, einen Speicherknoten außer Betrieb zu nehmen, sollten Sie die ILM-Richtlinie Ihres StorageGRID Systems überprüfen, bevor Sie mit dem Außerbetriebnahmeprozess beginnen.

Während der Außerbetriebnahme werden alle Objektdaten vom außer Betrieb genommenen Speicherknoten auf andere Speicherknoten migriert.

Die ILM-Richtlinie, die Sie *während* der Außerbetriebnahme haben, wird auch *nach* der Außerbetriebnahme verwendet. Sie müssen sicherstellen, dass diese Richtlinie Ihren Datenanforderungen sowohl vor Beginn der Außerbetriebnahme als auch nach Abschluss der Außerbetriebnahme entspricht.

Sie sollten die Regeln in jedem"aktive ILM-Richtlinie" um sicherzustellen, dass das StorageGRID -System weiterhin über genügend Kapazität des richtigen Typs und an den richtigen Standorten verfügt, um die Außerbetriebnahme eines Speicherknotens zu ermöglichen.

Beachten Sie Folgendes:

- Wird es ILM-Auswertungsdiensten möglich sein, Objektdaten so zu kopieren, dass die ILM-Regeln eingehalten werden?
- Was passiert, wenn ein Standort während der Stilllegung vorübergehend nicht verfügbar ist? Können zusätzliche Kopien an einem anderen Ort erstellt werden?
- Welche Auswirkungen hat der Außerbetriebnahmeprozess auf die endgültige Verbreitung der Inhalte? Wie beschrieben in"Konsolidieren Sie Speicherknoten" , Du solltest"neue Speicherknoten hinzufügen" bevor Sie alte außer Betrieb nehmen. Wenn Sie nach der Außerbetriebnahme eines kleineren Speicherknotens einen größeren Ersatzspeicherknoten hinzufügen, ist die Kapazität der alten Speicherknoten möglicherweise fast erschöpft und der neue Speicherknoten enthält möglicherweise fast keinen Inhalt. Die meisten Schreibvorgänge für neue Objektdaten würden dann auf den neuen Speicherknoten gerichtet, was die Gesamteffizienz der Systemvorgänge verringern würde.

- Verfügt das System jederzeit über genügend Speicherknoten, um die aktiven ILM-Richtlinien zu erfüllen?

> Eine ILM-Richtlinie, die nicht erfüllt werden kann, führt zu Rückständen und Warnungen und kann den Betrieb des StorageGRID -Systems stoppen.

Überprüfen Sie, ob die vorgeschlagene Topologie, die sich aus dem Außerbetriebnahmeprozess ergibt, der ILM-Richtlinie entspricht, indem Sie die in der Tabelle aufgeführten Bereiche bewerten.

Zu bewertender Bereich	Was ist zu beachten
Verfügbare Kapazität	Wird genügend Speicherkapazität vorhanden sein, um alle im StorageGRID System gespeicherten Objektdaten aufzunehmen, einschließlich der permanenten Kopien der Objektdaten, die derzeit auf dem zu stilllegenden Storage Node gespeichert sind? Wird es für einen angemessenen Zeitraum nach der Stilllegung genügend Kapazität geben, um das erwartete Wachstum der gespeicherten Objektdaten zu bewältigen?
Speicherort	Wenn im StorageGRID -System als Ganzes genügend Kapazität verbleibt, ist die Kapazität dann an den richtigen Standorten, um die Geschäftsregeln des StorageGRID Systems zu erfüllen?
Speichertyp	Wird es nach der Stilllegung genügend Lagerkapazitäten des entsprechenden Typs geben? Beispielsweise können ILM-Regeln Inhalte von einem Speichertyp auf einen anderen verschieben, wenn sie älter werden. In diesem Fall müssen Sie sicherstellen, dass in der endgültigen Konfiguration des StorageGRID -Systems genügend Speicher des entsprechenden Typs verfügbar ist.

Konsolidieren Sie Speicherknoten

Sie können Speicherknoten konsolidieren, um die Anzahl der Speicherknoten für eine Site oder Bereitstellung zu reduzieren und gleichzeitig die Speicherkapazität zu erhöhen.

Wenn Sie Storage Nodes konsolidieren,"Erweitern Sie das StorageGRID -System" durch Hinzufügen neuer Speicherknoten mit größerer Kapazität und anschließende Außerbetriebnahme der alten Speicherknoten mit geringerer Kapazität. Während des Außerbetriebnahmeverfahrens werden Objekte von den alten Speicherknoten auf die neuen Speicherknoten migriert.

> Wenn Sie ältere und kleinere Geräte mit neuen Modellen oder Geräten mit größerer Kapazität konsolidieren, sollten Sie Folgendes bedenken: "Klonen des Appliance-Knotens" (oder verwenden Sie das Klonen von Appliance-Knoten und das Außerbetriebnahmeverfahren, wenn Sie keinen Eins-zu-eins-Ersatz durchführen).

Sie könnten beispielsweise zwei neue Speicherknoten mit größerer Kapazität hinzufügen, um drei ältere Speicherknoten zu ersetzen. Sie würden zunächst das Erweiterungsverfahren verwenden, um die beiden neuen, größeren Speicherknoten hinzuzufügen, und dann das Außerbetriebnahmeverfahren verwenden, um die drei alten Speicherknoten mit geringerer Kapazität zu entfernen.

Indem Sie neue Kapazität hinzufügen, bevor Sie vorhandene Speicherknoten entfernen, stellen Sie eine ausgewogenere Verteilung der Daten im StorageGRID -System sicher. Sie verringern außerdem die Möglichkeit, dass ein vorhandener Speicherknoten über die Speicher-Wasserzeichenebene hinaus geschoben wird.

Mehrere Speicherknoten außer Betrieb nehmen

Wenn Sie mehr als einen Speicherknoten entfernen müssen, können Sie diese entweder nacheinander oder parallel außer Betrieb nehmen.

> Seien Sie vorsichtig, wenn Sie Speicherknoten in einem Grid außer Betrieb nehmen, das softwarebasierte Knoten enthält, die nur Metadaten enthalten. Wenn Sie alle Knoten außer Betrieb nehmen, die zum Speichern von *sowohl* Objekten als auch Metadaten konfiguriert sind, wird die Möglichkeit zum Speichern von Objekten aus dem Raster entfernt. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

- Wenn Sie Speicherknoten nacheinander außer Betrieb nehmen, müssen Sie warten, bis die Außerbetriebnahme des ersten Speicherknotens abgeschlossen ist, bevor Sie mit der Außerbetriebnahme des nächsten Speicherknotens beginnen.
- Wenn Sie Speicherknoten parallel außer Betrieb nehmen, verarbeiten die Speicherknoten gleichzeitig die Außerbetriebnahmeaufgaben für alle außer Betrieb genommenen Speicherknoten. Dies kann dazu führen, dass alle permanenten Kopien einer Datei als „schreibgeschützt“ gekennzeichnet werden, wodurch das Löschen in Rastern, in denen diese Funktion aktiviert ist, vorübergehend deaktiviert wird.

Überprüfen Sie die Datenreparaturaufträge

Bevor Sie einen Grid-Knoten außer Betrieb nehmen, müssen Sie bestätigen, dass keine Datenreparaturjobs aktiv sind. Wenn Reparaturen fehlgeschlagen sind, müssen Sie diese neu starten und abschließen lassen, bevor Sie die Außerbetriebnahme durchführen.

Informationen zu diesem Vorgang

Wenn Sie einen getrennten Speicherknoten außer Betrieb nehmen müssen, führen Sie diese Schritte auch nach Abschluss des Außerbetriebnahmevorgangs aus, um sicherzustellen, dass der Datenreparaturauftrag erfolgreich abgeschlossen wurde. Sie müssen sicherstellen, dass alle Erasure-Coded-Fragmente, die sich auf dem entfernten Knoten befanden, erfolgreich wiederhergestellt wurden.

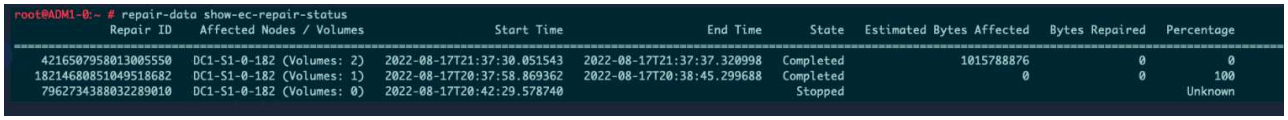
Diese Schritte gelten nur für Systeme mit Erasure-Coded-Objekten.

Schritte

1. Melden Sie sich beim primären Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Auf laufende Reparaturen prüfen: `repair-data show-ec-repair-status`

- Wenn Sie noch nie einen Datenreparaturjob ausgeführt haben, lautet die Ausgabe `No job found`. Sie müssen keine Reparaturarbeiten neu starten.
- Wenn der Datenreparaturauftrag zuvor ausgeführt wurde oder derzeit ausgeführt wird, werden in der Ausgabe Informationen zur Reparatur aufgelistet. Jede Reparatur hat eine eindeutige Reparatur-ID.



> Optional können Sie mit dem Grid Manager laufende Wiederherstellungsprozesse überwachen und einen Wiederherstellungsverlauf anzeigen. Sehen "Wiederherstellen von Objektdaten mit Grid Manager" .

3. Wenn der Staat für alle Reparaturen `Completed` , müssen Sie keine Reparaturarbeiten neu starten.
4. Wenn der Staat für eine Reparatur `Stopped` , müssen Sie die Reparatur neu starten.
   a. Ermitteln Sie die Reparatur-ID für die fehlgeschlagene Reparatur aus der Ausgabe.
   b. Führen Sie den `repair-data start-ec-node-repair` Befehl.

      Verwenden Sie die `--repair-id` Option zum Angeben der Reparatur-ID. Wenn Sie beispielsweise eine Reparatur mit der Reparatur-ID 949292 wiederholen möchten, führen Sie diesen Befehl aus: `repair-data start-ec-node-repair --repair-id 949292`

   c. Verfolgen Sie den Status der EC-Datenreparaturen weiter, bis der Status für alle Reparaturen `Completed` .

Benötigte Materialien zusammenstellen

Bevor Sie die Außerbetriebnahme eines Netzknotens durchführen, müssen Sie die folgenden Informationen einholen.

Artikel	Hinweise
Wiederherstellungspaket `.zip` Datei	Sie müssen"Laden Sie das neueste Wiederherstellungspaket herunter" `.zip` Datei(`sgws-recovery-package-`*`id-revision`*`.zip`). Mit der Wiederherstellungspaketdatei können Sie das System im Falle eines Fehlers wiederherstellen.
`Passwords.txt`Datei	Diese Datei enthält die für den Zugriff auf Grid-Knoten über die Befehlszeile erforderlichen Passwörter und ist im Wiederherstellungspaket enthalten.
Bereitstellungspassphrase	Die Passphrase wird bei der Erstinstallation des StorageGRID -Systems erstellt und dokumentiert. Die Bereitstellungspassphrase ist nicht in der `Passwords.txt` Datei.
Beschreibung der Topologie des StorageGRID -Systems vor der Außerbetriebnahme	Besorgen Sie sich, sofern verfügbar, alle Unterlagen, die die aktuelle Topologie des Systems beschreiben.

Ähnliche Informationen

"Anforderungen an den Webbrowser"

Zugriff auf die Seite „Knoten außer Betrieb nehmen“

Wenn Sie im Grid Manager auf die Seite „Knoten außer Betrieb nehmen“ zugreifen, können Sie auf einen Blick sehen, welche Knoten außer Betrieb genommen werden können.

Bevor Sie beginnen

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

> ⚠ Seien Sie vorsichtig, wenn Sie Speicherknoten in einem Grid außer Betrieb nehmen, das softwarebasierte Knoten enthält, die nur Metadaten enthalten. Wenn Sie alle Knoten außer Betrieb nehmen, die zum Speichern von *sowohl* Objekten als auch Metadaten konfiguriert sind, wird die Möglichkeit zum Speichern von Objekten aus dem Raster entfernt. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

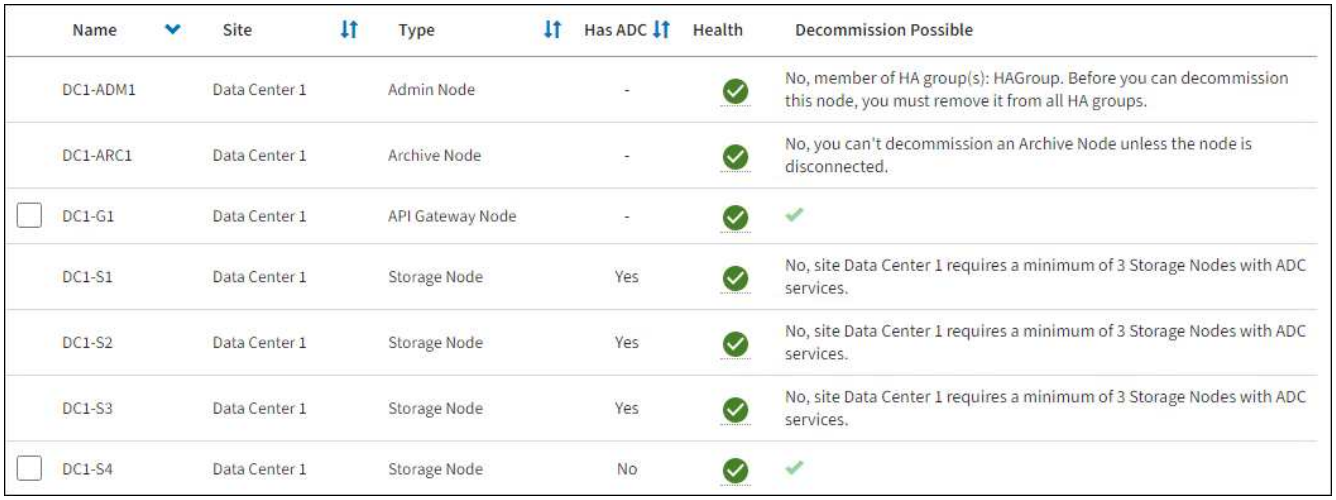
Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Außerbetriebnahme**.
2. Wählen Sie **Knoten außer Betrieb nehmen**.

   Die Seite „Knoten außer Betrieb nehmen“ wird angezeigt. Auf dieser Seite können Sie:

   - Ermitteln Sie, welche Netzknoten aktuell stillgelegt werden können.
   - Sehen Sie den Zustand aller Grid-Knoten
   - Sortieren Sie die Liste in aufsteigender oder absteigender Reihenfolge nach **Name**, **Site**, **Typ** oder **Hat ADC**.
   - Geben Sie Suchbegriffe ein, um bestimmte Knoten schnell zu finden.

     In diesem Beispiel gibt die Spalte „Außerbetriebnahme möglich“ an, dass Sie den Gateway-Knoten und einen der vier Speicherknoten außer Betrieb nehmen können.



Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, you can't decommission an Archive Node unless the node is disconnected.
☐ DC1-G1	Data Center 1	API Gateway Node	-	✓	✓
DC1-S1	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
☐ DC1-S4	Data Center 1	Storage Node	No	✓	✓

3. Überprüfen Sie die Spalte **Außerbetriebnahme möglich** für jeden Knoten, den Sie außer Betrieb nehmen

möchten.

Wenn ein Netzknoten außer Betrieb genommen werden kann, enthält diese Spalte ein grünes Häkchen und die linke Spalte ein Kontrollkästchen. Wenn ein Knoten nicht außer Betrieb genommen werden kann, wird das Problem in dieser Spalte beschrieben. Wenn es mehr als einen Grund gibt, warum ein Knoten nicht außer Betrieb genommen werden kann, wird der schwerwiegendste Grund angezeigt.

Außerbetriebnahme Möglicher Grund	Beschreibung	Schritte zur Lösung
Nein, die Außerbetriebnahme des Knotentyps wird nicht unterstützt.	Sie können den primären Admin-Knoten nicht außer Betrieb nehmen.	Keiner.
Nein, mindestens ein Netzknoten ist getrennt. **Hinweis:** Diese Nachricht wird nur für verbundene Grid-Knoten angezeigt.	Sie können einen verbundenen Grid-Knoten nicht außer Betrieb nehmen, wenn ein beliebiger Grid-Knoten getrennt ist. Die Spalte **Health** enthält eines dieser Symbole für getrennte Grid-Knoten: • (grau): Administrativ ausgefallen • (blau): Unbekannt	Sie müssen alle getrennten Knoten wieder online bringen oder"alle getrennten Knoten außer Betrieb nehmen" bevor Sie einen verbundenen Knoten entfernen können. **Hinweis**: Wenn Ihr Netz mehrere getrennte Knoten enthält, müssen Sie diese gemäß der Software alle gleichzeitig außer Betrieb nehmen, wodurch das Risiko unerwarteter Ergebnisse steigt.
Nein, ein oder mehrere erforderliche Knoten sind derzeit getrennt und müssen wiederhergestellt werden. **Hinweis:** Diese Meldung wird nur für getrennte Grid-Knoten angezeigt.	Sie können einen getrennten Grid-Knoten nicht außer Betrieb nehmen, wenn ein oder mehrere erforderliche Knoten ebenfalls getrennt sind (z. B. ein Speicherknoten, der für das ADC-Quorum erforderlich ist).	a. Überprüfen Sie die Meldungen zur möglichen Außerbetriebnahme für alle getrennten Knoten. b. Bestimmen Sie, welche Knoten nicht außer Betrieb genommen werden können, weil sie benötigt werden. ◦ Wenn der Zustand eines erforderlichen Knotens „Administrativ ausgefallen“ lautet, bringen Sie den Knoten wieder online. ◦ Wenn der Zustand eines erforderlichen Knotens unbekannt ist, führen Sie ein Knotenwiederherstellungsverfahren durch, um den erforderlichen Knoten wiederherzustellen.

Außerbetriebnahme Möglicher Grund	Beschreibung	Schritte zur Lösung
Nein, Mitglied der HA-Gruppe(n): *Gruppenname*. Bevor Sie diesen Knoten außer Betrieb nehmen können, müssen Sie ihn aus allen HA-Gruppen entfernen.	Sie können einen Admin-Knoten oder Gateway-Knoten nicht außer Betrieb nehmen, wenn eine Knotenschnittstelle zu einer Hochverfügbarkeitsgruppe (HA) gehört.	Bearbeiten Sie die HA-Gruppe, um die Schnittstelle des Knotens zu entfernen, oder entfernen Sie die gesamte HA-Gruppe. Sehen "Konfigurieren von Hochverfügbarkeitsgruppen" .
Nein, Site *x* erfordert mindestens *n* Speicherknoten mit ADC-Diensten.	**Nur Speicherknoten.** Sie können einen Speicherknoten nicht außer Betrieb nehmen, wenn am Standort nicht genügend Knoten verbleiben, um die ADC-Quorumanforderungen zu erfüllen.	Führen Sie eine Erweiterung durch. Fügen Sie der Site einen neuen Speicherknoten hinzu und geben Sie an, dass dieser über einen ADC-Dienst verfügen soll. Informationen zu den"ADC-Quorum" .

Außerbetriebnahme Möglicher Grund	Beschreibung	Schritte zur Lösung
Nein, ein oder mehrere Erasure-Coding-Profile benötigen mindestens *n* Speicherknoten. Wenn das Profil nicht in einer ILM-Regel verwendet wird, können Sie es deaktivieren.	**Nur Speicherknoten.** Sie können einen Speicherknoten nicht außer Betrieb nehmen, es sei denn, es bleiben genügend Knoten für die vorhandenen Erasure-Coding-Profile übrig. Wenn beispielsweise ein Erasure-Coding-Profil für 4+2 Erasure Coding vorhanden ist, müssen mindestens 6 Storage Nodes verbleiben.	Führen Sie für jedes betroffene Erasure-Coding-Profil einen der folgenden Schritte aus, je nachdem, wie das Profil verwendet wird: • **Wird in aktiven ILM-Richtlinien verwendet**: Führen Sie eine Erweiterung durch. Fügen Sie genügend neue Speicherknoten hinzu, um die Erasure Coding-Funktion fortsetzen zu können. Siehe die Anweisungen für"Erweitern Sie Ihr Netz" . • **Wird in einer ILM-Regel verwendet, aber nicht in aktiven ILM-Richtlinien**: Bearbeiten oder löschen Sie die Regel und deaktivieren Sie dann das Erasure-Coding-Profil. • **Wird in keiner ILM-Regel verwendet**: Deaktivieren Sie das Erasure-Coding-Profil. **Hinweis:** Wenn Sie versuchen, ein Erasure-Coding-Profil zu deaktivieren und dem Profil noch Objektdaten zugeordnet sind, wird eine Fehlermeldung angezeigt. Möglicherweise müssen Sie mehrere Wochen warten, bevor Sie den Deaktivierungsvorgang erneut versuchen. Erfahren Sie mehr über"Deaktivieren eines Erasure-Coding-Profils" .
Nein, Sie können einen Archivknoten nicht außer Betrieb nehmen, es sei denn, die Verbindung zum Knoten wird getrennt.	Wenn ein Archivknoten noch verbunden ist, können Sie ihn nicht entfernen.	**Hinweis**: Die Unterstützung für Archivknoten wurde entfernt. Wenn Sie einen Archivknoten außer Betrieb nehmen müssen, lesen Sie "Außerbetriebnahme von Grid-Knoten (StorageGRID 11.8-Dokumentationsseite)"

Abgeschaltete Netzknoten außer Betrieb nehmen

Möglicherweise müssen Sie einen Knoten außer Betrieb nehmen, der derzeit nicht mit dem Netz verbunden ist (einen Knoten, dessen Zustand unbekannt oder administrativ ausgefallen ist).

Bevor Sie beginnen

- Sie verstehen die Überlegungen zur Stilllegung"Admin- und Gateway-Knoten" und die Überlegungen zur Stilllegung"Speicherknoten" .
- Sie haben alle erforderlichen Elemente erhalten.
- Sie haben sichergestellt, dass keine Datenreparaturaufträge aktiv sind. Sehen "Überprüfen Sie die Datenreparaturaufträge" .
- Sie haben bestätigt, dass die Wiederherstellung des Speicherknotens nirgendwo im Grid läuft. Wenn dies der Fall ist, müssen Sie warten, bis alle im Rahmen der Wiederherstellung durchgeführten Cassandra-Neuaufbauten abgeschlossen sind. Anschließend können Sie mit der Außerbetriebnahme fortfahren.
- Sie haben sichergestellt, dass während der Knoten-Außerbetriebnahme keine anderen Wartungsvorgänge ausgeführt werden, es sei denn, die Knoten-Außerbetriebnahme wird angehalten.
- Die Spalte **Außerbetriebnahme möglich** für den oder die getrennten Knoten, die Sie außer Betrieb nehmen möchten, enthält ein grünes Häkchen.
- Sie haben die Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Sie können getrennte Knoten identifizieren, indem Sie nach dem blauen Symbol „Unbekannt“ suchen. oder das graue Symbol „Administrativ deaktiviert“ in der Spalte **Gesundheit**.

Beachten Sie vor der Außerbetriebnahme eines getrennten Knotens Folgendes:

- Dieses Verfahren ist in erster Linie zum Entfernen eines einzelnen getrennten Knotens gedacht. Wenn Ihr Netz mehrere getrennte Knoten enthält, müssen Sie diese gemäß der Software alle gleichzeitig außer Betrieb nehmen, wodurch das Risiko unerwarteter Ergebnisse steigt.

  Wenn Sie mehrere getrennte Speicherknoten gleichzeitig außer Betrieb nehmen, kann es zu Datenverlust kommen. Sehen "Überlegungen zu getrennten Speicherknoten" .

  Seien Sie vorsichtig, wenn Sie Speicherknoten in einem Grid außer Betrieb nehmen, das softwarebasierte Knoten enthält, die nur Metadaten enthalten. Wenn Sie alle Knoten außer Betrieb nehmen, die zum Speichern von *sowohl* Objekten als auch Metadaten konfiguriert sind, wird die Möglichkeit zum Speichern von Objekten aus dem Raster entfernt. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

- Wenn ein getrennter Knoten nicht entfernt werden kann (z. B. ein Speicherknoten, der für das ADC-Quorum erforderlich ist), kann kein anderer getrennter Knoten entfernt werden.

Schritte

1. Sofern Sie keinen Archivknoten außer Betrieb nehmen (der getrennt werden muss), versuchen Sie, alle getrennten Grid-Knoten wieder online zu bringen oder wiederherzustellen.

   Sehen"Verfahren zur Wiederherstellung von Grid-Knoten" Anweisungen hierzu finden Sie unter.

2. Wenn Sie einen getrennten Grid-Knoten nicht wiederherstellen können und ihn außer Betrieb nehmen möchten, während er getrennt ist, aktivieren Sie das Kontrollkästchen für diesen Knoten.

   Wenn Ihr Netz mehrere getrennte Knoten enthält, müssen Sie diese gemäß der Software alle gleichzeitig außer Betrieb nehmen, wodurch das Risiko unerwarteter Ergebnisse steigt.

   Seien Sie vorsichtig, wenn Sie mehr als einen getrennten Grid-Knoten gleichzeitig außer Betrieb nehmen, insbesondere wenn Sie mehrere getrennte Speicherknoten auswählen. Wenn Sie über mehr als einen getrennten Speicherknoten verfügen, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu bestimmen.

3. Geben Sie die Bereitstellungspassphrase ein.

   Die Schaltfläche **Außerbetriebnahme starten** ist aktiviert.

4. Klicken Sie auf **Außerbetriebnahme starten**.

   Es wird eine Warnung angezeigt, die darauf hinweist, dass Sie einen getrennten Knoten ausgewählt haben und dass Objektdaten verloren gehen, wenn der Knoten die einzige Kopie eines Objekts enthält.

5. Überprüfen Sie die Liste der Knoten und klicken Sie auf **OK**.

   Der Außerbetriebnahmevorgang wird gestartet und der Fortschritt wird für jeden Knoten angezeigt. Während des Vorgangs wird ein neues Wiederherstellungspaket generiert, das die Änderung der Netzkonfiguration enthält.

6. Sobald das neue Wiederherstellungspaket verfügbar ist, klicken Sie auf den Link oder wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**, um auf die Seite „Wiederherstellungspaket“ zuzugreifen. Laden Sie dann die `.zip` Datei.

   Siehe die Anweisungen für"Herunterladen des Wiederherstellungspakets" .

   Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Netz wiederherstellen können, falls während der Außerbetriebnahme etwas schiefgeht.

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

7. Überwachen Sie regelmäßig die Seite „Außerbetriebnahme“, um sicherzustellen, dass alle ausgewählten Knoten erfolgreich außer Betrieb genommen werden.

   Die Außerbetriebnahme von Speicherknoten kann Tage oder Wochen dauern. Wenn alle Aufgaben abgeschlossen sind, wird die Knotenauswahlliste mit einer Erfolgsmeldung erneut angezeigt. Wenn Sie einen getrennten Speicherknoten außer Betrieb genommen haben, zeigt eine Informationsmeldung an, dass die Reparaturaufträge gestartet wurden.

8. Nachdem die Knoten im Rahmen des Außerbetriebnahmeverfahrens automatisch heruntergefahren wurden, entfernen Sie alle verbleibenden virtuellen Maschinen oder anderen Ressourcen, die mit dem außer Betrieb genommenen Knoten verknüpft sind.

Führen Sie diesen Schritt erst aus, wenn die Knoten automatisch heruntergefahren wurden.

9. Wenn Sie einen Speicherknoten außer Betrieb nehmen, überwachen Sie den Status der Reparaturaufträge für **replizierte Daten** und **löschcodierte (EC) Daten**, die während des Außerbetriebnahmeprozesses automatisch gestartet werden.

Replizierte Daten

- Um einen geschätzten Prozentsatz der Fertigstellung der replizierten Reparatur zu erhalten, addieren Sie die `show-replicated-repair-status` Option zum Befehl „repair-data“.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob die Reparaturen abgeschlossen sind:
  a. Wählen Sie **NODES** > ***Speicherknoten wird repariert*** > **ILM**.
  b. Überprüfen Sie die Attribute im Abschnitt „Bewertung“. Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut **Warten – Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
  a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
  b. Wählen Sie ***grid*** > ***Reparierter Speicherknoten*** > **LDR** > **Datenspeicher**.
  c. Verwenden Sie eine Kombination der folgenden Attribute, um so gut wie möglich zu bestimmen, ob replizierte Reparaturen abgeschlossen sind.

> ⓘ Möglicherweise liegen Cassandra-Inkonsistenzen vor und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

    - **Reparaturversuche (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt replizierter Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Speicherknoten versucht, ein Hochrisikoobjekt zu reparieren. Wenn dieses Attribut über einen Zeitraum, der länger ist als der aktuelle Scanzeitraum (bereitgestellt durch das Attribut **Scanzeitraum – Geschätzt**), nicht ansteigt, bedeutet dies, dass beim ILM-Scan auf keinem Knoten ein Hochrisikoobjekt gefunden wurde, das repariert werden muss.

> ⓘ Hochrisikoobjekte sind Objekte, bei denen die Gefahr eines vollständigen Verlusts besteht. Dies schließt keine Objekte ein, die ihrer ILM-Konfiguration nicht entsprechen.

    - **Scan-Zeitraum – Geschätzt (XSCM)**: Verwenden Sie dieses Attribut, um abzuschätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn das Attribut **Reparaturversuche** über einen Zeitraum, der länger als der aktuelle Scanzeitraum ist, nicht ansteigt, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt wurden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period – Estimated (XSCM)** gilt für das gesamte Raster und ist das Maximum aller Knoten-Scan-Perioden. Sie können den Attributverlauf **Scan-Zeitraum – Geschätzt** für das Raster abfragen, um einen geeigneten Zeitrahmen zu bestimmen.

Löschcodierte (EC) Daten

So überwachen Sie die Reparatur von Erasure-Code-Daten und wiederholen alle möglicherweise fehlgeschlagenen Anfragen:

1. Bestimmen Sie den Status der Datenreparaturen mit Erasure Code:
   - Wählen Sie **SUPPORT** > **Tools** > **Metriken**, um die geschätzte Zeit bis zur Fertigstellung und den Fertigstellungsgrad für den aktuellen Auftrag anzuzeigen. Wählen Sie dann im Abschnitt „Grafana“ die Option „EC-Übersicht“ aus. Sehen Sie sich die Dashboards **Geschätzte Zeit bis zur Fertigstellung des Grid EC-Jobs** und **Prozentsatz der Fertigstellung des Grid EC-Jobs**

an.

- Verwenden Sie diesen Befehl, um den Status eines bestimmten `repair-data` Betrieb:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

  ```
  repair-data show-ec-repair-status
  ```

Die Ausgabe listet Informationen auf, einschließlich `repair ID` , für alle bisherigen und laufenden Reparaturen.

2. Wenn die Ausgabe zeigt, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie die `--repair-id` Option zum erneuten Versuch der Reparatur.

   Mit diesem Befehl wird eine fehlgeschlagene Knotenreparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Mit diesem Befehl wird eine fehlgeschlagene Volumereparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Nach Abschluss

Sobald die getrennten Knoten außer Betrieb genommen wurden und alle Datenreparaturaufträge abgeschlossen sind, können Sie alle verbundenen Grid-Knoten nach Bedarf außer Betrieb nehmen.

Führen Sie anschließend die folgenden Schritte aus, nachdem Sie die Außerbetriebnahme abgeschlossen haben:

- Stellen Sie sicher, dass die Laufwerke des außer Betrieb genommenen Netzknotens gelöscht werden. Verwenden Sie ein im Handel erhältliches Tool oder einen Dienst zum Löschen von Daten, um Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn Sie einen Appliance-Knoten außer Betrieb genommen haben und die Daten auf der Appliance mithilfe einer Knotenverschlüsselung geschützt waren, verwenden Sie das StorageGRID Appliance Installer, um die Konfiguration des Schlüsselverwaltungsservers zu löschen (Clear KMS). Sie müssen die KMS-Konfiguration löschen, wenn Sie die Appliance zu einem anderen Grid hinzufügen möchten. Anweisungen hierzu finden Sie unter "Überwachen der Knotenverschlüsselung im Wartungsmodus" .

Angeschlossene Netzknoten außer Betrieb nehmen

Sie können Knoten, die mit dem Netz verbunden sind, außer Betrieb nehmen und dauerhaft entfernen.

Bevor Sie beginnen

- Sie verstehen die Überlegungen zur Stilllegung"Admin- und Gateway-Knoten" und die Überlegungen zur Stilllegung"Speicherknoten" .
- Sie haben alle erforderlichen Materialien gesammelt.

- Sie haben sichergestellt, dass keine Datenreparaturaufträge aktiv sind.
- Sie haben bestätigt, dass die Wiederherstellung des Speicherknotens nirgendwo im Grid läuft. Wenn dies der Fall ist, warten Sie, bis alle im Rahmen der Wiederherstellung durchgeführten Cassandra-Neuaufbauten abgeschlossen sind. Anschließend können Sie mit der Außerbetriebnahme fortfahren.
- Sie haben sichergestellt, dass während der Knoten-Außerbetriebnahme keine anderen Wartungsvorgänge ausgeführt werden, es sei denn, die Knoten-Außerbetriebnahme wird angehalten.
- Sie haben die Bereitstellungspassphrase.
- Gitterknoten sind verbunden.
- Die Spalte **Außerbetriebnahme möglich** für den oder die Knoten, die Sie außer Betrieb nehmen möchten, enthält ein grünes Häkchen.

> Die Außerbetriebnahme wird nicht gestartet, wenn ein oder mehrere Volumes offline (nicht gemountet) sind oder wenn sie online (gemountet) sind, sich aber in einem Fehlerzustand befinden.

> Wenn während einer Außerbetriebnahme ein oder mehrere Volumes offline gehen, wird der Außerbetriebnahmevorgang abgeschlossen, nachdem diese Volumes wieder online sind.

- Alle Gitterknoten haben einen normalen (grünen) Gesundheitszustand . Wenn Sie eines dieser Symbole in der Spalte **Health** sehen, müssen Sie versuchen, das Problem zu beheben:

Symbol	Farbe	Schwere
	Gelb	Beachten
	Hellorange	Unerheblich
	Dunkelorange	Wesentlich
	Rot	Kritisch

- Wenn Sie zuvor einen getrennten Speicherknoten außer Betrieb genommen haben, wurden alle Datenreparaturaufträge erfolgreich abgeschlossen. Sehen "Überprüfen Sie die Datenreparaturaufträge" .

> Entfernen Sie die virtuelle Maschine oder andere Ressourcen eines Grid-Knotens erst, wenn Sie in diesem Verfahren dazu aufgefordert werden.

> Seien Sie vorsichtig, wenn Sie Speicherknoten in einem Grid außer Betrieb nehmen, das softwarebasierte Knoten enthält, die nur Metadaten enthalten. Wenn Sie alle Knoten außer Betrieb nehmen, die zum Speichern von *sowohl* Objekten als auch Metadaten konfiguriert sind, wird die Möglichkeit zum Speichern von Objekten aus dem Raster entfernt. Sehen"Arten von Speicherknoten" Weitere Informationen zu reinen Metadaten-Speicherknoten.

Informationen zu diesem Vorgang

Wenn ein Knoten außer Betrieb genommen wird, werden seine Dienste deaktiviert und der Knoten

automatisch heruntergefahren.

Schritte

1. Aktivieren Sie auf der Seite „Knoten außer Betrieb nehmen“ das Kontrollkästchen für jeden Grid-Knoten, den Sie außer Betrieb nehmen möchten.
2. Geben Sie die Bereitstellungspassphrase ein.

   Die Schaltfläche **Außerbetriebnahme starten** ist aktiviert.
3. Wählen Sie **Außerbetriebnahme starten**.
4. Überprüfen Sie die Liste der Knoten im Bestätigungsdialogfeld und wählen Sie **OK**.

   Der Vorgang zur Außerbetriebnahme des Knotens wird gestartet und der Fortschritt wird für jeden Knoten angezeigt.

   > Nehmen Sie einen Speicherknoten nicht offline, nachdem der Außerbetriebnahmevorgang begonnen hat. Das Ändern des Status kann dazu führen, dass einige Inhalte nicht an andere Speicherorte kopiert werden.
5. Sobald das neue Wiederherstellungspaket verfügbar ist, wählen Sie den Link „Wiederherstellungspaket“ im Banner oder wählen Sie „WARTUNG“ > „System“ > „Wiederherstellungspaket“*, um auf die Seite „Wiederherstellungspaket“ zuzugreifen. Laden Sie dann die `.zip` Datei.

   Sehen "Herunterladen des Wiederherstellungspakets" .

   > Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Netz wiederherstellen können, falls während der Außerbetriebnahme etwas schiefgeht.
6. Überwachen Sie regelmäßig die Seite „Knoten außer Betrieb nehmen“, um sicherzustellen, dass alle ausgewählten Knoten erfolgreich außer Betrieb genommen werden.

   > Die Außerbetriebnahme von Speicherknoten kann Tage oder Wochen dauern.

   Wenn alle Aufgaben abgeschlossen sind, wird die Knotenauswahlliste mit einer Erfolgsmeldung erneut angezeigt.

Nach Abschluss

Führen Sie diese Schritte aus, nachdem Sie die Außerbetriebnahme des Knotens abgeschlossen haben:

1. Befolgen Sie die entsprechenden Schritte für Ihre Plattform. Beispiel:
   - **Linux**: Möglicherweise möchten Sie die Volumes trennen und die Knotenkonfigurationsdateien löschen, die Sie während der Installation erstellt haben. Sehen"Installieren Sie StorageGRID unter Red Hat Enterprise Linux" Und"Installieren Sie StorageGRID unter Ubuntu oder Debian" .
   - **VMware**: Sie können die virtuelle Maschine mit der vCenter-Option „Von Festplatte löschen“ löschen. Möglicherweise müssen Sie auch alle Datenträger löschen, die von der virtuellen Maschine unabhängig sind.
   - * StorageGRID -Gerät*: Der Geräteknoten wird automatisch in einen nicht bereitgestellten Zustand zurückgesetzt, in dem Sie auf das StorageGRID -Geräteinstallationsprogramm zugreifen können. Sie können das Gerät ausschalten oder zu einem anderen StorageGRID -System hinzufügen.

2. Stellen Sie sicher, dass die Laufwerke des außer Betrieb genommenen Netzknotens gelöscht werden. Verwenden Sie ein im Handel erhältliches Tool oder einen Dienst zum Löschen von Daten, um Daten dauerhaft und sicher von den Laufwerken zu entfernen.
3. Wenn Sie einen Appliance-Knoten außer Betrieb genommen haben und die Daten auf der Appliance mithilfe einer Knotenverschlüsselung geschützt waren, verwenden Sie das StorageGRID Appliance Installer, um die Konfiguration des Schlüsselverwaltungsservers zu löschen (Clear KMS). Sie müssen die KMS-Konfiguration löschen, wenn Sie die Appliance zu einem anderen Grid hinzufügen möchten. Anweisungen hierzu finden Sie unter "Überwachen der Knotenverschlüsselung im Wartungsmodus" .

Außerbetriebnahmeprozess für Speicherknoten anhalten und fortsetzen

Wenn Sie einen zweiten Wartungsvorgang durchführen müssen, können Sie den Außerbetriebnahmevorgang für einen Speicherknoten während bestimmter Phasen anhalten. Nachdem die anderen Schritte abgeschlossen sind, können Sie mit der Außerbetriebnahme fortfahren.

> ⓘ Die Schaltfläche **Pause** ist nur aktiviert, wenn die Phasen der ILM-Auswertung oder der Außerbetriebnahme von Erasure-Coded-Daten erreicht sind. Die ILM-Auswertung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Außerbetriebnahme**.

   Die Seite „Außerbetriebnahme“ wird angezeigt.

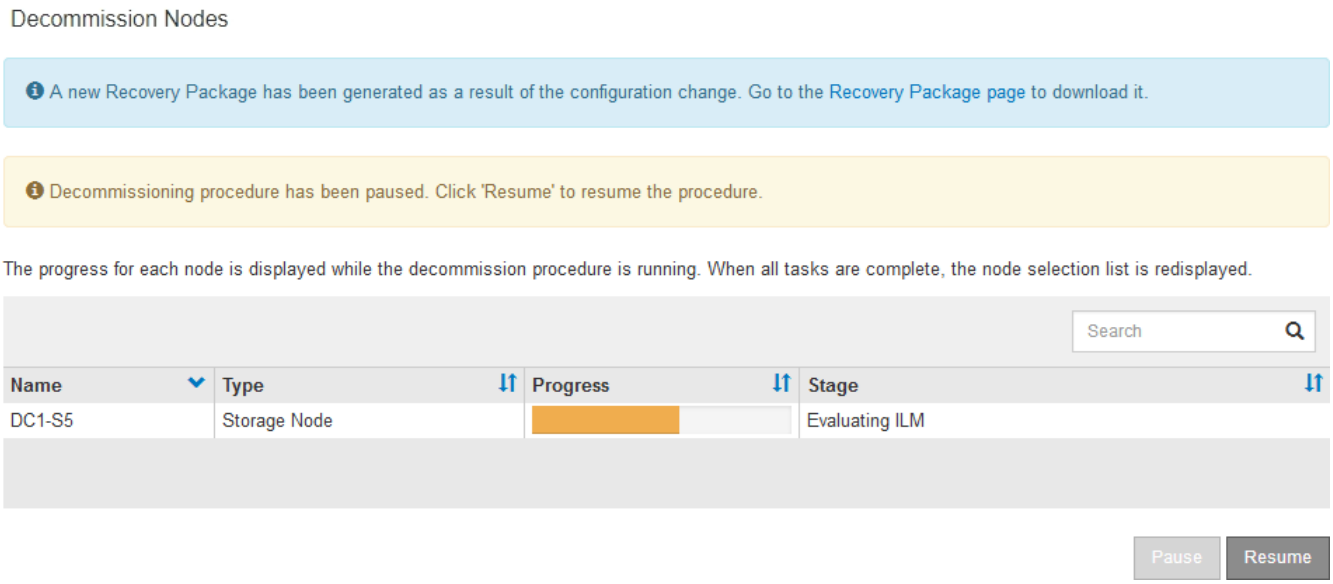
2. Wählen Sie **Knoten außer Betrieb nehmen**.

   Die Seite „Knoten außer Betrieb nehmen“ wird angezeigt. Wenn der Außerbetriebnahmevorgang eine der folgenden Phasen erreicht, wird die Schaltfläche **Pause** aktiviert.

   - Evaluierung von ILM
   - Außerbetriebnahme von Erasure-Coded-Daten

3. Wählen Sie **Pause**, um den Vorgang anzuhalten.

   Die aktuelle Phase wird angehalten und die Schaltfläche **Fortsetzen** wird aktiviert.



4. Nachdem die anderen Wartungsvorgänge abgeschlossen sind, wählen Sie **Fortsetzen**, um mit der Außerbetriebnahme fortzufahren.

Stilllegungsstandort

Überlegungen zum Entfernen einer Site

Bevor Sie das Verfahren zur Außerbetriebnahme einer Site zum Entfernen einer Site verwenden, müssen Sie die Überlegungen überprüfen.

Was passiert, wenn Sie eine Site außer Betrieb nehmen?

Wenn Sie eine Site außer Betrieb nehmen, entfernt StorageGRID dauerhaft alle Knoten an der Site und die Site selbst aus dem StorageGRID -System.

Wenn das Verfahren zur Außerbetriebnahme des Standorts abgeschlossen ist:

- Sie können StorageGRID nicht mehr verwenden, um die Site oder einen der Knoten auf der Site anzuzeigen oder darauf zuzugreifen.
- Sie können keine Speicherpools oder Erasure-Coding-Profile mehr verwenden, die auf die Site verwiesen. Wenn StorageGRID eine Site außer Betrieb nimmt, entfernt es automatisch diese Speicherpools und deaktiviert diese Erasure-Coding-Profile.

Unterschiede zwischen den Stilllegungsverfahren für verbundene und getrennte Standorte

Sie können das Verfahren zur Site-Außerbetriebnahme verwenden, um eine Site zu entfernen, bei der alle Knoten mit StorageGRID verbunden sind (als Außerbetriebnahme einer verbundenen Site bezeichnet), oder um eine Site zu entfernen, bei der alle Knoten von StorageGRID getrennt sind (als Außerbetriebnahme einer getrennten Site bezeichnet). Bevor Sie beginnen, müssen Sie die Unterschiede zwischen diesen Verfahren verstehen.

Wenn eine Site eine Mischung aus verbundenen ( ) und getrennte Knoten (oder), müssen Sie alle Offline-Knoten wieder online bringen.

- Durch die Außerbetriebnahme einer verbundenen Site können Sie eine Betriebssite aus dem StorageGRID

-System entfernen. Sie können beispielsweise eine verbundene Site-Außerbetriebnahme durchführen, um eine Site zu entfernen, die zwar funktioniert, aber nicht mehr benötigt wird.

- Wenn StorageGRID eine verbundene Site entfernt, verwendet es ILM, um die Objektdaten an der Site zu verwalten. Bevor Sie mit der Außerbetriebnahme einer verbundenen Site beginnen können, müssen Sie die Site aus allen ILM-Regeln entfernen und eine neue ILM-Richtlinie aktivieren. Die ILM-Prozesse zum Migrieren von Objektdaten und die internen Prozesse zum Entfernen einer Site können gleichzeitig ablaufen. Die beste Vorgehensweise besteht jedoch darin, die ILM-Schritte abzuschließen, bevor Sie mit dem eigentlichen Außerbetriebnahmeverfahren beginnen.
- Durch die Außerbetriebnahme einer getrennten Site können Sie eine ausgefallene Site aus dem StorageGRID -System entfernen. Sie können beispielsweise eine getrennte Site-Stilllegung durchführen, um eine Site zu entfernen, die durch einen Brand oder eine Überschwemmung zerstört wurde.

  Wenn StorageGRID eine getrennte Site entfernt, betrachtet es alle Knoten als nicht wiederherstellbar und unternimmt keinen Versuch, die Daten zu erhalten. Bevor Sie jedoch mit der Außerbetriebnahme einer getrennten Site beginnen können, müssen Sie die Site aus allen ILM-Regeln entfernen und eine neue ILM-Richtlinie aktivieren.

> Bevor Sie ein Verfahren zur Außerbetriebnahme eines getrennten Standorts durchführen, müssen Sie sich an Ihren NetApp Kundenbetreuer wenden. NetApp überprüft Ihre Anforderungen, bevor alle Schritte im Assistenten „Site außer Betrieb nehmen“ aktiviert werden. Sie sollten nicht versuchen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie glauben, dass es möglich sein könnte, die Site wiederherzustellen oder Objektdaten von der Site wiederherzustellen.

Allgemeine Voraussetzungen für das Entfernen einer verbundenen oder getrennten Site

Bevor Sie eine verbundene oder getrennte Site entfernen, müssen Sie sich der folgenden Anforderungen bewusst sein:

- Sie können eine Site, die den primären Admin-Knoten enthält, nicht außer Betrieb nehmen.
- Sie können eine Site nicht außer Betrieb nehmen, wenn einer der Knoten über eine Schnittstelle verfügt, die zu einer Hochverfügbarkeitsgruppe (HA) gehört. Sie müssen entweder die HA-Gruppe bearbeiten, um die Schnittstelle des Knotens zu entfernen, oder die gesamte HA-Gruppe entfernen.
- Sie können eine Site nicht außer Betrieb nehmen, wenn sie eine Mischung aus verbundenen ( ) und getrennt (oder) Knoten.
- Sie können eine Site nicht außer Betrieb nehmen, wenn ein Knoten an einer anderen Site getrennt ist (oder).
- Sie können das Verfahren zur Außerbetriebnahme der Site nicht starten, wenn ein EC-Knoten-Reparaturvorgang ausgeführt wird. Sehen"Überprüfen Sie die Datenreparaturaufträge" um die Reparatur von löschcodierten Daten zu verfolgen.
- Während das Verfahren zur Außerbetriebnahme des Standorts läuft:
  - Sie können keine ILM-Regeln erstellen, die sich auf die Außerbetriebnahme der Site beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf die Site zu verweisen.
  - Sie können keine anderen Wartungsvorgänge wie Erweiterungen oder Upgrades durchführen.

Wenn Sie während der Außerbetriebnahme einer verbundenen Site eine weitere Wartungsprozedur durchführen müssen, können Sie"Unterbrechen Sie den Vorgang, während die Speicherknoten entfernt werden" . Die Schaltfläche **Pause** ist nur aktiviert, wenn die Phasen der ILM-Auswertung oder der Außerbetriebnahme von Erasure-Coded-Daten erreicht sind. Die ILM-Auswertung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt. Nachdem die zweite Wartungsprozedur abgeschlossen ist, können Sie mit der Außerbetriebnahme fortfahren.

    - Wenn Sie nach dem Start des Site-Außerbetriebnahmeverfahrens einen Knoten wiederherstellen müssen, müssen Sie sich an den Support wenden.
- Sie können nicht mehr als eine Site gleichzeitig außer Betrieb nehmen.
- Wenn die Site einen oder mehrere Admin-Knoten enthält und Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, müssen Sie alle Vertrauensstellungen der vertrauenden Seite für die Site aus Active Directory Federation Services (AD FS) entfernen.

Anforderungen an das Information Lifecycle Management (ILM)

Beim Entfernen einer Site müssen Sie Ihre ILM-Konfiguration aktualisieren. Der Assistent „Site außer Betrieb nehmen“ führt Sie durch eine Reihe von erforderlichen Schritten, um Folgendes sicherzustellen:

- Auf die Site wird in keiner ILM-Richtlinie verwiesen. Wenn dies der Fall ist, müssen Sie die Richtlinien bearbeiten oder Richtlinien mit neuen ILM-Regeln erstellen und aktivieren.
- Es beziehen sich keine ILM-Regeln auf die Site, auch wenn diese Regeln in keiner Richtlinie verwendet werden. Sie müssen alle Regeln löschen oder bearbeiten, die sich auf die Site beziehen.

Wenn StorageGRID die Site außer Betrieb nimmt, werden automatisch alle nicht verwendeten Erasure-Coding-Profile deaktiviert, die sich auf die Site beziehen, und alle nicht verwendeten Speicherpools gelöscht, die sich auf die Site beziehen. Wenn der Speicherpool „Alle Speicherknoten“ vorhanden ist (StorageGRID 11.6 und früher), wird er entfernt, da er alle Sites verwendet.

Bevor Sie eine Site entfernen können, müssen Sie möglicherweise neue ILM-Regeln erstellen und eine neue ILM-Richtlinie aktivieren. Diese Anweisungen setzen voraus, dass Sie die Funktionsweise von ILM gut verstehen und mit der Erstellung von Speicherpools, Erasure-Coding-Profilen, ILM-Regeln sowie der Simulation und Aktivierung einer ILM-Richtlinie vertraut sind. Sehen "Objekte mit ILM verwalten" .

Überlegungen zu den Objektdaten an einem verbundenen Standort

Wenn Sie eine verbundene Site außer Betrieb nehmen, müssen Sie entscheiden, was mit den vorhandenen Objektdaten auf der Site geschehen soll, wenn Sie neue ILM-Regeln und eine neue ILM-Richtlinie erstellen. Sie können eine oder beide der folgenden Aktionen ausführen:

- Verschieben Sie Objektdaten von der ausgewählten Site zu einer oder mehreren anderen Sites in Ihrem Raster.

  Beispiel für das Verschieben von Daten: Angenommen, Sie möchten einen Standort in Raleigh außer Betrieb nehmen, weil Sie einen neuen Standort in Sunnyvale hinzugefügt haben. In diesem Beispiel möchten Sie alle Objektdaten von der alten Site auf die neue Site verschieben. Bevor Sie Ihre ILM-Regeln und ILM-Richtlinien aktualisieren, müssen Sie die Kapazität an beiden Standorten überprüfen. Sie müssen sicherstellen, dass der Standort Sunnyvale über genügend Kapazität verfügt, um die Objektdaten vom Standort Raleigh aufzunehmen, und dass in Sunnyvale ausreichend Kapazität für zukünftiges Wachstum verbleibt.

Um sicherzustellen, dass ausreichend Kapazität zur Verfügung steht, müssen Sie möglicherweise"ein Raster erweitern" indem Sie Speichervolumes oder Speicherknoten zu einer vorhandenen Site hinzufügen oder eine neue Site hinzufügen, bevor Sie dieses Verfahren ausführen.

- Löschen Sie Objektkopien von der ausgewählten Site.

  Beispiel zum Löschen von Daten: Angenommen, Sie verwenden derzeit eine 3-Kopien-ILM-Regel, um Objektdaten über drei Standorte hinweg zu replizieren. Bevor Sie einen Standort außer Betrieb nehmen, können Sie eine entsprechende ILM-Regel mit zwei Kopien erstellen, um Daten nur an zwei Standorten zu speichern. Wenn Sie eine neue ILM-Richtlinie aktivieren, die die 2-Kopien-Regel verwendet, löscht StorageGRID die Kopien vom dritten Standort, da sie die ILM-Anforderungen nicht mehr erfüllen. Die Objektdaten bleiben jedoch weiterhin geschützt und die Kapazität der beiden verbleibenden Standorte bleibt unverändert.

  Erstellen Sie niemals eine ILM-Regel für eine einzelne Kopie, um die Entfernung einer Site zu ermöglichen. Eine ILM-Regel, die für einen bestimmten Zeitraum nur eine replizierte Kopie erstellt, birgt das Risiko eines dauerhaften Datenverlusts. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

Zusätzliche Anforderungen für die Stilllegung eines verbundenen Standorts

Bevor StorageGRID eine verbundene Site entfernen kann, müssen Sie Folgendes sicherstellen:

- Alle Knoten in Ihrem StorageGRID -System müssen den Verbindungsstatus **Verbunden** haben ( ); die Knoten können jedoch aktive Warnungen haben.

  Sie können die Schritte 1 bis 4 des Assistenten „Site außer Betrieb nehmen“ abschließen, wenn ein oder mehrere Knoten getrennt sind. Sie können Schritt 5 des Assistenten, der den Außerbetriebnahmeprozess startet, jedoch erst abschließen, wenn alle Knoten verbunden sind.

- Wenn die Site, die Sie entfernen möchten, einen Gateway-Knoten oder einen Admin-Knoten enthält, der für den Lastenausgleich verwendet wird, müssen Sie möglicherweise"ein Raster erweitern" um einen gleichwertigen neuen Knoten an einem anderen Standort hinzuzufügen. Stellen Sie sicher, dass Clients eine Verbindung zum Ersatzknoten herstellen können, bevor Sie mit der Außerbetriebnahme der Site beginnen.
- Wenn die Site, die Sie entfernen möchten, Gateway-Knoten oder Admin-Knoten enthält, die sich in einer Hochverfügbarkeitsgruppe (HA) befinden, können Sie die Schritte 1 bis 4 des Assistenten „Site außer Betrieb nehmen“ ausführen. Sie können Schritt 5 des Assistenten, der den Außerbetriebnahmeprozess startet, jedoch erst abschließen, wenn Sie diese Knoten aus allen HA-Gruppen entfernt haben. Wenn vorhandene Clients eine Verbindung zu einer HA-Gruppe herstellen, die Knoten von der Site enthält, müssen Sie sicherstellen, dass sie nach dem Entfernen der Site weiterhin eine Verbindung zu StorageGRID herstellen können.
- Wenn Clients eine direkte Verbindung zu Speicherknoten an dem Standort herstellen, den Sie entfernen möchten, müssen Sie sicherstellen, dass sie eine Verbindung zu Speicherknoten an anderen Standorten herstellen können, bevor Sie mit der Außerbetriebnahme des Standorts beginnen.
- Sie müssen auf den verbleibenden Sites ausreichend Speicherplatz bereitstellen, um alle Objektdaten unterzubringen, die aufgrund von Änderungen an einer aktiven ILM-Richtlinie verschoben werden. In

manchen Fällen müssen Sie möglicherweise"ein Raster erweitern" durch Hinzufügen von Speicherknoten, Speichervolumes oder neuen Sites, bevor Sie die Außerbetriebnahme einer verbundenen Site abschließen können.

- Sie müssen ausreichend Zeit einplanen, damit der Außerbetriebnahmevorgang abgeschlossen werden kann. Es kann Tage, Wochen oder sogar Monate dauern, bis StorageGRID ILM-Prozesse Objektdaten von der Site verschieben oder löschen, bevor die Site außer Betrieb genommen werden kann.

> Das Verschieben oder Löschen von Objektdaten von einer Site kann Tage, Wochen oder sogar Monate dauern, abhängig von der Datenmenge an der Site, der Auslastung Ihres Systems, den Netzwerklatenzen und der Art der erforderlichen ILM-Änderungen.

- Wenn möglich, sollten Sie die Schritte 1–4 des Assistenten „Site außer Betrieb nehmen“ so früh wie möglich abschließen. Der Außerbetriebnahmevorgang wird schneller und mit weniger Unterbrechungen und Leistungseinbußen abgeschlossen, wenn Sie das Verschieben von Daten von der Site zulassen, bevor Sie mit dem eigentlichen Außerbetriebnahmevorgang beginnen (indem Sie in Schritt 5 des Assistenten „Außerbetriebnahme starten“ auswählen).

Zusätzliche Anforderungen für die Stilllegung eines abgekoppelten Standorts

Bevor StorageGRID eine getrennte Site entfernen kann, müssen Sie Folgendes sicherstellen:

- Sie haben Ihren NetApp Kundenbetreuer kontaktiert. NetApp überprüft Ihre Anforderungen, bevor alle Schritte im Assistenten „Site außer Betrieb nehmen“ aktiviert werden.

> Sie sollten nicht versuchen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie glauben, dass es möglich sein könnte, die Site wiederherzustellen oder Objektdaten von der Site wiederherzustellen. Sehen "So stellt der technische Support eine Site wieder her" .

- Alle Knoten am Standort müssen einen der folgenden Verbindungsstatus aufweisen:
  - **Unbekannt** ( ): Aus einem unbekannten Grund wird ein Knoten getrennt oder die Dienste auf dem Knoten sind unerwartet ausgefallen. Beispielsweise könnte ein Dienst auf dem Knoten gestoppt worden sein oder der Knoten könnte aufgrund eines Stromausfalls oder einer unerwarteten Störung seine Netzwerkverbindung verloren haben.
  - **Administrativ nicht erreichbar** ( ): Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurden der Knoten oder die Dienste auf dem Knoten ordnungsgemäß heruntergefahren.
- Alle Knoten an allen anderen Standorten müssen den Verbindungsstatus **Verbunden** haben ( ); diese anderen Knoten können jedoch aktive Warnungen haben.
- Sie müssen verstehen, dass Sie StorageGRID nicht mehr verwenden können, um auf der Site gespeicherte Objektdaten anzuzeigen oder abzurufen. Wenn StorageGRID dieses Verfahren durchführt, unternimmt es keinen Versuch, Daten vom getrennten Standort zu erhalten.

> Wenn Ihre ILM-Regeln und -Richtlinien zum Schutz vor dem Verlust einer einzelnen Site konzipiert wurden, sind auf den verbleibenden Sites weiterhin Kopien Ihrer Objekte vorhanden.

- Sie müssen sich darüber im Klaren sein, dass das Objekt verloren geht und nicht wiederhergestellt werden kann, wenn die Site die einzige Kopie eines Objekts enthält.

Überlegungen zur Konsistenz beim Entfernen einer Site

Die Konsistenz für einen S3-Bucket bestimmt, ob StorageGRID Objektmetadaten vollständig auf alle Knoten und Sites repliziert, bevor einem Client mitgeteilt wird, dass die Objektaufnahme erfolgreich war. Konsistenz sorgt für ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Standorte hinweg.

Wenn StorageGRID eine Site entfernt, muss sichergestellt werden, dass keine Daten auf die zu entfernende Site geschrieben werden. Dadurch wird die Konsistenz für jeden Bucket oder Container vorübergehend außer Kraft gesetzt. Nachdem Sie den Site-Außerbetriebnahmeprozess gestartet haben, verwendet StorageGRID vorübergehend eine starke Site-Konsistenz, um zu verhindern, dass Objektmetadaten auf die zu entfernende Site geschrieben werden.

Beachten Sie, dass aufgrund dieser vorübergehenden Außerkraftsetzung alle Schreib-, Aktualisierungs- und Löschvorgänge des Clients, die während der Außerbetriebnahme eines Standorts erfolgen, fehlschlagen können, wenn mehrere Knoten an den verbleibenden Standorten nicht mehr verfügbar sind.

Benötigte Materialien zusammenstellen

Bevor Sie eine Site außer Betrieb nehmen, müssen Sie die folgenden Materialien beschaffen.

Artikel	Hinweise
Wiederherstellungspaket `.zip` Datei	Sie müssen das neueste Wiederherstellungspaket herunterladen `.zip` Datei(`sgws-recovery-package-id-revision.zip`). Mit der Wiederherstellungspaketdatei können Sie das System im Falle eines Fehlers wiederherstellen. "Laden Sie das Wiederherstellungspaket herunter"
`Passwords.txt`Datei	Diese Datei enthält die für den Zugriff auf Grid-Knoten über die Befehlszeile erforderlichen Passwörter und ist im Wiederherstellungspaket enthalten.
Bereitstellungspassphrase	Die Passphrase wird bei der Erstinstallation des StorageGRID -Systems erstellt und dokumentiert. Die Bereitstellungspassphrase ist nicht in der `Passwords.txt` Datei.
Beschreibung der Topologie des StorageGRID -Systems vor der Außerbetriebnahme	Besorgen Sie sich, sofern verfügbar, alle Unterlagen, die die aktuelle Topologie des Systems beschreiben.

Ähnliche Informationen

"Anforderungen an den Webbrowser"

Schritt 1: Site auswählen

Um festzustellen, ob eine Site stillgelegt werden kann, rufen Sie zunächst den Assistenten „Site stilllegen“ auf.

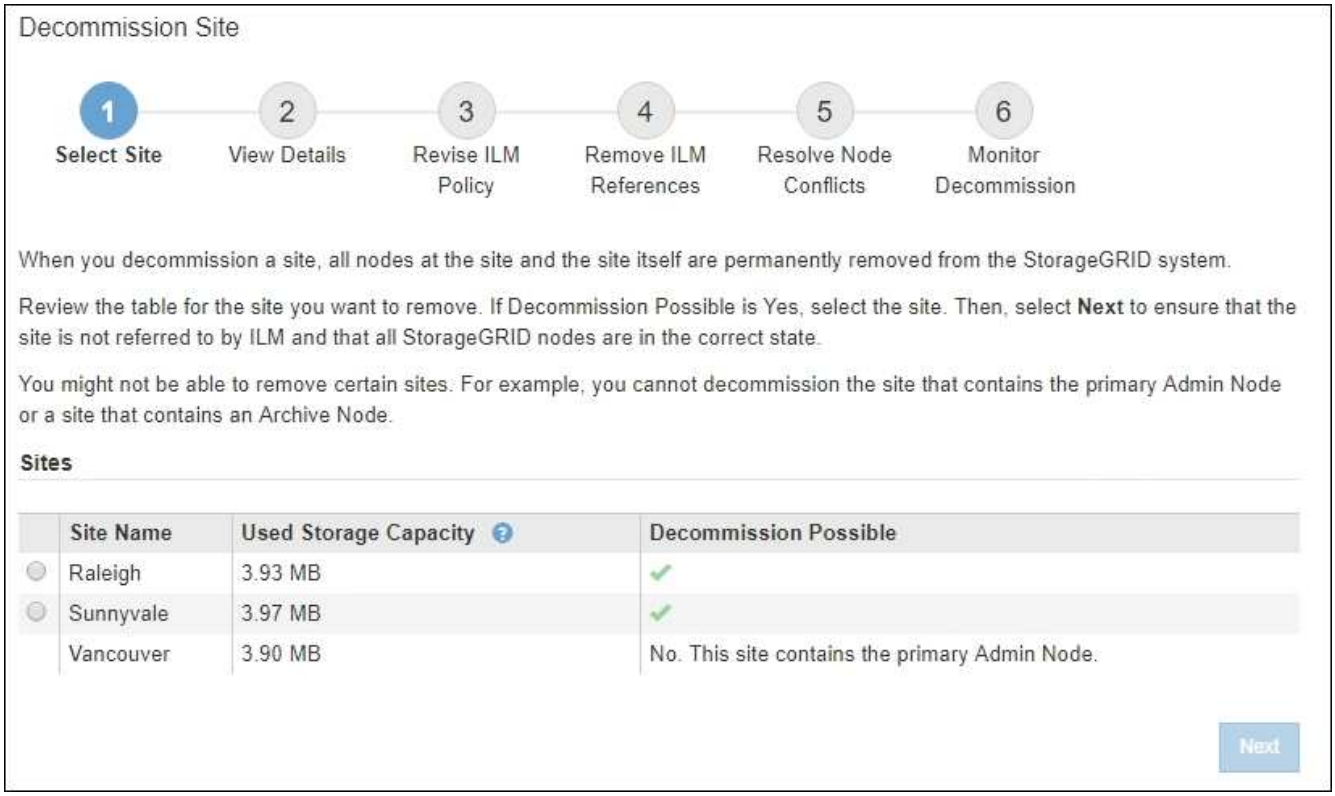
Bevor Sie beginnen

- Sie haben alle erforderlichen Materialien besorgt.
- Sie haben die Überlegungen zum Entfernen einer Site überprüft.
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung oder die Wartungs- und ILM-Berechtigungen" .

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Außerbetriebnahme**.
2. Wählen Sie **Site außer Betrieb nehmen**.

   Schritt 1 (Standort auswählen) des Assistenten „Standort außer Betrieb nehmen“ wird angezeigt. Dieser Schritt umfasst eine alphabetische Liste der Sites in Ihrem StorageGRID -System.



3. Sehen Sie sich die Werte in der Spalte **Verwendete Speicherkapazität** an, um zu ermitteln, wie viel Speicher derzeit an jedem Standort für Objektdaten verwendet wird.

   Die genutzte Speicherkapazität ist eine Schätzung. Wenn Knoten offline sind, ist die verwendete Speicherkapazität der letzte bekannte Wert für die Site.

   - Bei der Außerbetriebnahme einer verbundenen Site gibt dieser Wert an, wie viele Objektdaten an andere Sites verschoben oder von ILM gelöscht werden müssen, bevor Sie diese Site sicher außer Betrieb nehmen können.
   - Bei der Außerbetriebnahme einer getrennten Site gibt dieser Wert an, wie viel des Datenspeichers Ihres Systems nicht mehr zugänglich ist, wenn Sie diese Site außer Betrieb nehmen.

   > Wenn Ihre ILM-Richtlinie zum Schutz vor dem Verlust einer einzelnen Site konzipiert wurde, sollten auf den verbleibenden Sites weiterhin Kopien Ihrer Objektdaten vorhanden sein.

4. Überprüfen Sie die Gründe in der Spalte **Stilllegung möglich**, um festzustellen, welche Sites derzeit stillgelegt werden können.

   Wenn es mehr als einen Grund gibt, warum eine Site nicht stillgelegt werden kann, wird der schwerwiegendste Grund angezeigt.

Außerbetriebnahme Möglicher Grund	Beschreibung	Nächster Schritt
Grünes Häkchen ( )	Sie können diese Site außer Betrieb nehmen.	Gehe zuder nächste Schritt .
Nein. Diese Site enthält den primären Admin-Knoten.	Sie können eine Site, die den primären Admin-Knoten enthält, nicht außer Betrieb nehmen.	Keiner. Sie können diesen Vorgang nicht durchführen.
Nein. Diese Site enthält einen oder mehrere Archivknoten.	Sie können eine Site, die einen Archivknoten enthält, nicht außer Betrieb nehmen.	Keiner. Sie können diesen Vorgang nicht durchführen.
Nein. Alle Knoten an dieser Site sind getrennt. Wenden Sie sich an Ihren NetApp -Kundenbetreuer.	Sie können eine verbundene Site erst dann außer Betrieb setzen, wenn alle Knoten der Site verbunden sind ( ).	Wenn Sie eine getrennte Site-Außerbetriebnahme durchführen möchten, müssen Sie sich an Ihren NetApp Kundenbetreuer wenden, der Ihre Anforderungen überprüft und den Rest des Assistenten zur Site-Außerbetriebnahme aktiviert. **WICHTIG**: Nehmen Sie Online-Knoten niemals offline, um eine Site zu entfernen. Sie verlieren Daten.

   Das Beispiel zeigt ein StorageGRID -System mit drei Standorten. Das grüne Häkchen ( ) für die Standorte Raleigh und Sunnyvale gibt an, dass Sie diese Standorte außer Betrieb nehmen können. Sie können den Standort Vancouver jedoch nicht außer Betrieb nehmen, da er den primären Admin-Knoten enthält.

1. Wenn eine Außerbetriebnahme möglich ist, wählen Sie das Optionsfeld für die Site aus.

   Die Schaltfläche **Weiter** ist aktiviert.

2. Wählen Sie **Weiter**.

   Schritt 2 (Details anzeigen) wird angezeigt.

Schritt 2: Details anzeigen

In Schritt 2 (Details anzeigen) des Assistenten „Site außer Betrieb nehmen“ können Sie

überprüfen, welche Knoten in der Site enthalten sind, sehen, wie viel Speicherplatz auf jedem Speicherknoten verwendet wurde, und beurteilen, wie viel freier Speicherplatz an den anderen Sites in Ihrem Grid verfügbar ist.

Bevor Sie beginnen

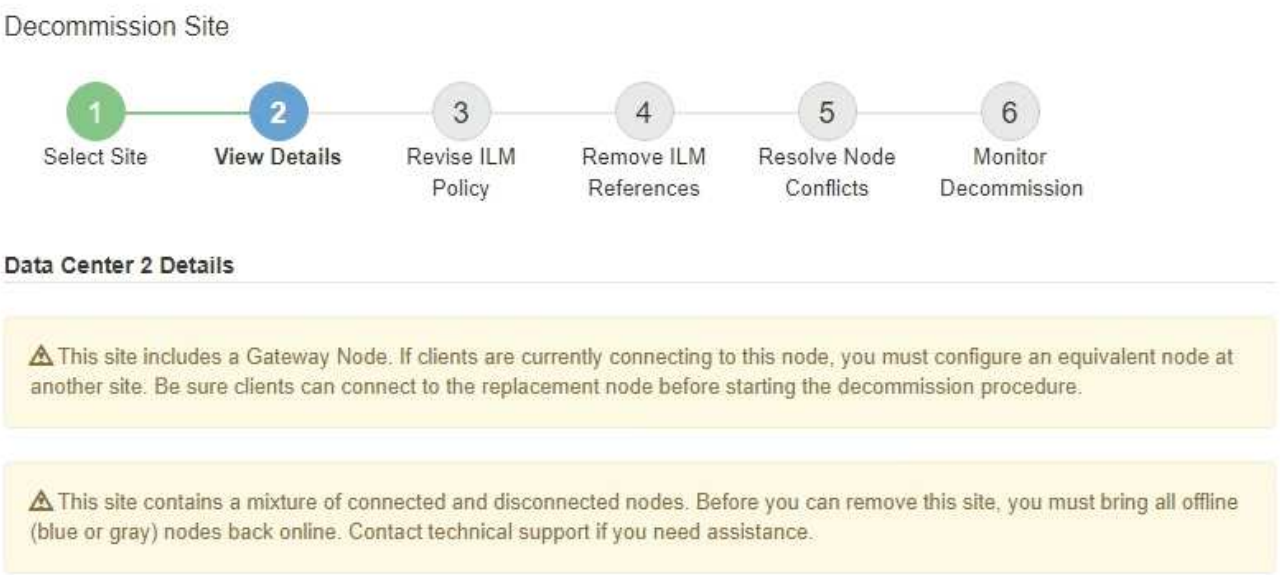
Bevor Sie eine Site außer Betrieb nehmen, müssen Sie überprüfen, wie viele Objektdaten an der Site vorhanden sind.

- Wenn Sie die Außerbetriebnahme einer verbundenen Site durchführen, müssen Sie wissen, wie viele Objektdaten derzeit an der Site vorhanden sind, bevor Sie ILM aktualisieren. Basierend auf den Standortkapazitäten und Ihren Datenschutzanforderungen können Sie neue ILM-Regeln erstellen, um Daten an andere Standorte zu verschieben oder Objektdaten vom Standort zu löschen.
- Führen Sie nach Möglichkeit alle erforderlichen Speicherknotenerweiterungen durch, bevor Sie mit der Außerbetriebnahme beginnen.
- Wenn Sie eine getrennte Site außer Betrieb nehmen, müssen Sie sich darüber im Klaren sein, wie viele Objektdaten durch die Entfernung der Site dauerhaft unzugänglich werden.

> Wenn Sie eine getrennte Site außer Betrieb nehmen, kann ILM keine Objektdaten verschieben oder löschen. Alle auf der Site verbleibenden Daten gehen verloren. Wenn Ihre ILM-Richtlinie jedoch zum Schutz vor dem Verlust einer einzelnen Site konzipiert wurde, sind auf den verbleibenden Sites weiterhin Kopien Ihrer Objektdaten vorhanden. Sehen "Aktivieren Sie den Site-Loss-Schutz" .

Schritte

1. Überprüfen Sie ab Schritt 2 (Details anzeigen) alle Warnungen im Zusammenhang mit der Site, die Sie zum Entfernen ausgewählt haben.

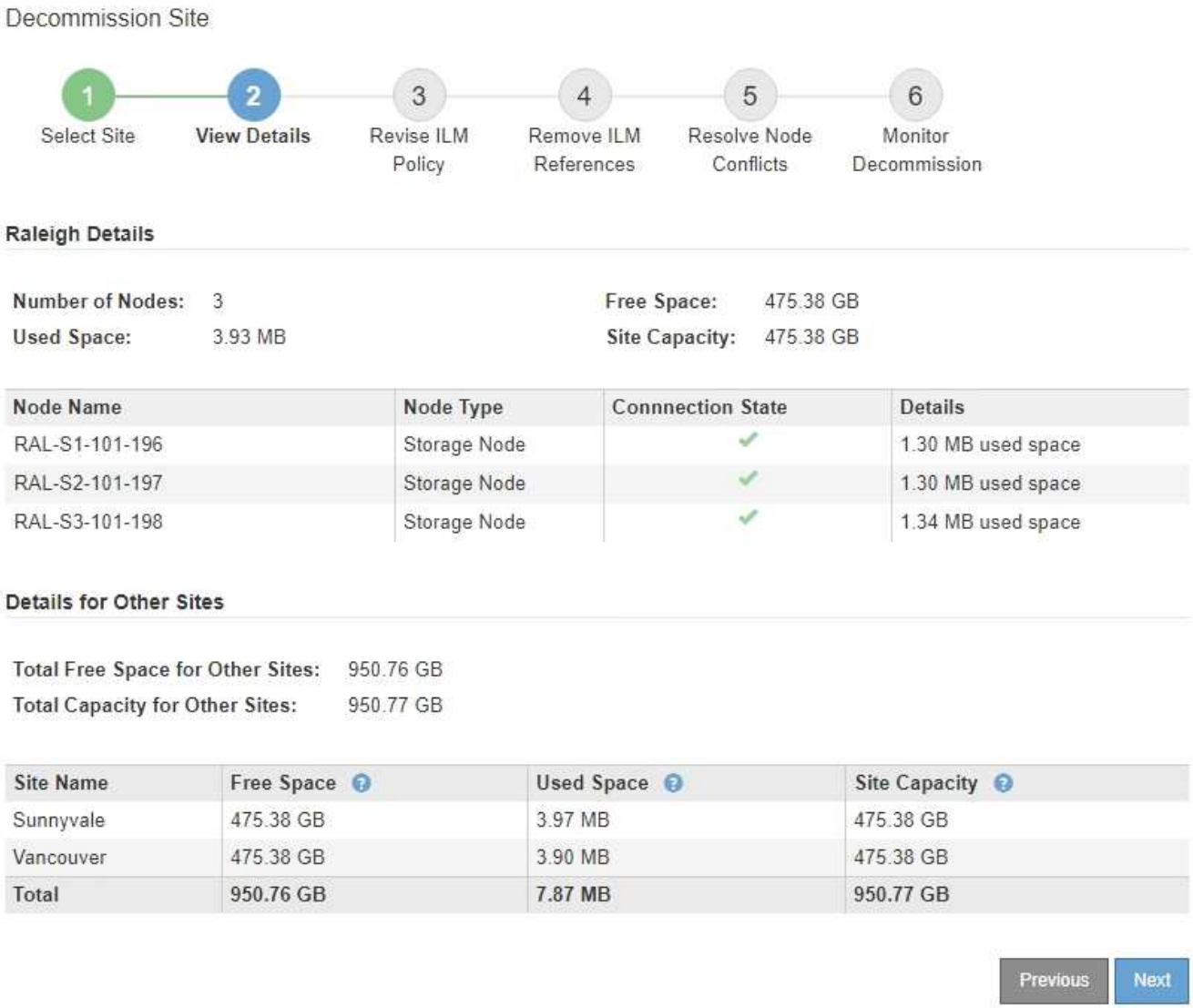


   In diesen Fällen wird eine Warnung angezeigt:

   - Die Site umfasst einen Gateway-Knoten. Wenn S3-Clients derzeit eine Verbindung zu diesem Knoten herstellen, müssen Sie einen entsprechenden Knoten an einem anderen Standort konfigurieren. Stellen Sie sicher, dass Clients eine Verbindung zum Ersatzknoten herstellen können, bevor Sie mit der Außerbetriebnahme fortfahren.

- Die Site enthält eine Mischung aus verbundenen ( ) und getrennte Knoten (oder). Bevor Sie diese Site entfernen können, müssen Sie alle Offline-Knoten wieder online bringen.

2. Überprüfen Sie die Details der Site, die Sie zum Entfernen ausgewählt haben.



Für den ausgewählten Standort sind folgende Informationen enthalten:

- Anzahl der Knoten
- Der insgesamt genutzte Speicherplatz, der freie Speicherplatz und die Kapazität aller Speicherknoten am Standort.
  - Bei der Außerbetriebnahme eines verbundenen Standorts gibt der Wert „Verwendeter Speicherplatz“ an, wie viele Objektdaten an andere Standorte verschoben oder mit ILM gelöscht werden müssen.
  - Bei der Außerbetriebnahme einer getrennten Site gibt der Wert „Benutzter Speicherplatz“ an, wie viele Objektdaten nicht mehr zugänglich sind, wenn Sie die Site entfernen.
- Knotennamen, Typen und Verbindungszustände:
  - (Verbunden)

- (Administrativ nicht erreichbar)
- (Unbekannt)

◦ Details zu jedem Knoten:

- Für jeden Speicherknoten die Menge an Speicherplatz, die für Objektdaten verwendet wurde.
- Bei Admin-Knoten und Gateway-Knoten: Ob der Knoten derzeit in einer Hochverfügbarkeitsgruppe (HA) verwendet wird. Sie können einen Admin-Knoten oder Gateway-Knoten, der in einer HA-Gruppe verwendet wird, nicht außer Betrieb nehmen. Bevor Sie mit der Außerbetriebnahme beginnen, bearbeiten Sie HA-Gruppen, um alle Knoten am Standort zu entfernen, oder entfernen Sie die HA-Gruppe, wenn sie nur Knoten von diesem Standort enthält. Anweisungen hierzu finden Sie unter"Verwalten von Hochverfügbarkeitsgruppen (HA)" .

3. Prüfen Sie im Abschnitt „Details für andere Sites“ der Seite, wie viel Platz an den anderen Sites in Ihrem Raster verfügbar ist.

   Wenn Sie eine verbundene Site außer Betrieb nehmen und ILM zum Verschieben von Objektdaten von der ausgewählten Site verwenden möchten (anstatt sie einfach zu löschen), müssen Sie sicherstellen, dass die anderen Sites über genügend Kapazität verfügen, um die verschobenen Daten aufzunehmen, und dass ausreichend Kapazität für zukünftiges Wachstum verbleibt.

   > Eine Warnung wird angezeigt, wenn der **belegte Speicherplatz** für die Site, die Sie entfernen möchten, größer ist als der **gesamte freie Speicherplatz für andere Sites**. Um sicherzustellen, dass nach der Entfernung der Site ausreichend Speicherkapazität zur Verfügung steht, müssen Sie möglicherweise vor der Durchführung dieses Verfahrens eine Erweiterung durchführen.

4. Wählen Sie **Weiter**.

   Schritt 3 (ILM-Richtlinie überarbeiten) wird angezeigt.

Schritt 3: ILM-Richtlinien überarbeiten

In Schritt 3 (ILM-Richtlinien überarbeiten) des Assistenten „Site außer Betrieb nehmen“ können Sie feststellen, ob auf die Site eine ILM-Richtlinie verweist.

Bevor Sie beginnen

Sie haben ein gutes Verständnis dafür, wie man"Objekte mit ILM verwalten" . Sie sind mit der Erstellung von Speicherpools und ILM-Regeln sowie mit der Simulation und Aktivierung einer ILM-Richtlinie vertraut.

Informationen zu diesem Vorgang

StorageGRID kann eine Site nicht außer Betrieb nehmen, wenn eine ILM-Regel in einer Richtlinie (aktiv oder inaktiv) auf diese Site verweist.

Wenn sich eine ILM-Richtlinie auf die Site bezieht, die Sie außer Betrieb nehmen möchten, müssen Sie diese Richtlinien entfernen oder bearbeiten, sodass sie die folgenden Anforderungen erfüllen:

- Vollständiger Schutz aller Objektdaten.
- Beziehen Sie sich nicht auf die Site, die Sie außer Betrieb nehmen.
- Verwenden Sie keine Speicherpools, die auf die Site verweisen, und verwenden Sie nicht die Option „Alle

Sites“.

- Verwenden Sie keine Erasure-Coding-Profile, die sich auf die Site beziehen.
- Verwenden Sie nicht die Regel „2 Kopien erstellen“ aus StorageGRID 11.6 oder früheren Installationen.

> Erstellen Sie niemals eine ILM-Regel für eine einzelne Kopie, um die Entfernung einer Site zu ermöglichen. Eine ILM-Regel, die für einen bestimmten Zeitraum nur eine replizierte Kopie erstellt, birgt das Risiko eines dauerhaften Datenverlusts. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

> Wenn Sie eine *Außerbetriebnahme einer verbundenen Site* durchführen, müssen Sie berücksichtigen, wie StorageGRID die Objektdaten verwalten soll, die sich derzeit auf der Site befinden, die Sie entfernen möchten. Je nach Ihren Datenschutzanforderungen können neue Regeln vorhandene Objektdaten an andere Standorte verschieben oder zusätzliche Objektkopien löschen, die nicht mehr benötigt werden.

Wenden Sie sich an den technischen Support, wenn Sie Hilfe beim Entwerfen einer neuen Richtlinie benötigen.

Schritte

1. Stellen Sie in Schritt 3 (ILM-Richtlinien überarbeiten) fest, ob sich ILM-Richtlinien auf die Site beziehen, die Sie zur Außerbetriebnahme ausgewählt haben.
2. Wenn keine Richtlinien aufgelistet sind, wählen Sie **Weiter**, um zu"Schritt 4: ILM-Referenzen entfernen" .
3. Wenn eine oder mehrere *aktive* ILM-Richtlinien aufgelistet sind, klonen Sie jede vorhandene Richtlinie oder erstellen Sie neue Richtlinien, die nicht auf die Site verweisen, die außer Betrieb genommen wird:

   a. Wählen Sie den Link für die Richtlinie in der Spalte „Richtlinienname“ aus.

      Die Detailseite der ILM-Richtlinie für die Richtlinie wird in einem neuen Browser-Tab angezeigt. Die Seite „Standort außer Betrieb nehmen“ bleibt auf der anderen Registerkarte geöffnet.

   b. Befolgen Sie bei Bedarf diese Richtlinien und Anweisungen:

      - Arbeiten mit ILM-Regeln:
        - "Erstellen Sie einen oder mehrere Speicherpools"die sich nicht auf die Site beziehen.
        - "Regeln bearbeiten oder ersetzen"die auf die Site verweisen.

          > Wählen Sie nicht die Regel **2 Kopien erstellen** aus, da diese Regel den Speicherpool **Alle Speicherknoten** verwendet, was nicht zulässig ist.

      - Arbeiten mit ILM-Richtlinien:
        - "Klonen einer vorhandenen ILM-Richtlinie"oder"Erstellen einer neuen ILM-Richtlinie" .
        - Stellen Sie sicher, dass sich die Standardregel und andere Regeln nicht auf die Site beziehen.

          > Sie müssen bestätigen, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte von den Regeln in der aufgeführten Reihenfolge (von oben beginnend) ausgewertet.

c. Nehmen Sie Testobjekte auf und simulieren Sie die Richtlinie, um sicherzustellen, dass die richtigen Regeln angewendet werden.

> Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbarem Datenverlust führen. Überprüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert.

> Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese zum Verwalten aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Überprüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und löschcodierter Objekte. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

d. Aktivieren Sie die neuen Richtlinien und stellen Sie sicher, dass die alten Richtlinien jetzt inaktiv sind.

   Wenn Sie mehrere Richtlinien aktivieren möchten,"Befolgen Sie die Schritte zum Erstellen von ILM-Richtlinientags" .

Wenn Sie eine verbundene Site außer Betrieb nehmen, beginnt StorageGRID mit dem Entfernen von Objektdaten von der ausgewählten Site, sobald Sie die neue ILM-Richtlinie aktivieren. Das Verschieben oder Löschen aller Objektkopien kann Wochen dauern. Obwohl Sie eine Site-Außerbetriebnahme sicher starten können, während sich noch Objektdaten auf der Site befinden, wird der Außerbetriebnahmevorgang schneller und mit weniger Unterbrechungen und Leistungseinbußen abgeschlossen, wenn Sie das Verschieben von Daten von der Site zulassen, bevor Sie den eigentlichen Außerbetriebnahmevorgang starten (indem Sie in Schritt 5 des Assistenten **Außerbetriebnahme starten** auswählen).

4. Bearbeiten oder entfernen Sie jede *inaktive* Richtlinie, indem Sie zunächst den Link für die jeweilige Richtlinie auswählen, wie in den vorherigen Schritten beschrieben.
   - "Bearbeiten der Richtlinie"Es handelt sich also nicht um den stillzulegenden Standort.
   - "Entfernen einer Richtlinie" .
5. Wenn Sie mit den Änderungen an den ILM-Regeln und -Richtlinien fertig sind, sollten in Schritt 3 (ILM-Richtlinien überarbeiten) keine weiteren Richtlinien mehr aufgeführt sein. Wählen Sie **Weiter**.

   Schritt 4 (ILM-Referenzen entfernen) wird angezeigt.

Schritt 4: ILM-Referenzen entfernen

Ab Schritt 4 (ILM-Referenzen entfernen) des Assistenten „Site außer Betrieb nehmen“ müssen Sie alle nicht verwendeten ILM-Regeln löschen oder bearbeiten, die auf die Site verweisen, auch wenn die Regeln in keiner ILM-Richtlinie verwendet werden.

Schritte

1. Stellen Sie fest, ob nicht verwendete ILM-Regeln auf die Site verweisen.

   Wenn ILM-Regeln aufgelistet sind, beziehen sich diese Regeln weiterhin auf die Site, werden jedoch in keiner Richtlinie verwendet.

Wenn StorageGRID die Site außer Betrieb nimmt, werden automatisch alle nicht verwendeten Erasure-Coding-Profile deaktiviert, die sich auf die Site beziehen, und alle nicht verwendeten Speicherpools gelöscht, die sich auf die Site beziehen. Der Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) wird entfernt, da er die Site „Alle Sites“ verwendet.

2. Bearbeiten oder löschen Sie jede nicht verwendete Regel:
   - Um eine Regel zu bearbeiten, gehen Sie zur ILM-Regelseite und aktualisieren Sie alle Platzierungen, die ein Erasure-Coding-Profil oder einen Speicherpool verwenden, der auf die Site verweist. Kehren Sie dann zu **Schritt 4 (ILM-Referenzen entfernen)** zurück.
   - Um eine Regel zu löschen, wählen Sie das Papierkorbsymbol und wählen Sie **OK**.

     Sie müssen die Regel **2 Kopien erstellen** löschen, bevor Sie eine Site außer Betrieb nehmen können.

3. Bestätigen Sie, dass keine ungenutzten ILM-Regeln auf die Site verweisen und die Schaltfläche **Weiter** aktiviert ist.
4. Wählen Sie **Weiter**.

   Alle verbleibenden Speicherpools und Erasure-Coding-Profile, die auf die Site verweisen, werden ungültig, wenn die Site entfernt wird. Wenn StorageGRID die Site außer Betrieb nimmt, werden automatisch alle nicht verwendeten Erasure-Coding-Profile deaktiviert, die sich auf die Site beziehen, und alle nicht verwendeten Speicherpools gelöscht, die sich auf die Site beziehen. Der Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) wird entfernt, da er die Site „Alle Sites“ verwendet.

   Schritt 5 (Knotenkonflikte lösen) wird angezeigt.

Schritt 5: Knotenkonflikte lösen (und Außerbetriebnahme starten)

In Schritt 5 (Knotenkonflikte lösen) des Assistenten „Site außer Betrieb nehmen“ können Sie feststellen, ob Knoten in Ihrem StorageGRID -System getrennt sind oder ob Knoten an der ausgewählten Site zu einer Hochverfügbarkeitsgruppe (HA) gehören. Nachdem alle Knotenkonflikte gelöst wurden, starten Sie den Außerbetriebnahmevorgang von dieser Seite aus.

Bevor Sie beginnen

Sie müssen sicherstellen, dass sich alle Knoten in Ihrem StorageGRID -System wie folgt im richtigen Zustand befinden:

- Alle Knoten in Ihrem StorageGRID -System müssen verbunden sein ( ).

  Wenn Sie die Außerbetriebnahme eines getrennten Standorts durchführen, müssen alle Knoten am Standort, den Sie entfernen, getrennt und alle Knoten an allen anderen Standorten verbunden werden.

Die Außerbetriebnahme wird nicht gestartet, wenn ein oder mehrere Volumes offline (nicht gemountet) sind oder wenn sie online (gemountet) sind, sich aber in einem Fehlerzustand befinden.

Wenn während einer Außerbetriebnahme ein oder mehrere Volumes offline gehen, wird der Außerbetriebnahmevorgang abgeschlossen, nachdem diese Volumes wieder online sind.

- Kein Knoten an der Site, die Sie entfernen, darf über eine Schnittstelle verfügen, die zu einer Hochverfügbarkeitsgruppe (HA) gehört.

Informationen zu diesem Vorgang

Wenn für Schritt 5 (Knotenkonflikte lösen) ein beliebiger Knoten aufgeführt ist, müssen Sie das Problem beheben, bevor Sie mit der Außerbetriebnahme beginnen können.

Bevor Sie mit der Außerbetriebnahme der Site auf dieser Seite beginnen, lesen Sie die folgenden Hinweise:

- Sie müssen ausreichend Zeit einplanen, damit der Außerbetriebnahmevorgang abgeschlossen werden kann.

  Das Verschieben oder Löschen von Objektdaten von einer Site kann Tage, Wochen oder sogar Monate dauern, abhängig von der Datenmenge an der Site, der Auslastung Ihres Systems, den Netzwerklatenzen und der Art der erforderlichen ILM-Änderungen.

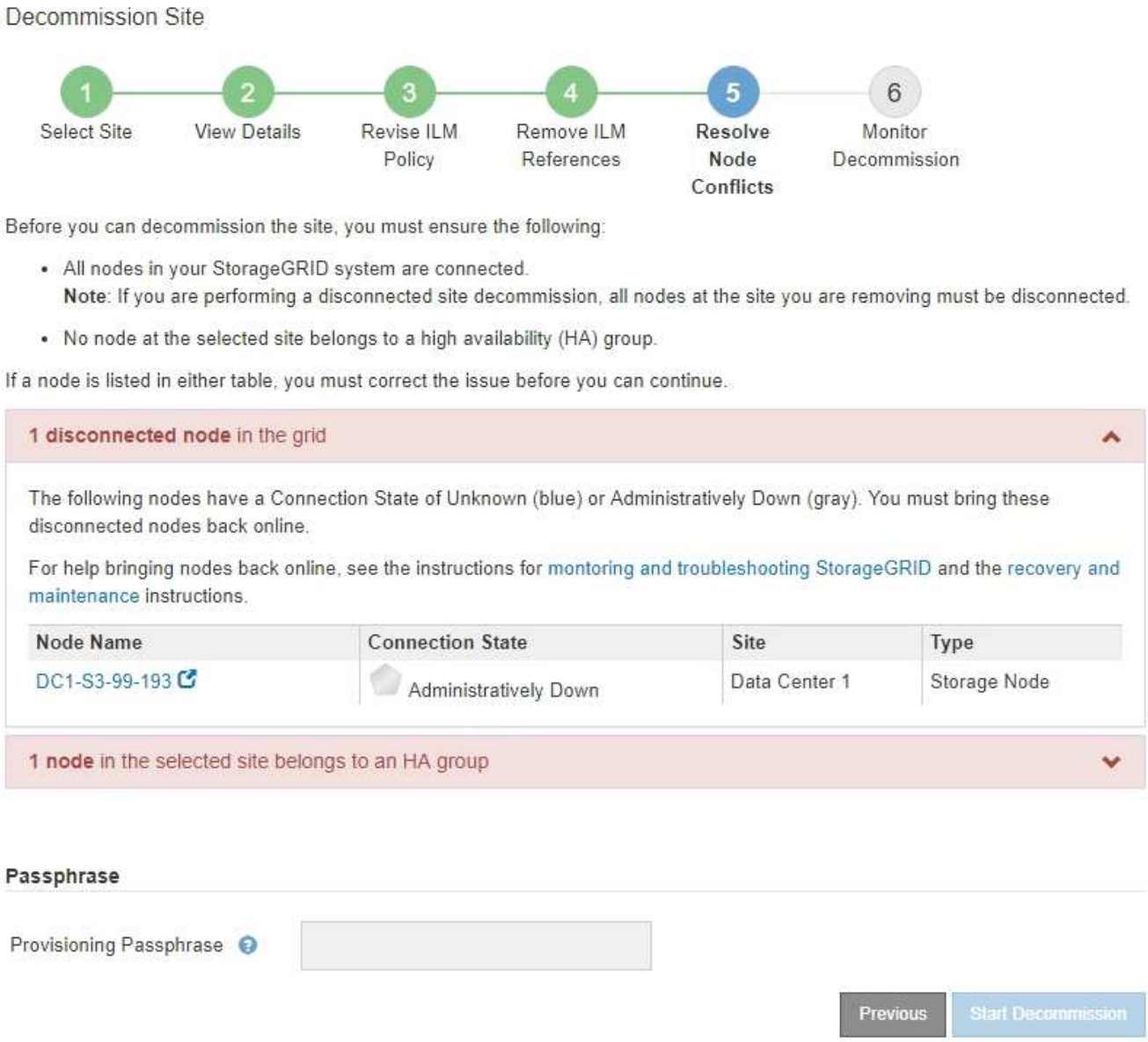
- Während das Verfahren zur Außerbetriebnahme des Standorts läuft:
  - Sie können keine ILM-Regeln erstellen, die sich auf die Außerbetriebnahme der Site beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf die Site zu verweisen.
  - Sie können keine anderen Wartungsvorgänge wie Erweiterungen oder Upgrades durchführen.

    Wenn Sie während der Außerbetriebnahme einer verbundenen Site ein weiteres Wartungsverfahren durchführen müssen, können Sie das Verfahren anhalten, während die Speicherknoten entfernt werden. Die Schaltfläche **Pause** ist während der Phase „Außerbetriebnahme replizierter und Erasure-Coded-Daten“ aktiviert.

  - Wenn Sie nach dem Start des Site-Außerbetriebnahmeverfahrens einen Knoten wiederherstellen müssen, müssen Sie sich an den Support wenden.

Schritte

1. Überprüfen Sie den Abschnitt zu getrennten Knoten in Schritt 5 (Knotenkonflikte lösen), um festzustellen, ob Knoten in Ihrem StorageGRID -System den Verbindungsstatus „Unbekannt“ aufweisen ( ) oder „Administrativ deaktiviert“ ( ).

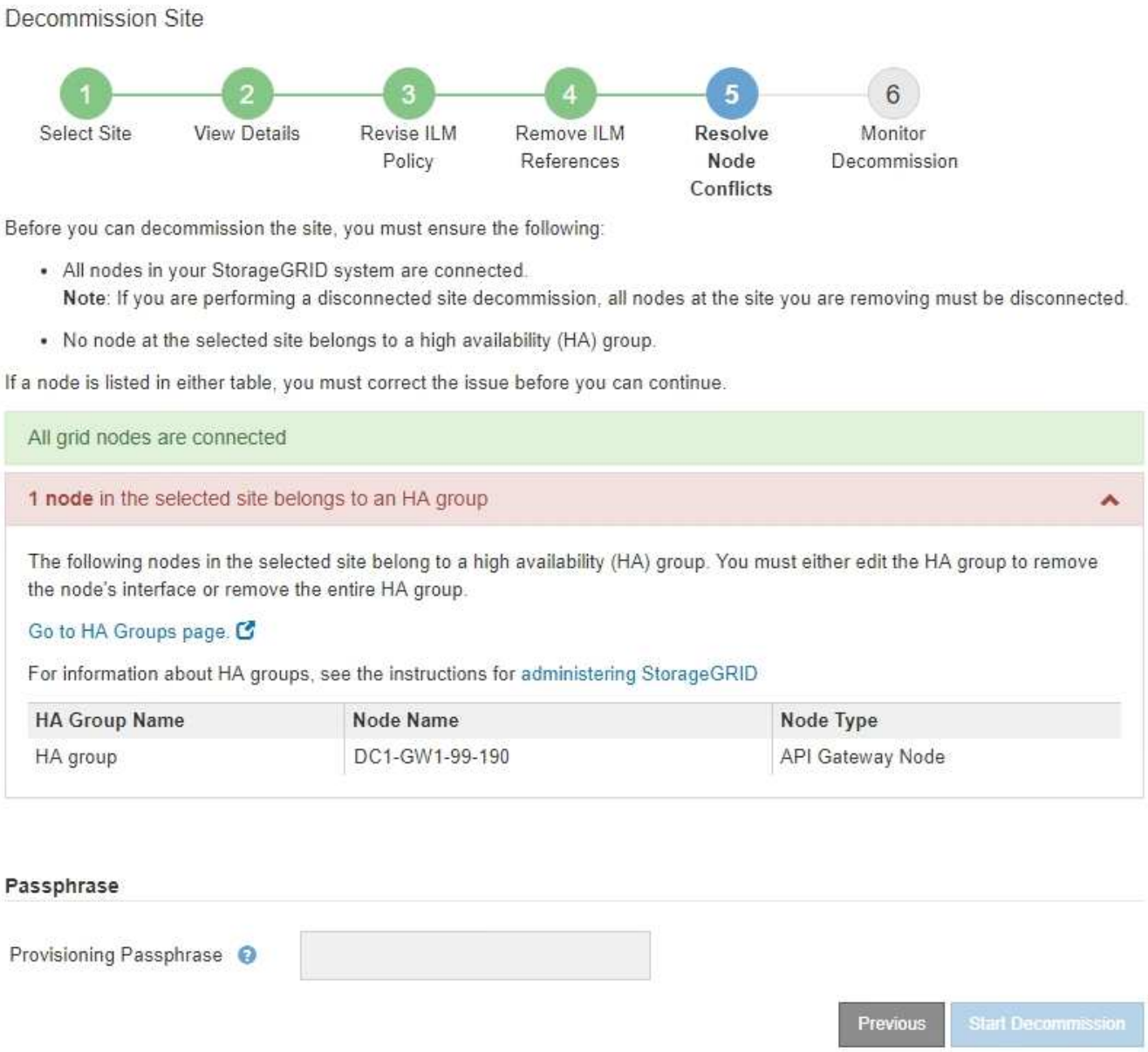


2. Wenn Knoten getrennt werden, bringen Sie sie wieder online.

   Siehe die"Knotenprozeduren" . Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen.

3. Wenn alle getrennten Knoten wieder online gebracht wurden, lesen Sie den Abschnitt „HA-Gruppen“ in Schritt 5 (Knotenkonflikte lösen).

   In dieser Tabelle sind alle Knoten am ausgewählten Standort aufgeführt, die zu einer Hochverfügbarkeitsgruppe (HA) gehören.

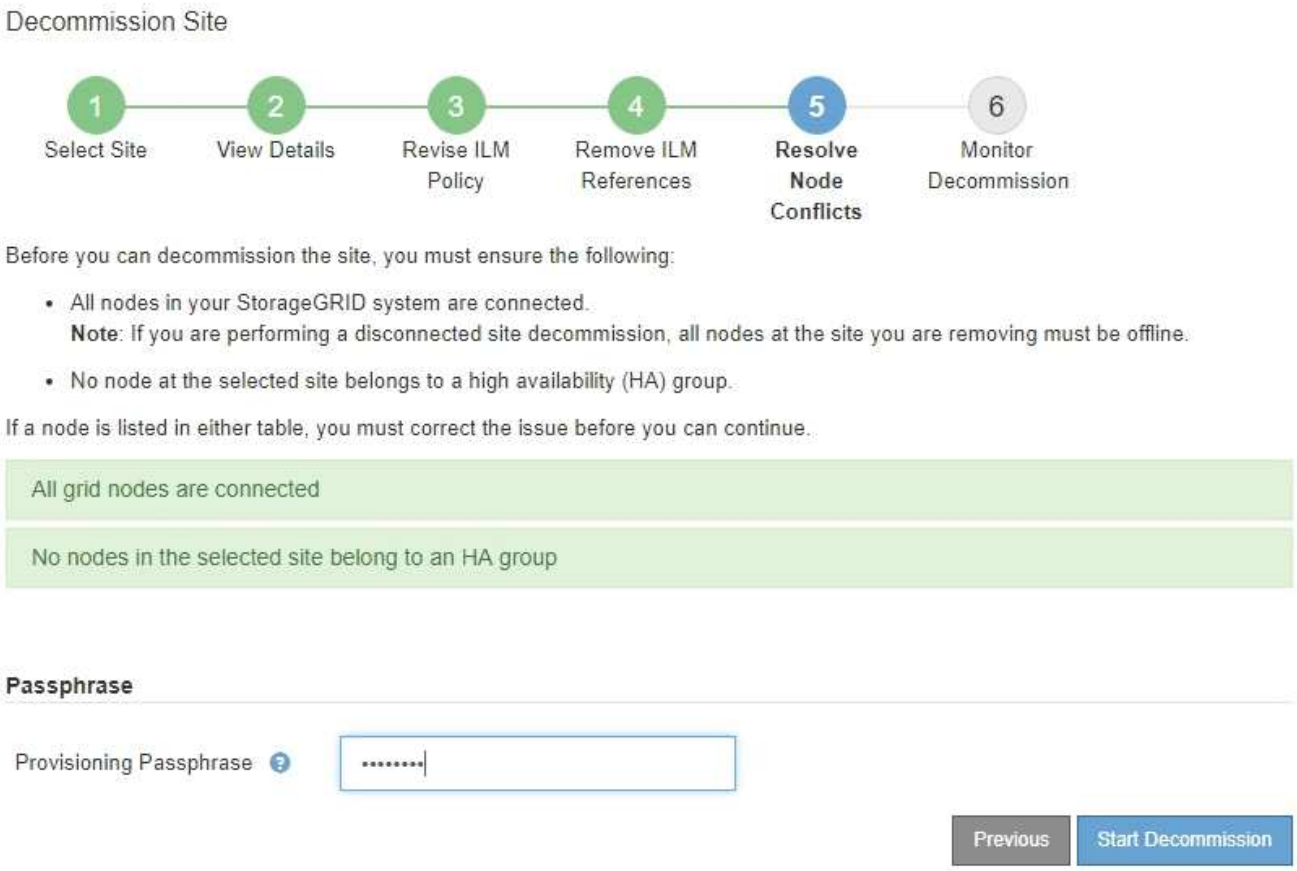


4. Wenn Knoten aufgelistet sind, führen Sie einen der folgenden Schritte aus:
   - Bearbeiten Sie jede betroffene HA-Gruppe, um die Knotenschnittstelle zu entfernen.
   - Entfernen Sie eine HA-Gruppe, die nur Knoten von dieser Site enthält. Siehe die Anweisungen zur Verwaltung von StorageGRID.

   Wenn alle Knoten verbunden sind und keine Knoten am ausgewählten Standort in einer HA-Gruppe verwendet werden, ist das Feld **Bereitstellungspassphrase** aktiviert.

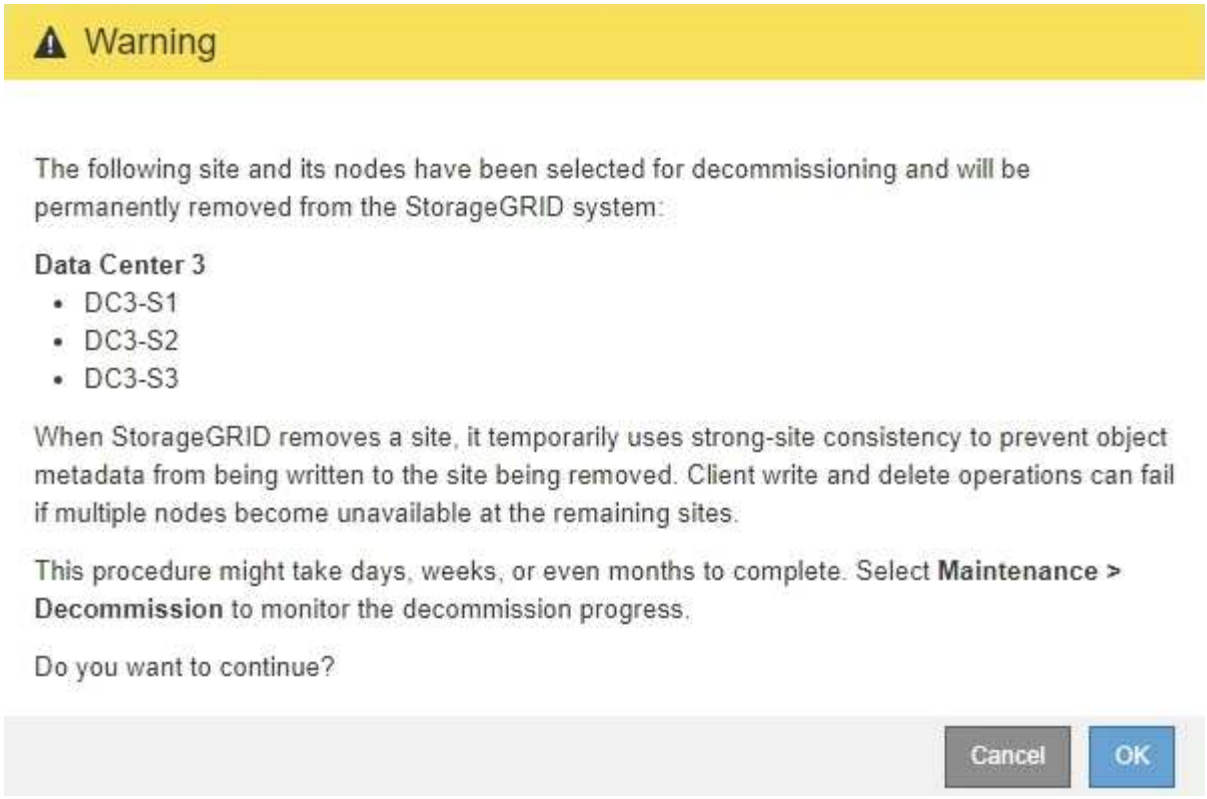
5. Geben Sie die Bereitstellungspassphrase ein.

   Die Schaltfläche **Außerbetriebnahme starten** wird aktiviert.



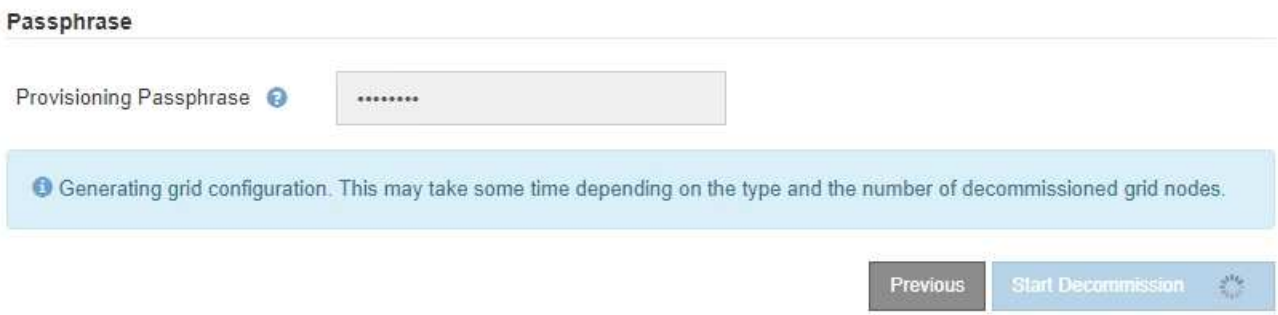
6. Wenn Sie bereit sind, mit der Außerbetriebnahme der Site zu beginnen, wählen Sie **Außerbetriebnahme starten**.

   In einer Warnung werden die Site und Knoten aufgelistet, die entfernt werden. Sie werden daran erinnert, dass es Tage, Wochen oder sogar Monate dauern kann, bis die Site vollständig entfernt ist.



7. Lesen Sie die Warnung. Wenn Sie bereit sind zu beginnen, wählen Sie **OK**.

   Während die neue Rasterkonfiguration generiert wird, wird eine Meldung angezeigt. Dieser Vorgang kann je nach Art und Anzahl der stillgelegten Netzknoten einige Zeit in Anspruch nehmen.



   Wenn die neue Netzkonfiguration erstellt wurde, wird Schritt 6 (Monitor-Außerbetriebnahme) angezeigt.

   Die Schaltfläche **Zurück** bleibt deaktiviert, bis die Außerbetriebnahme abgeschlossen ist.

Schritt 6: Außerbetriebnahme überwachen

Ab Schritt 6 (Außerbetriebnahme überwachen) des Assistenten „Site außer Betrieb nehmen“ können Sie den Fortschritt beim Entfernen der Site überwachen.

Informationen zu diesem Vorgang

Wenn StorageGRID eine verbundene Site entfernt, werden die Knoten in dieser Reihenfolge entfernt:

1. Gateway-Knoten

2. Admin-Knoten
3. Speicherknoten

Wenn StorageGRID eine getrennte Site entfernt, werden die Knoten in dieser Reihenfolge entfernt:

1. Gateway-Knoten
2. Speicherknoten
3. Admin-Knoten

Das Entfernen jedes Gateway-Knotens oder Admin-Knotens kann möglicherweise nur wenige Minuten oder eine Stunde dauern, bei Speicherknoten kann es jedoch Tage oder Wochen dauern.

Schritte

1. Sobald ein neues Wiederherstellungspaket erstellt wurde, laden Sie die Datei herunter.

   > Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Netz wiederherstellen können, falls während der Außerbetriebnahme etwas schiefgeht.

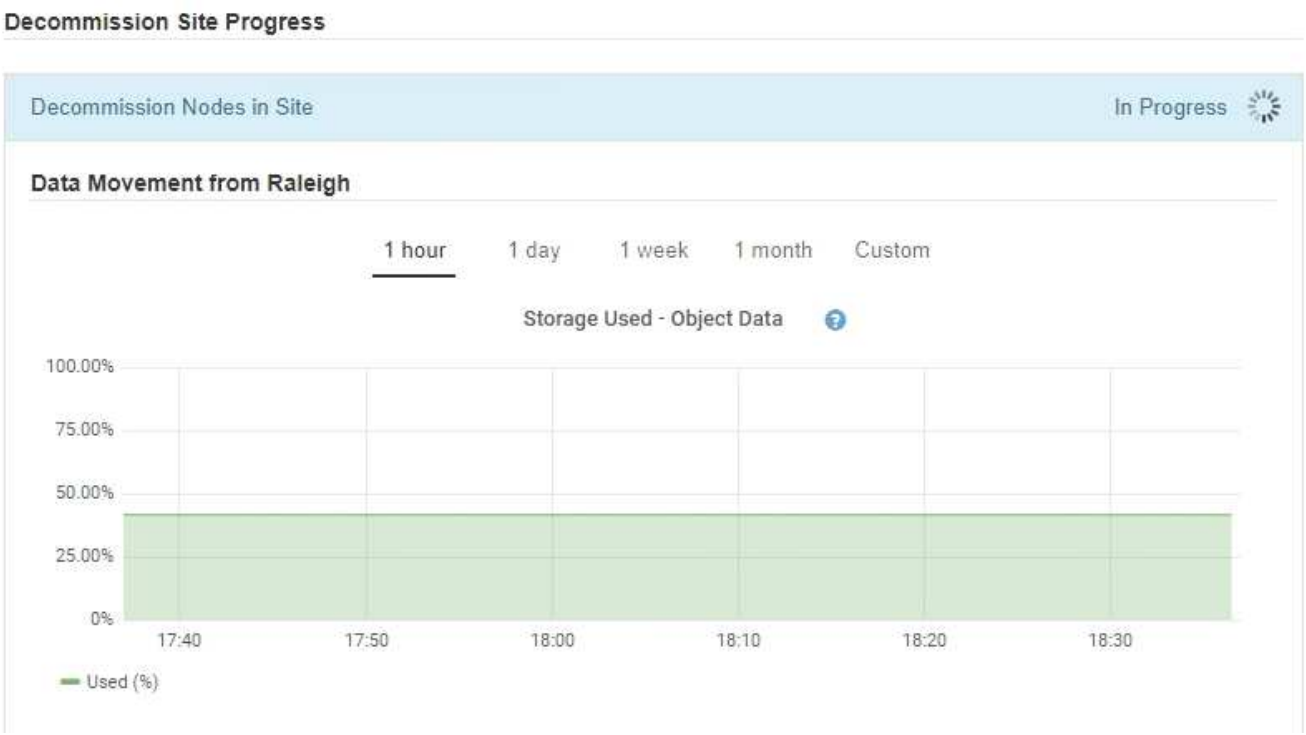
   a. Wählen Sie den Link in der Nachricht oder wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
   b. Laden Sie die `.zip` Datei.

      Siehe die Anweisungen für"Herunterladen des Wiederherstellungspakets" .

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

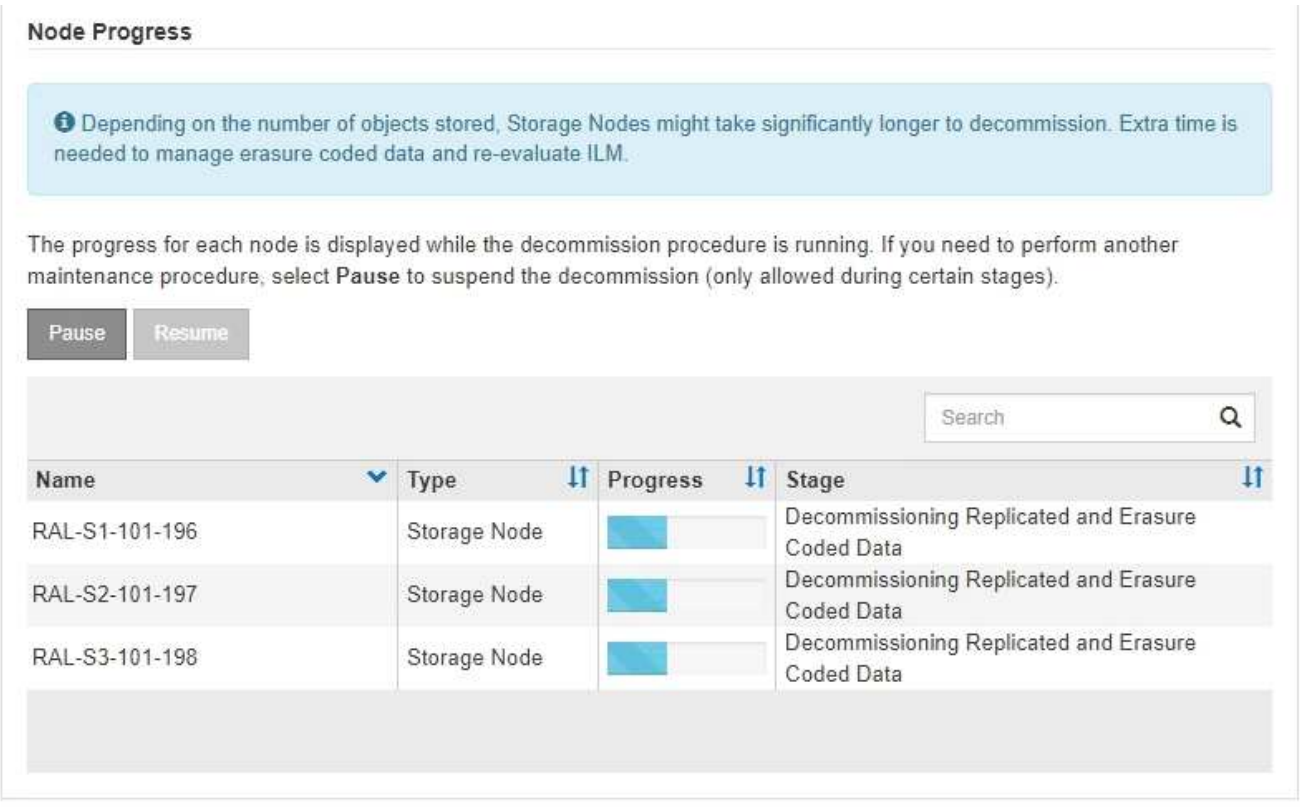
2. Überwachen Sie mithilfe des Datenbewegungsdiagramms die Bewegung von Objektdaten von dieser Site zu anderen Sites.

   Die Datenbewegung begann, als Sie in Schritt 3 (ILM-Richtlinie überarbeiten) die neue ILM-Richtlinie aktiviert haben. Während des gesamten Außerbetriebnahmeverfahrens werden Daten verschoben.



3. Überwachen Sie im Abschnitt „Knotenfortschritt“ der Seite den Fortschritt des Außerbetriebnahmeverfahrens, während Knoten entfernt werden.

   Wenn ein Speicherknoten entfernt wird, durchläuft jeder Knoten eine Reihe von Phasen. Obwohl die meisten dieser Phasen schnell oder sogar unmerklich ablaufen, müssen Sie je nach der zu verschiebenden Datenmenge möglicherweise Tage oder sogar Wochen warten, bis andere Phasen abgeschlossen sind. Für die Verwaltung von Erasure-Coded-Daten und die Neubewertung von ILM ist zusätzliche Zeit erforderlich.



Wenn Sie den Fortschritt der Außerbetriebnahme eines verbundenen Standorts überwachen, finden Sie in dieser Tabelle Informationen zu den Außerbetriebnahmephasen eines Speicherknotens:

Bühne	Geschätzte Dauer
Ausstehend	Minute oder weniger
Warten auf Sperren	Minuten
Aufgabe vorbereiten	Minute oder weniger
Kennzeichnung LDR außer Betrieb genommen	Minuten
Außerbetriebnahme replizierter und Erasure-Coded-Daten	Stunden, Tage oder Wochen, je nach Datenmenge **Hinweis**: Wenn Sie andere Wartungsaktivitäten durchführen müssen, können Sie die Außerbetriebnahme der Site während dieser Phase unterbrechen.
LDR-Einstellungsstatus	Minuten
Audit-Warteschlangen leeren	Minuten bis Stunden, basierend auf der Anzahl der Nachrichten und der Netzwerklatenz.
Vollständig	Minuten

Wenn Sie den Fortschritt der Außerbetriebnahme eines getrennten Standorts überwachen, finden Sie in dieser Tabelle Informationen zu den Außerbetriebnahmephasen eines Speicherknotens:

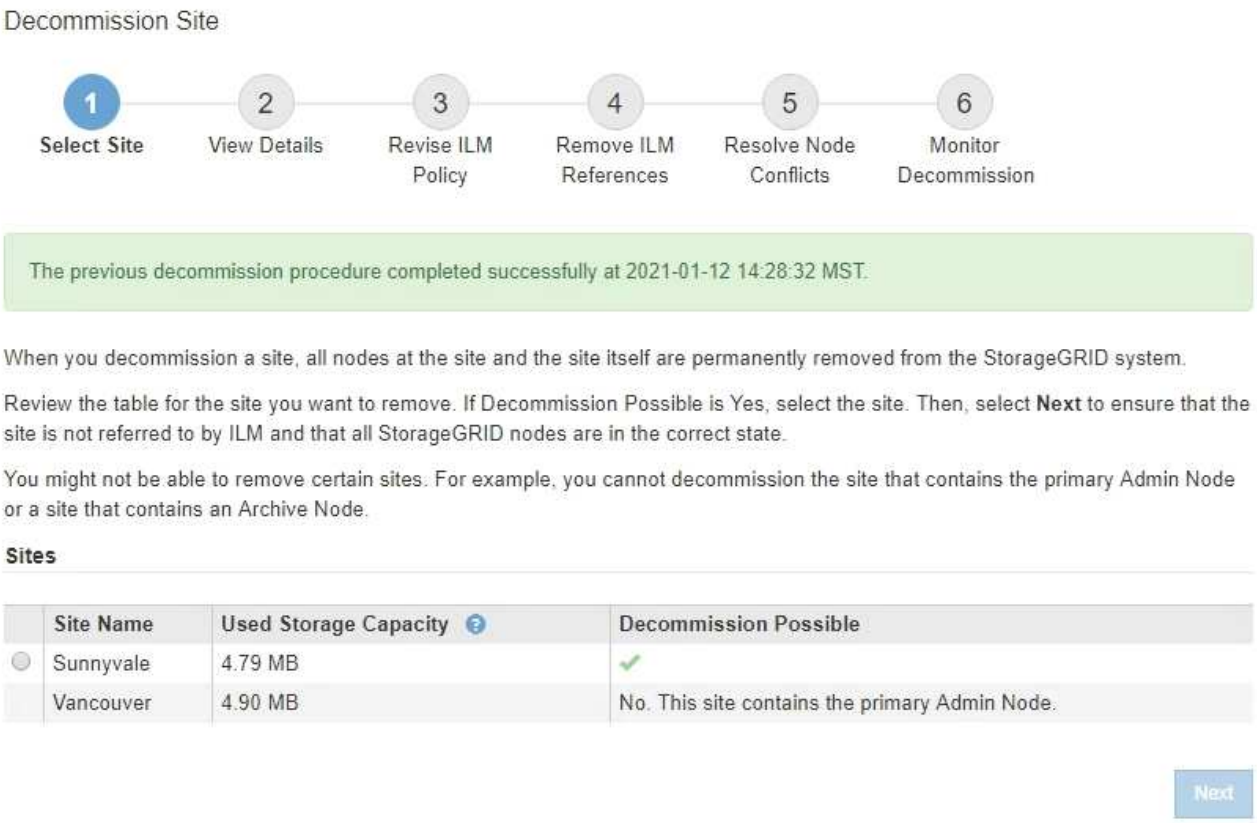
Bühne	Geschätzte Dauer
Ausstehend	Minute oder weniger
Warten auf Sperren	Minuten
Aufgabe vorbereiten	Minute oder weniger
Externe Dienste deaktivieren	Minuten
Zertifikatssperrung	Minuten
Knoten abmelden	Minuten
Storage Grade-Registrierung aufheben	Minuten
Entfernen einer Speichergruppe	Minuten

Bühne	Geschätzte Dauer
Entitätsentfernung	Minuten
Vollständig	Minuten

4. Nachdem alle Knoten die Phase „Abgeschlossen“ erreicht haben, warten Sie, bis die verbleibenden Außerbetriebnahmevorgänge der Site abgeschlossen sind.
   - Während des Schritts **Cassandra reparieren** führt StorageGRID alle notwendigen Reparaturen an den Cassandra-Clustern durch, die in Ihrem Grid verbleiben. Diese Reparaturen können mehrere Tage oder länger dauern, je nachdem, wie viele Speicherknoten in Ihrem Netz verbleiben.
   - Während des Schritts **EC-Profile deaktivieren und Speicherpools löschen** werden die folgenden ILM-Änderungen vorgenommen:
     - Alle Erasure-Coding-Profile, die auf die Site verwiesen, werden deaktiviert.
     - Alle Speicherpools, die auf die Site verwiesen, werden gelöscht.

       Der Speicherpool „All Storage Nodes“ (StorageGRID 11.6 und früher) wird ebenfalls entfernt, da er die Site „All Sites“ verwendet.
   - Schließlich werden während des Schritts **Konfiguration entfernen** alle verbleibenden Verweise auf die Site und ihre Knoten aus dem Rest des Rasters entfernt.

5. Wenn der Außerbetriebnahmevorgang abgeschlossen ist, wird auf der Seite „Site außer Betrieb nehmen“ eine Erfolgsmeldung angezeigt und die entfernte Site wird nicht mehr angezeigt.



Nach Abschluss

Führen Sie diese Aufgaben aus, nachdem Sie das Verfahren zur Außerbetriebnahme der Site abgeschlossen haben:

- Stellen Sie sicher, dass die Laufwerke aller Speicherknoten am stillgelegten Standort gelöscht werden. Verwenden Sie ein handelsübliches Tool oder einen Dienst zum Löschen von Daten, um Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn die Site einen oder mehrere Admin-Knoten umfasst und Single Sign-On (SSO) für Ihr StorageGRID -System aktiviert ist, entfernen Sie alle Vertrauensstellungen der vertrauenden Seite für die Site aus Active Directory Federation Services (AD FS).
- Nachdem die Knoten im Rahmen der Außerbetriebnahme der verbundenen Site automatisch und ordnungsgemäß ausgeschaltet wurden, entfernen Sie die zugehörigen virtuellen Maschinen.

Raster, Site oder Knoten umbenennen

Verwenden Sie das Umbenennungsverfahren

Bei Bedarf können Sie die Anzeigenamen ändern, die im gesamten Grid Manager für das gesamte Grid, jede Site und jeden Knoten angezeigt werden. Sie können Anzeigenamen jederzeit und sicher aktualisieren.

Wie läuft das Umbenennungsverfahren ab?

Wenn Sie StorageGRID zum ersten Mal installieren, geben Sie einen Namen für das Grid, jede Site und jeden Knoten an. Diese anfänglichen Namen werden als *Systemnamen* bezeichnet und sind die Namen, die

anfänglich in StorageGRID angezeigt werden.

Systemnamen sind für interne StorageGRID -Vorgänge erforderlich und können nicht geändert werden. Sie können jedoch das Umbenennungsverfahren verwenden, um neue *Anzeigenamen* für das Raster, jede Site und jeden Knoten zu definieren. Diese Anzeigenamen erscheinen an verschiedenen StorageGRID Standorten anstelle (oder in einigen Fällen zusätzlich) der zugrunde liegenden Systemnamen.

Verwenden Sie das Umbenennungsverfahren, um Tippfehler zu korrigieren, eine andere Namenskonvention zu implementieren oder anzuzeigen, dass eine Site und alle ihre Knoten verschoben wurden. Im Gegensatz zu Systemnamen können Anzeigenamen bei Bedarf und ohne Auswirkungen auf den StorageGRID -Betrieb aktualisiert werden.

Wo erscheinen System- und Anzeigenamen?

Die folgende Tabelle fasst zusammen, wo Systemnamen und Anzeigenamen in der StorageGRID Benutzeroberfläche und in StorageGRID Dateien angezeigt werden.

Standort	Systemname	Anzeigename
Grid Manager-Seiten	Wird angezeigt, sofern das Element nicht umbenannt wird	Wenn ein Element umbenannt wird, wird es anstelle des Systemnamens an diesen Stellen angezeigt: • Dashboard • Knotenseite • Konfigurationsseiten für Hochverfügbarkeitsgruppen, Load Balancer-Endpunkte, VLAN-Schnittstellen, Schlüsselverwaltungsserver, Grid-Passwörter und Firewall-Steuerung • Warnungen • Speicherpooldefinitionen • Suchseite für Objektmetadaten • Seiten zu Wartungsverfahren, einschließlich Upgrade, Hotfix, SANtricity OS-Upgrade, Außerbetriebnahme, Erweiterung, Wiederherstellung und Objektexistenzprüfung • Supportseiten (Protokolle und Diagnose) • Single-Sign-On-Seite, neben dem Hostnamen des Admin-Knotens in der Tabelle für Admin-Knoten-Details
NODES > Registerkarte **Übersicht** für einen Knoten	Immer angezeigt	Wird nur angezeigt, wenn das Element umbenannt wird

Standort	Systemname	Anzeigename
Legacy-Seiten im Grid Manager (z. B. **SUPPORT** > **Grid-Topologie**)	Gezeigt	Nicht angezeigt
Knotenzustand API	Immer wieder	Wird nur zurückgegeben, wenn das Element umbenannt wird

Eingabeaufforderung bei Verwendung von SSH für den Zugriff auf einen Knoten	Wird als primärer Name angezeigt, sofern das Element nicht umbenannt wurde:
	
	`admin@SYSTEM-NAME: ~ $`
	
	In Klammern enthalten, wenn das Element umbenannt wird:
	
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		Wird als primärer Name angezeigt, wenn das Element umbenannt wird:
		
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt`Datei im Wiederherstellungspaket	Dargestellt als `Server Name`	Dargestellt als `Display Name`
`/etc/hosts`Datei auf allen Knoten Beispiel: `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	Wird immer in der zweiten Spalte angezeigt	Wenn das Element umbenannt wird, wird in der vierten Spalte angezeigt
`topology-display-names.json`, in den AutoSupport Daten enthalten	Nicht enthalten	Leer, sofern die Elemente nicht umbenannt wurden. Andernfalls werden Raster-, Site- und Knoten-IDs ihren Anzeigenamen zugeordnet.

Anforderungen für den Anzeigenamen

Überprüfen Sie vor der Verwendung dieses Verfahrens die Anforderungen für Anzeigenamen.

Anzeigenamen für Knoten

Anzeigenamen für Knoten müssen diesen Regeln entsprechen:

- Muss in Ihrem StorageGRID -System eindeutig sein.

- Darf nicht mit dem Systemnamen eines anderen Elements in Ihrem StorageGRID System identisch sein.
- Muss mindestens 1 und darf nicht mehr als 32 Zeichen enthalten.
- Kann Zahlen, Bindestriche (-) sowie Groß- und Kleinbuchstaben enthalten.
- Kann mit einem Buchstaben oder einer Zahl beginnen oder enden, darf aber nicht mit einem Bindestrich beginnen oder enden.
- Es können nicht nur Zahlen sein.
- Unterscheiden nicht zwischen Groß- und Kleinschreibung. Zum Beispiel, `DC1-ADM` Und `dc1-adm` werden als Duplikate betrachtet.

Sie können einen Knoten mit einem Anzeigenamen umbenennen, der zuvor von einem anderen Knoten verwendet wurde, solange die Umbenennung nicht zu einem doppelten Anzeigenamen oder Systemnamen führt.

Anzeigenamen für Raster und Sites

Für die Anzeigenamen des Rasters und der Sites gelten die gleichen Regeln mit folgenden Ausnahmen:

- Kann Leerzeichen enthalten.
- Kann diese Sonderzeichen enthalten: `= - _ : , . @ !`
- Kann mit Sonderzeichen, einschließlich Bindestrichen, beginnen und enden.
- Können alle Zahlen oder Sonderzeichen sein.

Bewährte Methoden für Anzeigenamen

Wenn Sie mehrere Elemente umbenennen möchten, dokumentieren Sie Ihr allgemeines Benennungsschema, bevor Sie dieses Verfahren verwenden. Entwickeln Sie ein System, das sicherstellt, dass die Namen eindeutig, konsistent und auf den ersten Blick leicht verständlich sind.

Sie können jede Namenskonvention verwenden, die Ihren organisatorischen Anforderungen entspricht. Beachten Sie die folgenden grundlegenden Vorschläge für die Einbeziehung:

- **Site-Indikator**: Wenn Sie mehrere Sites haben, fügen Sie jedem Knotennamen einen Site-Code hinzu.
- **Knotentyp**: Knotennamen geben normalerweise den Typ des Knotens an. Sie können Abkürzungen verwenden wie `s` , `adm` , Und `gw` (Speicherknoten, Admin-Knoten und Gateway-Knoten).
- **Knotennummer**: Wenn eine Site mehr als einen Knoten eines bestimmten Typs enthält, fügen Sie dem Namen jedes Knotens eine eindeutige Nummer hinzu.

Überlegen Sie es sich zweimal, bevor Sie den Namen spezifische Details hinzufügen, die sich im Laufe der Zeit wahrscheinlich ändern. Fügen Sie beispielsweise keine IP-Adressen in Knotennamen ein, da diese Adressen geändert werden können. Ebenso können sich Rack-Standorte oder Gerätemodellnummern ändern, wenn Sie Geräte verschieben oder die Hardware aktualisieren.

Beispiele für Anzeigenamen

Angenommen, Ihr StorageGRID -System verfügt über drei Rechenzentren und in jedem Rechenzentrum über Knoten unterschiedlichen Typs. Ihre Anzeigenamen könnten so einfach sein wie diese:

- **Netz**: `StorageGRID Deployment`
- **Erste Seite**: `Data Center 1`

- dc1-adm1
- dc1-s1
- dc1-s2
- dc1-s3
- dc1-gw1

- **Zweite Site**: Data Center 2
  - dc2-adm2
  - dc2-s1
  - dc2-s2
  - dc2-s3
- **Dritte Site**: Data Center 3
  - dc3-s1
  - dc3-s2
  - dc3-s3

Anzeigenamen hinzufügen oder aktualisieren

Mit diesem Verfahren können Sie die für Ihr Raster, Ihre Sites und Knoten verwendeten Anzeigenamen hinzufügen oder aktualisieren. Sie können ein einzelnes Element, mehrere Elemente oder sogar alle Elemente gleichzeitig umbenennen. Das Definieren oder Aktualisieren eines Anzeigenamens hat keinerlei Auswirkungen auf StorageGRID Vorgänge.

Bevor Sie beginnen

- Vom **primären Admin-Knoten** aus werden Sie beim Grid Manager mit einem"unterstützter Webbrowser" .

> Sie können Anzeigenamen von einem nicht primären Admin-Knoten aus hinzufügen oder aktualisieren, Sie müssen jedoch beim primären Admin-Knoten angemeldet sein, um ein Wiederherstellungspaket herunterzuladen.

- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben die Bereitstellungspassphrase.
- Sie verstehen die Anforderungen und Best Practices für Anzeigenamen. Sehen "Raster, Sites und Knoten umbenennen" .

So benennen Sie Raster, Sites oder Knoten um

Sie können Ihr StorageGRID -System, einen oder mehrere Standorte oder einen oder mehrere Knoten umbenennen.

Sie können einen Anzeigenamen verwenden, der zuvor von einem anderen Knoten verwendet wurde, solange die Umbenennung nicht zu einem doppelten Anzeigenamen oder Systemnamen führt.

Wählen Sie die umzubenennenden Elemente aus

Wählen Sie zunächst die Elemente aus, die Sie umbenennen möchten.

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Raster, Sites und Knoten umbenennen**.
2. Wählen Sie im Schritt **Namen auswählen** die Elemente aus, die Sie umbenennen möchten.

Zu ändernder Artikel	Anweisung
Namen von allem (oder fast allem) in Ihrem System	a. Wählen Sie **Alles auswählen**. b. Löschen Sie optional alle Elemente, die Sie nicht umbenennen möchten.
Name des Rasters	Aktivieren Sie das Kontrollkästchen für das Raster.
Name einer Site und einiger oder aller ihrer Knoten	a. Aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift für die Site. b. Löschen Sie optional alle Knoten, die Sie nicht umbenennen möchten.
Name einer Site	Aktivieren Sie das Kontrollkästchen für die Site.
Name eines Knotens	Aktivieren Sie das Kontrollkästchen für den Knoten.

3. Wählen Sie **Weiter**.
4. Überprüfen Sie die Tabelle, die die von Ihnen ausgewählten Elemente enthält.
   - In der Spalte **Anzeigename** wird der aktuelle Name für jedes Element angezeigt. Wenn das Element nie umbenannt wurde, ist sein Anzeigename derselbe wie sein Systemname.
   - In der Spalte **Systemname** wird der Name angezeigt, den Sie während der Installation für jedes Element eingegeben haben. Systemnamen werden für interne StorageGRID -Vorgänge verwendet und können nicht geändert werden. Beispielsweise könnte der Systemname eines Knotens sein Hostname sein.
   - Die Spalte **Typ** gibt den Typ des Elements an: Raster, Site oder der spezifische Knotentyp.

Neue Namen vorschlagen

Im Schritt **Neue Namen vorschlagen** können Sie für jedes Element einzeln einen Anzeigenamen eingeben oder Elemente auf einmal umbenennen.

Elemente einzeln umbenennen

Befolgen Sie diese Schritte, um für jedes Element, das Sie umbenennen möchten, einen Anzeigenamen einzugeben.

Schritte

1. Geben Sie im Feld **Anzeigename** einen vorgeschlagenen Anzeigenamen für jedes Element in der Liste ein.

   Sehen"Raster, Sites und Knoten umbenennen" um die Namensanforderungen zu erfahren.

2. Um alle Elemente zu entfernen, die Sie nicht umbenennen möchten, wählen Sie ✕ in der Spalte **Aus Liste entfernen**.

   Wenn Sie für einen Artikel keinen neuen Namen vorschlagen, müssen Sie ihn aus der Tabelle entfernen.

3. Wenn Sie für alle Elemente in der Tabelle neue Namen vorgeschlagen haben, wählen Sie **Umbenennen**.

   Es erscheint eine Erfolgsmeldung. Die neuen Anzeigenamen werden jetzt im gesamten Grid Manager verwendet.

Elemente in großen Mengen umbenennen

Verwenden Sie das Tool zum Massenumbenennen, wenn Elementnamen eine gemeinsame Zeichenfolge aufweisen, die Sie durch eine andere Zeichenfolge ersetzen möchten.

Schritte

1. Wählen Sie für den Schritt **Neue Namen vorschlagen** die Option **Tool zur Massenumbenennung verwenden**.

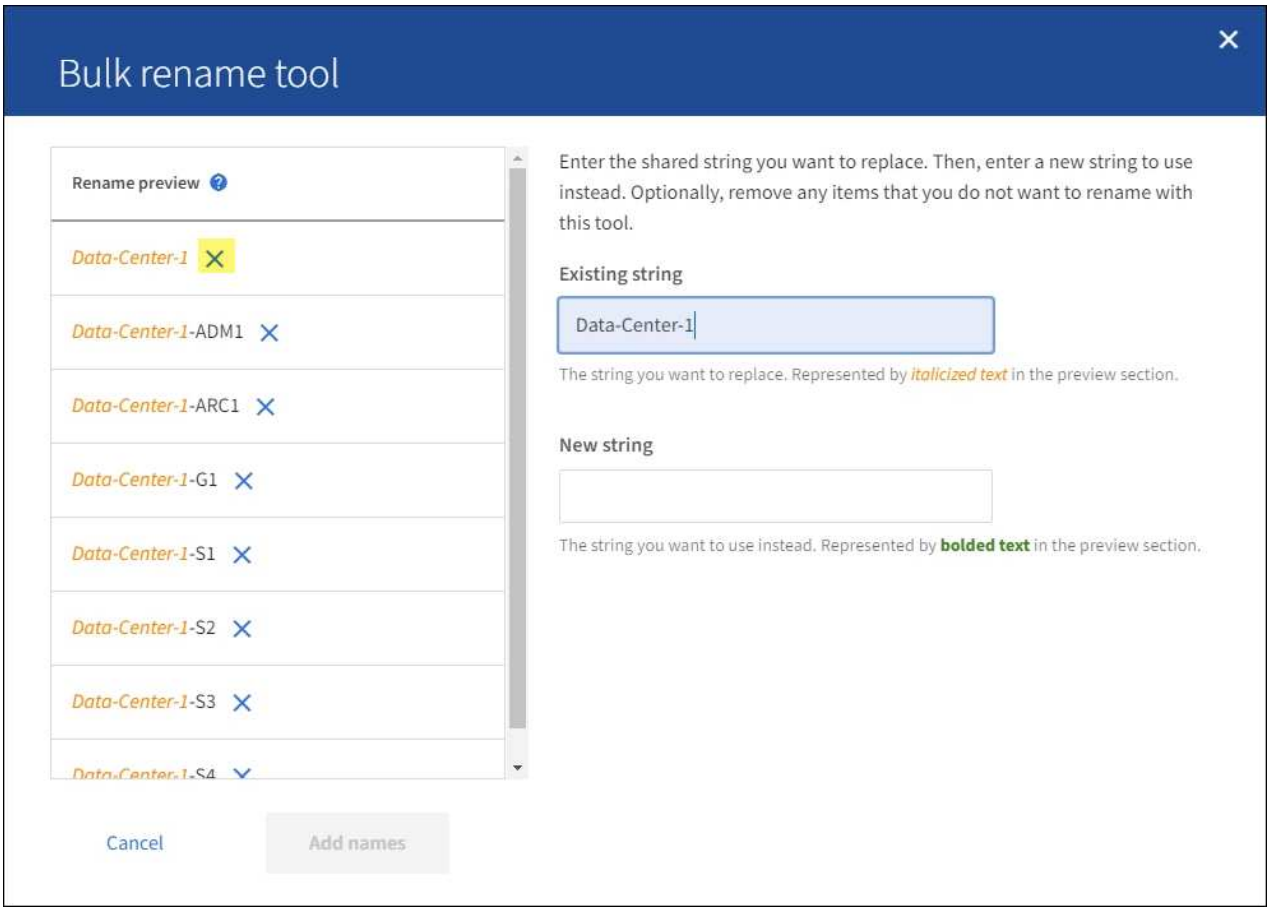
   Die **Umbenennungsvorschau** umfasst alle Elemente, die für den Schritt **Neue Namen vorschlagen** angezeigt wurden. Sie können die Vorschau verwenden, um zu sehen, wie Anzeigenamen aussehen, nachdem Sie eine freigegebene Zeichenfolge ersetzt haben.

2. Geben Sie im Feld **Vorhandene Zeichenfolge** die freigegebene Zeichenfolge ein, die Sie ersetzen möchten. Wenn die Zeichenfolge, die Sie ersetzen möchten, beispielsweise `Data-Center-1` , geben Sie **Data-Center-1** ein.

   Während der Eingabe wird Ihr Text überall dort hervorgehoben, wo er in den Namen auf der linken Seite vorkommt.

3. Wählen ✕ um alle Elemente zu entfernen, die Sie mit diesem Tool nicht umbenennen möchten.

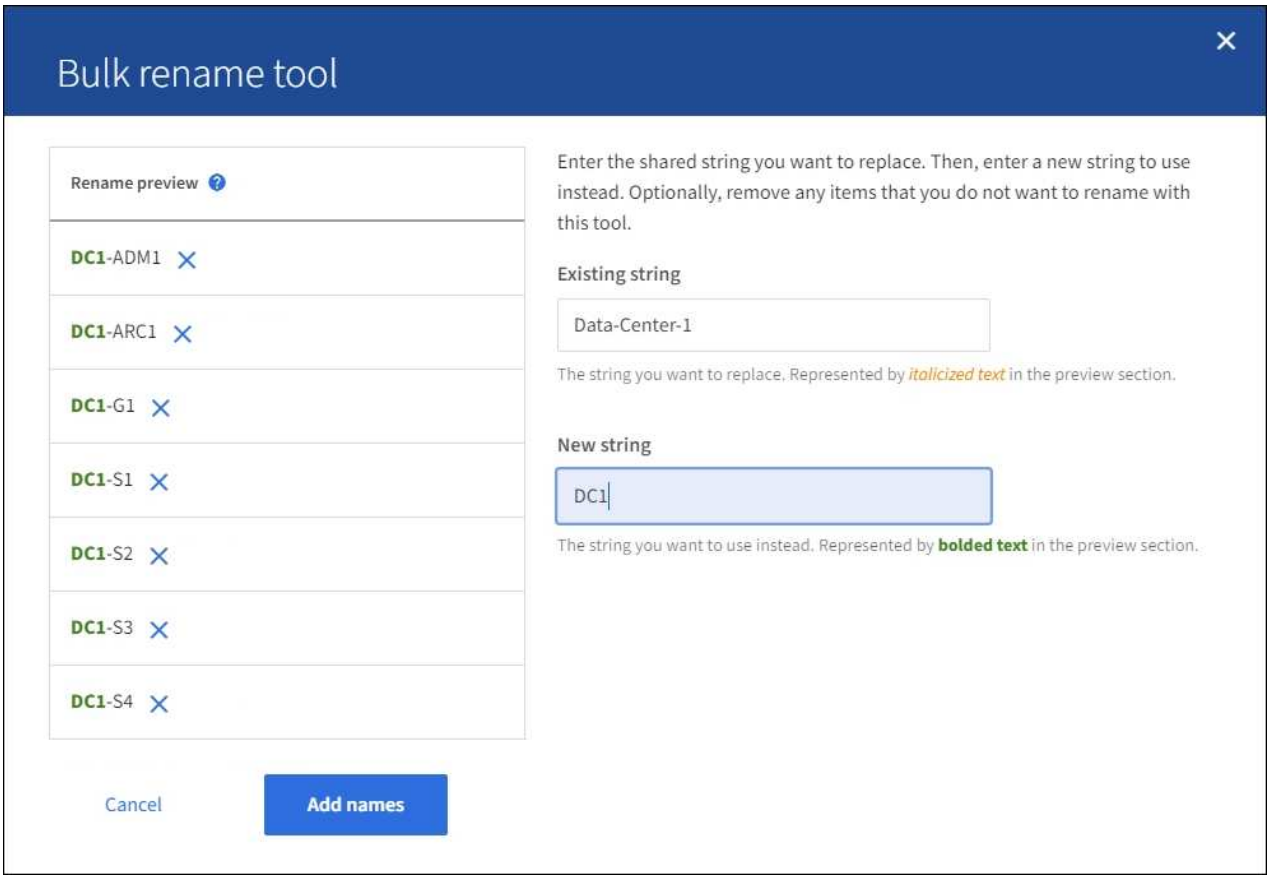
   Angenommen, Sie möchten alle Knoten umbenennen, die die Zeichenfolge enthalten `Data-Center-1` , aber Sie möchten die `Data-Center-1` Website selbst. Wählen ✕ um die Site aus der Umbenennungsvorschau zu entfernen.



4. Geben Sie im Feld **Neue Zeichenfolge** die Ersatzzeichenfolge ein, die Sie stattdessen verwenden möchten. Geben Sie beispielsweise **DC1** ein.

   Sehen"Raster, Sites und Knoten umbenennen" um die Namensanforderungen zu erfahren.

   Während Sie die Ersetzungszeichenfolge eingeben, werden die Namen auf der linken Seite aktualisiert, sodass Sie überprüfen können, ob die neuen Namen richtig sind.



5. Wenn Sie mit den in der Vorschau angezeigten Namen zufrieden sind, wählen Sie **Namen hinzufügen**, um die Namen für den Schritt **Neue Namen vorschlagen** zur Tabelle hinzuzufügen.
6. Nehmen Sie alle erforderlichen weiteren Änderungen vor oder wählen Sie ✕, um alle Elemente zu entfernen, die Sie nicht umbenennen möchten.
7. Wenn Sie bereit sind, alle Elemente in der Tabelle umzubenennen, wählen Sie **Umbenennen**.

   Es wird eine Erfolgsmeldung angezeigt. Die neuen Anzeigenamen werden jetzt im gesamten Grid Manager verwendet.

Laden Sie das Wiederherstellungspaket herunter

Wenn Sie mit dem Umbenennen der Elemente fertig sind, laden Sie ein neues Wiederherstellungspaket herunter und speichern Sie es. Die neuen Anzeigenamen für die umbenannten Elemente sind in der `Passwords.txt` Datei.

Schritte

1. Geben Sie die Bereitstellungspassphrase ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.

   Der Download beginnt sofort.

3. Wenn der Download abgeschlossen ist, öffnen Sie die `Passwords.txt` Datei, um den Servernamen für alle Knoten und die Anzeigenamen für alle umbenannten Knoten anzuzeigen.
4. Kopieren Sie die `sgws-recovery-package-id-revision.zip` Datei 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.

5. Wählen Sie **Fertig**, um zum ersten Schritt zurückzukehren.

Anzeigenamen wieder auf Systemnamen zurücksetzen

Sie können ein umbenanntes Raster, eine Site oder einen Knoten wieder auf seinen ursprünglichen Systemnamen zurücksetzen. Wenn Sie ein Element wieder auf seinen Systemnamen zurücksetzen, wird auf den Grid Manager-Seiten und anderen StorageGRID Standorten kein **Anzeigename** mehr für dieses Element angezeigt. Es wird nur der Systemname des Artikels angezeigt.

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Raster, Sites und Knoten umbenennen**.
2. Wählen Sie im Schritt **Namen auswählen** alle Elemente aus, die Sie wieder auf Systemnamen zurücksetzen möchten.
3. Wählen Sie **Weiter**.
4. Setzen Sie im Schritt **Neue Namen vorschlagen** die Anzeigenamen einzeln oder in großen Mengen wieder auf Systemnamen zurück.

Einzelne Systemnamen wiederherstellen

a. Kopieren Sie den ursprünglichen Systemnamen jedes Elements und fügen Sie ihn in das Feld **Anzeigename** ein, oder wählen Sie ✕ um alle Elemente zu entfernen, die Sie nicht wiederherstellen möchten.

   Um einen Anzeigenamen zurückzusetzen, muss der Systemname im Feld **Anzeigename** erscheinen, die Groß-/Kleinschreibung wird jedoch nicht berücksichtigt.

b. Wählen Sie **Umbenennen**.

   Es erscheint eine Erfolgsmeldung. Die Anzeigenamen für diese Elemente werden nicht mehr verwendet.

Massenweises Zurücksetzen auf Systemnamen

a. Wählen Sie für den Schritt **Neue Namen vorschlagen** die Option **Tool zur Massenumbenennung verwenden**.

b. Geben Sie im Feld **Vorhandene Zeichenfolge** die Zeichenfolge des Anzeigenamens ein, die Sie ersetzen möchten.

c. Geben Sie im Feld **Neue Zeichenfolge** die Systemnamenzeichenfolge ein, die Sie stattdessen verwenden möchten.

d. Wählen Sie **Namen hinzufügen**, um die Namen für den Schritt **Neue Namen vorschlagen** zur Tabelle hinzuzufügen.

e. Vergewissern Sie sich, dass jeder Eintrag im Feld **Anzeigename** mit dem Namen im Feld **Systemname** übereinstimmt. Nehmen Sie Änderungen vor oder wählen Sie ✕ um alle Elemente zu entfernen, die Sie nicht wiederherstellen möchten.

   Um einen Anzeigenamen zurückzusetzen, muss der Systemname im Feld **Anzeigename** erscheinen, die Groß-/Kleinschreibung wird jedoch nicht berücksichtigt.

f. Wählen Sie **Umbenennen**.

   Es wird eine Erfolgsmeldung angezeigt. Die Anzeigenamen für diese Elemente werden nicht mehr verwendet.

5. Laden Sie ein neues Wiederherstellungspaket herunter und speichern Sie es .

   Anzeigenamen für die Elemente, die Sie zurückgesetzt haben, sind nicht mehr in der `Passwords.txt` Datei.

Knotenprozeduren

Knotenwartungsverfahren

Möglicherweise müssen Sie Wartungsverfahren im Zusammenhang mit bestimmten Grid-Knoten oder Knotendiensten durchführen.

Server Manager-Verfahren

Der Server Manager wird auf jedem Grid-Knoten ausgeführt, um das Starten und Stoppen von Diensten zu überwachen und sicherzustellen, dass die Dienste dem StorageGRID -System ordnungsgemäß beitreten und es verlassen. Server Manager überwacht außerdem die Dienste auf jedem Grid-Knoten und versucht automatisch, alle Dienste neu zu starten, die Fehler melden.

Um Server Manager-Verfahren auszuführen, müssen Sie normalerweise auf die Befehlszeile des Knotens zugreifen.

> Sie sollten nur auf den Server Manager zugreifen, wenn Sie vom technischen Support dazu aufgefordert wurden.

> Sie müssen die aktuelle Befehlsshell-Sitzung schließen und sich abmelden, nachdem Sie mit Server Manager fertig sind. Eingeben: `exit`

Neustart-, Herunterfahr- und Einschaltvorgänge für Knoten

Mit diesen Verfahren können Sie einen oder mehrere Knoten neu starten, Knoten herunterfahren und neu starten oder Knoten aus- und wieder einschalten.

Port-Neuzuordnungsverfahren

Sie können die Port-Neuzuordnungsverfahren verwenden, um die Port-Neuzuordnungen von einem Knoten zu entfernen, beispielsweise, wenn Sie einen Load Balancer-Endpunkt mit einem zuvor neu zugeordneten Port konfigurieren möchten.

Server Manager-Verfahren

Anzeigen des Status und der Version des Server-Managers

Für jeden Grid-Knoten können Sie den aktuellen Status und die Version des Server Managers anzeigen, der auf diesem Grid-Knoten ausgeführt wird. Sie können auch den aktuellen Status aller auf diesem Grid-Knoten ausgeführten Dienste abrufen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Zeigen Sie den aktuellen Status des Server Managers an, der auf dem Grid-Knoten ausgeführt wird:
   `service servermanager status`

   Der aktuelle Status des auf dem Grid-Knoten ausgeführten Server Managers wird gemeldet (läuft oder

nicht). Wenn der Status des Server Managers `running` wird die Laufzeit seit dem letzten Start aufgelistet. Beispiel:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Zeigen Sie die aktuelle Version von Server Manager an, die auf einem Grid-Knoten ausgeführt wird: **`service servermanager version`**

   Die aktuelle Version wird aufgelistet. Beispiel:

```
11.1.0-20180425.1905.39c9493
```

4. Melden Sie sich von der Befehlsshell ab: **`exit`**

Aktuellen Status aller Dienste anzeigen

Sie können jederzeit den aktuellen Status aller auf einem Grid-Knoten laufenden Dienste einsehen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`grid_node_IP`*

   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

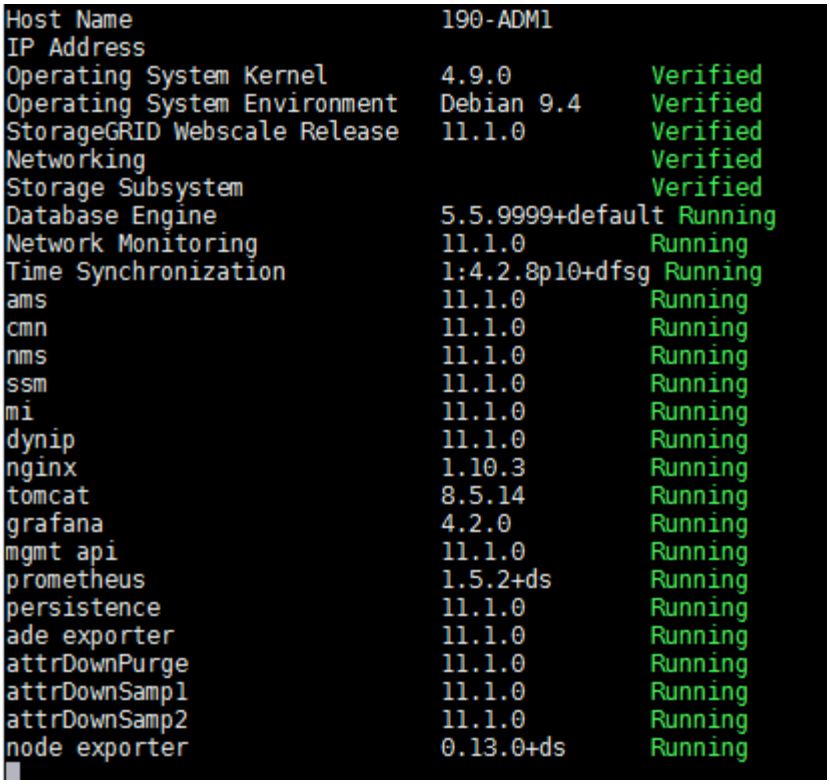
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

   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. Zeigen Sie den Status aller auf dem Grid-Knoten ausgeführten Dienste an: `storagegrid-status`

   Beispielsweise zeigt die Ausgabe für den primären Admin-Knoten den aktuellen Status der AMS-, CMN- und NMS-Dienste als „Ausgeführt“ an. Diese Ausgabe wird sofort aktualisiert, wenn sich der Status eines Dienstes ändert.



3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Optional können Sie einen statischen Bericht für alle auf dem Grid-Knoten ausgeführten Dienste anzeigen: `/usr/local/servermanager/reader.rb`

   Dieser Bericht enthält dieselben Informationen wie der kontinuierlich aktualisierte Bericht, wird jedoch nicht aktualisiert, wenn sich der Status eines Dienstes ändert.

5. Melden Sie sich von der Befehlsshell ab: `exit`

Starten Sie den Server-Manager und alle Dienste

Möglicherweise müssen Sie den Server Manager starten, der auch alle Dienste auf dem Grid-Knoten startet.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Das Starten von Server Manager auf einem Grid-Knoten, auf dem er bereits ausgeführt wird, führt zu einem Neustart von Server Manager und allen Diensten auf dem Grid-Knoten.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`grid_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. Starten Sie den Server-Manager: `service servermanager start`
3. Melden Sie sich von der Befehlsshell ab: `exit`

Starten Sie den Server-Manager und alle Dienste neu

Möglicherweise müssen Sie den Server-Manager und alle auf einem Grid-Knoten ausgeführten Dienste neu starten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Starten Sie Server Manager und alle Dienste auf dem Grid-Knoten neu: `service servermanager restart`

   Server Manager und alle Dienste auf dem Grid-Knoten werden gestoppt und anschließend neu gestartet.

   > Verwenden des `restart` Der Befehl ist dasselbe wie die Verwendung des `stop` Befehl gefolgt von `start` Befehl.
3. Melden Sie sich von der Befehlsshell ab: `exit`

Stoppen Sie den Server Manager und alle Dienste

Server Manager soll ständig ausgeführt werden, Sie müssen jedoch möglicherweise Server Manager und alle auf einem Grid-Knoten ausgeführten Dienste beenden.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Stoppen Sie den Server-Manager und alle auf dem Grid-Knoten laufenden Dienste: `service servermanager stop`

   Server Manager und alle auf dem Grid-Knoten ausgeführten Dienste werden ordnungsgemäß beendet. Das Herunterfahren der Dienste kann bis zu 15 Minuten dauern.

3. Melden Sie sich von der Befehlsshell ab: `exit`

Aktuellen Servicestatus anzeigen

Sie können den aktuellen Status eines auf einem Grid-Knoten ausgeführten Dienstes jederzeit anzeigen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Zeigen Sie den aktuellen Status eines auf einem Grid-Knoten ausgeführten Dienstes an: `**service *servicename* status** Der aktuelle Status des angeforderten Dienstes, der auf dem Grid-Knoten ausgeführt wird, wird gemeldet (läuft oder nicht). Beispiel:

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. Melden Sie sich von der Befehlsshell ab: **`exit`**

Dienst beenden

Bei einigen Wartungsvorgängen müssen Sie einen einzelnen Dienst stoppen, während andere Dienste auf dem Grid-Knoten weiterlaufen. Beenden Sie einzelne Dienste nur, wenn Sie durch eine Wartungsprozedur dazu aufgefordert werden.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Wenn Sie diese Schritte verwenden, um einen Dienst „administrativ zu stoppen“, startet Server Manager den Dienst nicht automatisch neu. Sie müssen entweder den einzelnen Dienst manuell starten oder den Server Manager neu starten.

Wenn Sie den LDR-Dienst auf einem Speicherknoten stoppen müssen, beachten Sie, dass das Stoppen des Dienstes eine Weile dauern kann, wenn aktive Verbindungen bestehen.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Beenden Sie einen einzelnen Dienst: `service servicename stop`

   Beispiel:

   ```
   service ldr stop
   ```

   Es kann bis zu 11 Minuten dauern, bis die Dienste anhalten.

3. Melden Sie sich von der Befehlsshell ab: `exit`

Ähnliche Informationen

"Beenden des Dienstes erzwingen"

Beenden des Dienstes erzwingen

Wenn Sie einen Dienst sofort beenden müssen, können Sie die `force-stop` Befehl.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Erzwingen Sie manuell die Beendigung des Dienstes: `service servicename force-stop`

   Beispiel:

   ```
   service ldr force-stop
   ```

   Das System wartet 30 Sekunden, bevor der Dienst beendet wird.

3. Melden Sie sich von der Befehlsshell ab: `exit`

Dienst starten oder neu starten

Möglicherweise müssen Sie einen Dienst starten, der gestoppt wurde, oder Sie müssen einen Dienst stoppen und neu starten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Entscheiden Sie, welcher Befehl ausgegeben werden soll, je nachdem, ob der Dienst derzeit ausgeführt wird oder gestoppt ist.

   - Wenn der Dienst derzeit gestoppt ist, verwenden Sie die `start` Befehl zum manuellen Starten des Dienstes: `service servicename start`

     Beispiel:

     ```
     service ldr start
     ```

   - Wenn der Dienst derzeit ausgeführt wird, verwenden Sie die `restart` Befehl zum Stoppen und Neustarten des Dienstes: `service servicename restart`

     Beispiel:

```
service ldr restart
```

+

Verwenden des `restart` Der Befehl ist dasselbe wie die Verwendung des `stop` Befehl gefolgt von `start` Befehl. Sie können `restart` auch wenn der Dienst derzeit gestoppt ist.

3. Melden Sie sich von der Befehlsshell ab: `exit`

Verwenden Sie eine DoNotStart-Datei

Wenn Sie unter Anleitung des technischen Supports verschiedene Wartungs- oder Konfigurationsverfahren durchführen, werden Sie möglicherweise aufgefordert, eine DoNotStart-Datei zu verwenden, um zu verhindern, dass Dienste gestartet werden, wenn Server Manager gestartet oder neu gestartet wird.

Sie sollten eine DoNotStart-Datei nur hinzufügen oder entfernen, wenn Sie vom technischen Support dazu aufgefordert werden.

Um den Start eines Dienstes zu verhindern, platzieren Sie eine DoNotStart-Datei im Verzeichnis des Dienstes, dessen Start Sie verhindern möchten. Beim Start sucht der Server Manager nach der DoNotStart-Datei. Wenn die Datei vorhanden ist, wird der Start des Dienstes (und aller davon abhängigen Dienste) verhindert. Wenn die DoNotStart-Datei entfernt wird, wird der zuvor gestoppte Dienst beim nächsten Start oder Neustart von Server Manager gestartet. Dienste werden nicht automatisch gestartet, wenn die DoNotStart-Datei entfernt wird.

Der effizienteste Weg, den Neustart aller Dienste zu verhindern, besteht darin, den Start des NTP-Dienstes zu verhindern. Alle Dienste sind vom NTP-Dienst abhängig und können nicht ausgeführt werden, wenn der NTP-Dienst nicht ausgeführt wird.

DoNotStart-Datei für den Dienst hinzufügen

Sie können den Start eines einzelnen Dienstes verhindern, indem Sie dem Verzeichnis dieses Dienstes auf einem Grid-Knoten eine DoNotStart-Datei hinzufügen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Fügen Sie eine DoNotStart-Datei hinzu: `touch /etc/sv/service/DoNotStart`

   Wo `service` ist der Name des Dienstes, dessen Start verhindert werden soll. Zum Beispiel,

```
touch /etc/sv/ldr/DoNotStart
```

Es wird eine DoNotStart-Datei erstellt. Es wird kein Dateiinhalt benötigt.

Wenn Server Manager oder der Grid-Knoten neu gestartet wird, wird Server Manager neu gestartet, der Dienst jedoch nicht.

3. Melden Sie sich von der Befehlsshell ab: `exit`

DoNotStart-Datei für den Dienst entfernen

Wenn Sie eine DoNotStart-Datei entfernen, die den Start eines Dienstes verhindert, müssen Sie diesen Dienst starten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Entfernen Sie die DoNotStart-Datei aus dem Serviceverzeichnis: `rm /etc/sv/service/DoNotStart`

   Wo `service` ist der Name des Dienstes. Zum Beispiel,

   ```
   rm /etc/sv/ldr/DoNotStart
   ```
3. Starten Sie den Dienst: `service servicename start`
4. Melden Sie sich von der Befehlsshell ab: `exit`

Fehlerbehebung beim Server-Manager

Wenn bei der Verwendung des Server Managers ein Problem auftritt, überprüfen Sie die Protokolldatei.

Fehlermeldungen im Zusammenhang mit Server Manager werden in der Server Manager-Protokolldatei erfasst, die sich hier befindet: `/var/local/log/servermanager.log`

Überprüfen Sie diese Datei auf Fehlermeldungen zu Fehlern. Leiten Sie das Problem bei Bedarf an den technischen Support weiter. Möglicherweise werden Sie aufgefordert, Protokolldateien an den technischen Support weiterzuleiten.

Dienst mit einem Fehlerzustand

Wenn Sie feststellen, dass ein Dienst in einen Fehlerzustand geraten ist, versuchen Sie, den Dienst neu zu starten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Server Manager überwacht Dienste und startet alle Dienste neu, die unerwartet beendet wurden. Wenn ein Dienst ausfällt, versucht Server Manager, ihn neu zu starten. Wenn innerhalb von fünf Minuten drei Versuche zum Starten eines Dienstes fehlschlagen, wechselt der Dienst in einen Fehlerzustand. Der Server-Manager versucht keinen weiteren Neustart.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Bestätigen Sie den Fehlerstatus des Dienstes: `service servicename status`

   Beispiel:

   ```
   service ldr status
   ```

   Wenn sich der Dienst in einem Fehlerzustand befindet, wird die folgende Meldung zurückgegeben: *`servicename`* `in error state` . Beispiel:

   ```
   ldr in error state
   ```

   > ⓘ Wenn der Dienststatus `disabled` , siehe die Anweisungen für"Entfernen einer DoNotStart-Datei für einen Dienst" .

3. Versuchen Sie, den Fehlerzustand durch einen Neustart des Dienstes zu beheben: `service` *`servicename`* `restart`

   Wenn der Dienst nicht neu gestartet werden kann, wenden Sie sich an den technischen Support.

4. Melden Sie sich von der Befehlsshell ab: `exit`

Neustart-, Herunterfahr- und Einschaltvorgänge

Führen Sie einen Rolling Reboot durch

Sie können einen Rolling Reboot durchführen, um mehrere Grid-Knoten neu zu starten, ohne eine Dienstunterbrechung zu verursachen.

Bevor Sie beginnen

- Sie sind beim Grid Manager auf dem primären Admin-Knoten angemeldet und verwenden einen"unterstützter Webbrowser" .

> Sie müssen beim primären Admin-Knoten angemeldet sein, um dieses Verfahren durchzuführen.

- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Verwenden Sie dieses Verfahren, wenn Sie mehrere Knoten gleichzeitig neu starten müssen. Sie können dieses Verfahren beispielsweise verwenden, nachdem Sie den FIPS-Modus für das Grid geändert haben."TLS- und SSH-Sicherheitsrichtlinie" . Wenn sich der FIPS-Modus ändert, müssen Sie alle Knoten neu starten, damit die Änderung wirksam wird.

> Wenn Sie nur einen Knoten neu starten müssen, können Sie"Starten Sie den Knoten über die Registerkarte „Aufgaben“ neu." .

Wenn StorageGRID Grid-Knoten neu startet, gibt es die `reboot` Befehl auf jedem Knoten, der dazu führt, dass der Knoten heruntergefahren und neu gestartet wird. Alle Dienste werden automatisch neu gestartet.

- Durch den Neustart eines VMware-Knotens wird die virtuelle Maschine neu gestartet.
- Durch den Neustart eines Linux-Knotens wird der Container neu gestartet.
- Durch den Neustart eines StorageGRID Appliance-Knotens wird der Compute-Controller neu gestartet.

Mit dem Rolling-Reboot-Verfahren können mehrere Knoten gleichzeitig neu gestartet werden, mit folgenden Ausnahmen:

- Zwei Knoten desselben Typs werden nicht gleichzeitig neu gestartet.
- Gateway-Knoten und Admin-Knoten werden nicht gleichzeitig neu gestartet.

Stattdessen werden diese Knoten nacheinander neu gestartet, um sicherzustellen, dass HA-Gruppen, Objektdaten und kritische Knotendienste immer verfügbar bleiben.

Wenn Sie den primären Admin-Knoten neu starten, verliert Ihr Browser vorübergehend den Zugriff auf den Grid Manager, sodass Sie den Vorgang nicht mehr überwachen können. Aus diesem Grund wird der primäre Admin-Knoten zuletzt neu gestartet.

Führen Sie einen Rolling Reboot durch

Sie wählen die Knoten aus, die Sie neu starten möchten, überprüfen Ihre Auswahl, starten den Neustartvorgang und überwachen den Fortschritt.

Knoten auswählen

Rufen Sie als ersten Schritt die Seite „Rolling Reboot“ auf und wählen Sie die Knoten aus, die Sie neu starten möchten.

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Rollierender Neustart**.
2. Überprüfen Sie den Verbindungsstatus und die Warnsymbole in der Spalte **Knotenname**.

   Sie können einen Knoten nicht neu starten, wenn er vom Netz getrennt ist. Die Kontrollkästchen sind für Knoten mit diesen Symbolen deaktiviert: oder .

3. Wenn für Knoten aktive Warnungen vorliegen, überprüfen Sie die Liste der Warnungen in der Spalte **Warnungszusammenfassung**.

   Um alle aktuellen Warnungen für einen Knoten anzuzeigen, können Sie auch die**Knoten › Registerkarte „Übersicht“** .

4. Führen Sie optional die empfohlenen Aktionen aus, um alle aktuellen Warnungen zu beheben.
5. Wenn alle Knoten verbunden sind und Sie alle neu starten möchten, aktivieren Sie optional das Kontrollkästchen in der Tabellenüberschrift und wählen Sie **Alle auswählen**. Andernfalls wählen Sie jeden Knoten aus, den Sie neu starten möchten.

   Sie können die Filteroptionen der Tabelle verwenden, um Teilmengen von Knoten anzuzeigen. Sie können beispielsweise nur Speicherknoten oder alle Knoten an einem bestimmten Standort anzeigen und auswählen.

6. Wählen Sie **Auswahl überprüfen**.

Auswahl überprüfen

In diesem Schritt können Sie bestimmen, wie lange der gesamte Neustartvorgang dauern könnte, und bestätigen, dass Sie die richtigen Knoten ausgewählt haben.

1. Überprüfen Sie auf der Seite „Auswahl überprüfen“ die Zusammenfassung. Darin wird angegeben, wie viele Knoten neu gestartet werden und wie lange der Neustart aller Knoten voraussichtlich insgesamt dauern wird.
2. Um optional einen bestimmten Knoten aus der Neustartliste zu entfernen, wählen Sie **Entfernen**.
3. Um optional weitere Knoten hinzuzufügen, wählen Sie **Vorheriger Schritt**, wählen Sie die zusätzlichen Knoten aus und wählen Sie **Auswahl überprüfen**.
4. Wenn Sie bereit sind, den Rolling-Reboot-Vorgang für alle ausgewählten Knoten zu starten, wählen Sie **Knoten neu starten**.
5. Wenn Sie den Neustart des primären Admin-Knotens ausgewählt haben, lesen Sie die Informationsmeldung und wählen Sie **Ja**.

   Der primäre Admin-Knoten ist der letzte Knoten, der neu gestartet wird. Während dieser Knoten neu gestartet wird, geht die Verbindung Ihres Browsers verloren. Wenn der primäre Admin-Knoten wieder verfügbar ist, müssen Sie die Seite „Rolling Reboot“ neu laden.

Überwachen eines rollierenden Neustarts

Während der Rolling-Reboot-Vorgang ausgeführt wird, können Sie ihn vom primären Admin-Knoten aus überwachen.

Schritte

1. Überprüfen Sie den Gesamtfortschritt des Vorgangs, der die folgenden Informationen enthält:
   - Anzahl der neu gestarteten Knoten
   - Anzahl der Knoten, die gerade neu gestartet werden
   - Anzahl der Knoten, die noch neu gestartet werden müssen
2. Überprüfen Sie die Tabelle für jeden Knotentyp.

   Die Tabellen bieten einen Fortschrittsbalken für den Vorgang auf jedem Knoten und zeigen die Neustartphase für diesen Knoten an. Dabei kann es sich um eine der folgenden handeln:

   - Warten auf den Neustart
   - Dienste beenden
   - System neu starten
   - Starten von Diensten
   - Neustart abgeschlossen

Stoppen Sie den Rolling Reboot-Vorgang

Sie können den Rolling-Reboot-Vorgang vom primären Admin-Knoten aus stoppen. Wenn Sie den Vorgang beenden, wird der Neustartvorgang für alle Knoten mit dem Status „Dienste werden gestoppt“, „System wird neu gestartet“ oder „Dienste werden gestartet“ abgeschlossen. Diese Knoten werden im Rahmen des Verfahrens jedoch nicht mehr verfolgt.

Schritte

1. Wählen Sie **WARTUNG** > **Aufgaben** > **Rollierender Neustart**.
2. Wählen Sie im Schritt **Neustart überwachen** die Option **Neustartvorgang stoppen**.

Starten Sie den Grid-Knoten über die Registerkarte „Aufgaben“ neu.

Sie können einen einzelnen Grid-Knoten über die Registerkarte „Aufgaben“ auf der Seite „Knoten“ neu starten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben die Bereitstellungspassphrase.
- Wenn Sie den primären Admin-Knoten oder einen beliebigen Speicherknoten neu starten, haben Sie die folgenden Überlegungen überprüft:
  - Wenn Sie den primären Admin-Knoten neu starten, verliert Ihr Browser vorübergehend den Zugriff auf den Grid Manager.
  - Wenn Sie zwei oder mehr Speicherknoten an einem bestimmten Standort neu starten, können Sie für die Dauer des Neustarts möglicherweise nicht auf bestimmte Objekte zugreifen. Dieses Problem kann

auftreten, wenn eine ILM-Regel die Aufnahmeoption **Dual Commit** verwendet (oder eine Regel **Balanced** angibt und es nicht möglich ist, alle erforderlichen Kopien sofort zu erstellen). In diesem Fall übergibt StorageGRID neu aufgenommene Objekte an zwei Speicherknoten am selben Standort und wertet ILM später aus.

- Um sicherzustellen, dass Sie während des Neustarts eines Speicherknotens auf alle Objekte zugreifen können, unterbrechen Sie die Aufnahme von Objekten an einem Standort etwa eine Stunde lang, bevor Sie den Knoten neu starten.

Informationen zu diesem Vorgang

Wenn StorageGRID einen Grid-Knoten neu startet, gibt es die `reboot` Befehl auf dem Knoten, der dazu führt, dass der Knoten heruntergefahren und neu gestartet wird. Alle Dienste werden automatisch neu gestartet.

- Durch den Neustart eines VMware-Knotens wird die virtuelle Maschine neu gestartet.
- Durch den Neustart eines Linux-Knotens wird der Container neu gestartet.
- Durch den Neustart eines StorageGRID Appliance-Knotens wird der Compute-Controller neu gestartet.

Wenn Sie mehr als einen Knoten neu starten müssen, können Sie die"Rolling-Reboot-Verfahren" .

Schritte

1. Wählen Sie **NODES**.
2. Wählen Sie den Grid-Knoten aus, den Sie neu starten möchten.
3. Wählen Sie die Registerkarte **Aufgaben**.
4. Wählen Sie **Neustart**.

   Ein Bestätigungsdialogfeld wird angezeigt. Wenn Sie den primären Admin-Knoten neu starten, werden Sie im Bestätigungsdialogfeld daran erinnert, dass die Verbindung Ihres Browsers zum Grid Manager vorübergehend verloren geht, wenn die Dienste gestoppt werden.

5. Geben Sie die Bereitstellungspassphrase ein und wählen Sie **OK**.
6. Warten Sie, bis der Knoten neu gestartet wurde.

   Es kann einige Zeit dauern, bis die Dienste heruntergefahren werden.

   Beim Neustart des Knotens wird auf der Seite „Knoten“ das graue Symbol (Administrativ ausgefallen) für den Knoten angezeigt. Wenn alle Dienste erneut gestartet wurden und der Knoten erfolgreich mit dem Grid verbunden ist, sollte auf der Seite „Knoten“ der normale Status angezeigt werden (keine Symbole links neben dem Knotennamen). Dies bedeutet, dass keine Warnungen aktiv sind und der Knoten mit dem Grid verbunden ist.

Starten Sie den Grid-Knoten über die Befehlsshell neu

Wenn Sie den Neustartvorgang genauer überwachen müssen oder nicht auf den Grid Manager zugreifen können, können Sie sich beim Grid-Knoten anmelden und den Neustartbefehl des Server Managers über die Befehlsshell ausführen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Optional können Sie Dienste beenden: `service servermanager stop`

   Das Beenden von Diensten ist ein optionaler, aber empfohlener Schritt. Das Herunterfahren von Diensten kann bis zu 15 Minuten dauern. Sie sollten sich möglicherweise per Fernzugriff beim System anmelden, um den Herunterfahrvorgang zu überwachen, bevor Sie den Knoten im nächsten Schritt neu starten.

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

4. Melden Sie sich von der Befehlsshell ab: `exit`

Grid-Knoten herunterfahren

Sie können einen Grid-Knoten über die Befehlsshell des Knotens herunterfahren.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Bevor Sie dieses Verfahren durchführen, sollten Sie die folgenden Überlegungen berücksichtigen:

- Generell sollten Sie nicht mehr als einen Knoten gleichzeitig herunterfahren, um Störungen zu vermeiden.
- Fahren Sie einen Knoten während eines Wartungsvorgangs nicht herunter, es sei denn, Sie werden in der Dokumentation oder vom technischen Support ausdrücklich dazu aufgefordert.
- Der Herunterfahrvorgang hängt davon ab, wo der Knoten installiert ist, und zwar wie folgt:
  - Durch das Herunterfahren eines VMware-Knotens wird die virtuelle Maschine heruntergefahren.
  - Durch das Herunterfahren eines Linux-Knotens wird der Container heruntergefahren.
  - Durch das Herunterfahren eines StorageGRID Appliance-Knotens wird der Compute-Controller heruntergefahren.
- Wenn Sie vorhaben, mehr als einen Speicherknoten an einem Standort herunterzufahren, stoppen Sie die Aufnahme von Objekten an diesem Standort etwa eine Stunde lang, bevor Sie die Knoten herunterfahren.

  Wenn eine ILM-Regel die Aufnahmeoption **Dual Commit** verwendet (oder wenn eine Regel die Option **Balanced** verwendet und nicht alle erforderlichen Kopien sofort erstellt werden können), übergibt StorageGRID alle neu aufgenommenen Objekte sofort an zwei Speicherknoten am selben Standort und wertet ILM später aus. Wenn mehr als ein Speicherknoten an einem Standort heruntergefahren wird, können Sie für die Dauer der Herunterfahrt möglicherweise nicht auf neu aufgenommene Objekte zugreifen. Schreibvorgänge können auch fehlschlagen, wenn am Standort zu wenige Speicherknoten verfügbar sind. Sehen "Objekte mit ILM verwalten" .

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Stoppen Sie alle Dienste: `service servermanager stop`

   Das Herunterfahren von Diensten kann bis zu 15 Minuten dauern. Sie möchten sich möglicherweise per Fernzugriff beim System anmelden, um den Herunterfahrvorgang zu überwachen.

3. Wenn der Knoten auf einer virtuellen VMware-Maschine ausgeführt wird oder es sich um einen Appliance-Knoten handelt, geben Sie den Befehl zum Herunterfahren ein: `shutdown -h now`

   Führen Sie diesen Schritt unabhängig vom Ergebnis der `service servermanager stop` Befehl.

   > Nachdem Sie die `shutdown -h now` Befehl auf einem Appliance-Knoten ausführen, müssen Sie die Appliance aus- und wieder einschalten, um den Knoten neu zu starten.

   Für das Gerät fährt dieser Befehl den Controller herunter, das Gerät bleibt jedoch eingeschaltet. Sie müssen den nächsten Schritt abschließen.

4. Wenn Sie einen Appliance-Knoten herunterfahren, befolgen Sie die Schritte für Ihre Appliance.

SG6160

a. Schalten Sie die Stromversorgung des SG6100-CN-Speichercontrollers aus.
b. Warten Sie, bis die blaue Betriebs-LED am SG6100-CN-Speichercontroller erlischt.

SGF6112

a. Schalten Sie die Stromversorgung des Geräts aus.
b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG6000

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite der Speichercontroller erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Schalten Sie das Gerät aus und warten Sie, bis die blaue Betriebs-LED erlischt.

SG5800

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite des Speichercontrollers erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Wählen Sie auf der Startseite des SANtricity System Managers **Laufende Vorgänge anzeigen** aus.
c. Bestätigen Sie, dass alle Vorgänge abgeschlossen sind, bevor Sie mit dem nächsten Schritt fortfahren.
d. Schalten Sie beide Netzschalter am Controller-Regal aus und warten Sie, bis alle LEDs am Controller-Regal erloschen sind.

SG5700

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite des Speichercontrollers erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und Siebensegmentanzeigen nicht mehr aktiv sind.

SG100 oder SG1000

a. Schalten Sie die Stromversorgung des Geräts aus.
b. Warten Sie, bis die blaue Betriebs-LED erlischt.

Host herunterfahren

Bevor Sie einen Host herunterfahren, müssen Sie die Dienste auf allen Grid-Knoten auf diesem Host stoppen.

Schritte

1. Melden Sie sich beim Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Stoppen Sie alle auf dem Knoten laufenden Dienste: `service servermanager stop`

   Das Herunterfahren von Diensten kann bis zu 15 Minuten dauern. Sie möchten sich möglicherweise per Fernzugriff beim System anmelden, um den Herunterfahrvorgang zu überwachen.

3. Wiederholen Sie die Schritte 1 und 2 für jeden Knoten auf dem Host.
4. Wenn Sie einen Linux-Host haben:

   a. Melden Sie sich beim Host-Betriebssystem an.

   b. Stoppen Sie den Knoten: `storagegrid node stop`

   c. Fahren Sie das Host-Betriebssystem herunter.

5. Wenn der Knoten auf einer virtuellen VMware-Maschine ausgeführt wird oder es sich um einen Appliance-Knoten handelt, geben Sie den Befehl zum Herunterfahren ein: `shutdown -h now`

   Führen Sie diesen Schritt unabhängig vom Ergebnis der `service servermanager stop` Befehl.

   > ⓘ Nachdem Sie die `shutdown -h now` Befehl auf einem Appliance-Knoten ausführen, müssen Sie die Appliance aus- und wieder einschalten, um den Knoten neu zu starten.

   Für das Gerät fährt dieser Befehl den Controller herunter, das Gerät bleibt jedoch eingeschaltet. Sie müssen den nächsten Schritt abschließen.

6. Wenn Sie einen Appliance-Knoten herunterfahren, befolgen Sie die Schritte für Ihre Appliance.

SG6160

a. Schalten Sie die Stromversorgung des SG6100-CN-Speichercontrollers aus.

b. Warten Sie, bis die blaue Betriebs-LED am SG6100-CN-Speichercontroller erlischt.

SGF6112

a. Schalten Sie die Stromversorgung des Geräts aus.

b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG6000

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite der Speichercontroller erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Schalten Sie das Gerät aus und warten Sie, bis die blaue Betriebs-LED erlischt.

SG5800

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite des Speichercontrollers erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Wählen Sie auf der Startseite des SANtricity System Managers **Laufende Vorgänge anzeigen** aus.

c. Bestätigen Sie, dass alle Vorgänge abgeschlossen sind, bevor Sie mit dem nächsten Schritt fortfahren.

d. Schalten Sie beide Netzschalter am Controller-Regal aus und warten Sie, bis alle LEDs am Controller-Regal erloschen sind.

SG5700

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite des Speichercontrollers erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und Siebensegmentanzeigen nicht mehr aktiv sind.

SG110 oder SG1100

a. Schalten Sie die Stromversorgung des Geräts aus.

b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG100 oder SG1000

a. Schalten Sie die Stromversorgung des Geräts aus.

b. Warten Sie, bis die blaue Betriebs-LED erlischt.

7. Melden Sie sich von der Befehlsshell ab: `exit`

Ähnliche Informationen

- "SGF6112 und SG6160 Speichergeräte"
- "SG6000-Speichergeräte"
- "SG5700-Speichergeräte"
- "SG5800-Speichergeräte"
- "SG110 und SG1100 Servicegeräte"
- "SG100 und SG1000 Servicegeräte"

Schalten Sie alle Knoten im Netz aus und wieder ein

Möglicherweise müssen Sie Ihr gesamtes StorageGRID -System herunterfahren, beispielsweise wenn Sie ein Rechenzentrum verlegen. Diese Schritte bieten einen allgemeinen Überblick über die empfohlene Reihenfolge zum Durchführen eines kontrollierten Herunterfahrens und Startens.

Wenn Sie alle Knoten in einer Site oder einem Grid ausschalten, können Sie nicht auf aufgenommene Objekte zugreifen, während die Speicherknoten offline sind.

Dienste stoppen und Grid-Knoten herunterfahren

Bevor Sie ein StorageGRID -System ausschalten können, müssen Sie alle auf jedem Grid-Knoten ausgeführten Dienste stoppen und dann alle virtuellen VMware-Maschinen, Container-Engines und StorageGRID Geräte herunterfahren.

Informationen zu diesem Vorgang

Stoppen Sie zuerst die Dienste auf den Admin-Knoten und Gateway-Knoten und dann die Dienste auf den Speicherknoten.

Mit diesem Ansatz können Sie den primären Admin-Knoten verwenden, um den Status der anderen Grid-Knoten so lange wie möglich zu überwachen.

> Wenn ein einzelner Host mehr als einen Grid-Knoten enthält, fahren Sie den Host erst herunter, wenn Sie alle Knoten auf diesem Host gestoppt haben. Wenn der Host den primären Admin-Knoten enthält, fahren Sie diesen Host zuletzt herunter.

> Bei Bedarf können Sie"Knoten von einem Linux-Host auf einen anderen migrieren" um Host-Wartungsarbeiten durchzuführen, ohne die Funktionalität oder Verfügbarkeit Ihres Grids zu beeinträchtigen.

Schritte

1. Verhindern Sie, dass alle Clientanwendungen auf das Grid zugreifen.
2. Melden Sie sich bei jedem Gateway-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Stoppen Sie alle auf dem Knoten laufenden Dienste: `service servermanager stop`

   Das Herunterfahren von Diensten kann bis zu 15 Minuten dauern. Sie möchten sich möglicherweise per Fernzugriff beim System anmelden, um den Herunterfahrvorgang zu überwachen.

4. Wiederholen Sie die beiden vorherigen Schritte, um die Dienste auf allen Speicherknoten und nicht primären Admin-Knoten zu stoppen.

   Sie können die Dienste auf diesen Knoten in beliebiger Reihenfolge stoppen.

   > Wenn Sie die `service servermanager stop` Befehl zum Stoppen der Dienste auf einem Appliance-Speicherknoten. Sie müssen die Appliance aus- und wieder einschalten, um den Knoten neu zu starten.

5. Für den primären Admin-Knoten wiederholen Sie die Schritte fürAnmelden am Knoten UndStoppen aller Dienste auf dem Knoten .
6. Für Knoten, die auf Linux-Hosts ausgeführt werden:
   a. Melden Sie sich beim Host-Betriebssystem an.
   b. Stoppen Sie den Knoten: `storagegrid node stop`
   c. Fahren Sie das Host-Betriebssystem herunter.
7. Geben Sie für Knoten, die auf virtuellen VMware-Maschinen ausgeführt werden, und für Appliance-Speicherknoten den Befehl „shutdown“ ein: `shutdown -h now`

   Führen Sie diesen Schritt unabhängig vom Ergebnis der `service servermanager stop` Befehl.

   Für die Appliance fährt dieser Befehl den Compute-Controller herunter, die Appliance bleibt jedoch weiterhin eingeschaltet. Sie müssen den nächsten Schritt abschließen.

8. Wenn Sie über Appliance-Knoten verfügen, befolgen Sie die Schritte für Ihre Appliance.

SG110 oder SG1100

a. Schalten Sie die Stromversorgung des Geräts aus.

b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG100 oder SG1000

a. Schalten Sie die Stromversorgung des Geräts aus.

b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG6160

a. Schalten Sie die Stromversorgung des SG6100-CN-Speichercontrollers aus.

b. Warten Sie, bis die blaue Betriebs-LED am SG6100-CN-Speichercontroller erlischt.

SGF6112

a. Schalten Sie die Stromversorgung des Geräts aus.

b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG6000

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite der Speichercontroller erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Schalten Sie das Gerät aus und warten Sie, bis die blaue Betriebs-LED erlischt.

SG5800

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite des Speichercontrollers erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Wählen Sie auf der Startseite des SANtricity System Managers **Laufende Vorgänge anzeigen** aus.

c. Bestätigen Sie, dass alle Vorgänge abgeschlossen sind, bevor Sie mit dem nächsten Schritt fortfahren.

d. Schalten Sie beide Netzschalter am Controller-Regal aus und warten Sie, bis alle LEDs am Controller-Regal erloschen sind.

SG5700

a. Warten Sie, bis die grüne Cache Active-LED auf der Rückseite des Speichercontrollers erlischt.

   Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED erlischt, bevor Sie die Stromversorgung ausschalten.

b. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und Siebensegmentanzeigen nicht mehr aktiv sind.

9. Melden Sie sich bei Bedarf von der Befehlsshell ab: `exit`

   Das StorageGRID -Netz wurde inzwischen abgeschaltet.

Grid-Knoten starten

> Wenn das gesamte Netz länger als 15 Tage heruntergefahren war, müssen Sie sich an den technischen Support wenden, bevor Sie Netzknoten hochfahren. Versuchen Sie nicht, die Wiederherstellungsverfahren zum Wiederherstellen von Cassandra-Daten durchzuführen. Dies kann zu Datenverlust führen.

Schalten Sie die Netzknoten nach Möglichkeit in dieser Reihenfolge ein:

- Schalten Sie zuerst die Admin-Knoten ein.
- Schalten Sie die Gateway-Knoten zuletzt ein.

> Wenn ein Host mehrere Grid-Knoten enthält, werden die Knoten automatisch wieder online geschaltet, wenn Sie den Host einschalten.

Schritte

1. Schalten Sie die Hosts für den primären Admin-Knoten und alle nicht primären Admin-Knoten ein.

   > Sie können sich erst bei den Admin-Knoten anmelden, wenn die Speicherknoten neu gestartet wurden.

2. Schalten Sie die Hosts für alle Speicherknoten ein.

   Sie können diese Knoten in beliebiger Reihenfolge einschalten.

3. Schalten Sie die Hosts für alle Gateway-Knoten ein.
4. Sign in .
5. Wählen Sie **NODES** aus und überwachen Sie den Status der Grid-Knoten. Stellen Sie sicher, dass neben den Knotennamen keine Warnsymbole angezeigt werden.

Ähnliche Informationen

- "SGF6112 und SG6160 Speichergeräte"
- "SG110 und SG1100 Servicegeräte"
- "SG100 und SG1000 Servicegeräte"
- "SG6000-Speichergeräte"
- "SG5800-Speichergeräte"
- "SG5700-Speichergeräte"

Port-Neuzuordnungsverfahren

Port-Neuzuordnungen entfernen

Wenn Sie einen Endpunkt für den Load Balancer-Dienst konfigurieren und einen Port verwenden möchten, der bereits als Mapped-To-Port einer Port-Neuzuordnung konfiguriert wurde, müssen Sie zuerst die vorhandene Port-Neuzuordnung entfernen, da der Endpunkt sonst nicht wirksam ist. Sie müssen auf jedem Admin-Knoten und Gateway-Knoten mit widersprüchlichen neu zugeordneten Ports ein Skript ausführen, um alle Port-Neuzuordnungen des Knotens zu entfernen.

Informationen zu diesem Vorgang

Durch dieses Verfahren werden alle Port-Neuzuordnungen entfernt. Wenn Sie einige der Neuzuordnungen behalten müssen, wenden Sie sich an den technischen Support.

Informationen zum Konfigurieren von Load Balancer-Endpunkten finden Sie unter"Konfigurieren von Load Balancer-Endpunkten" .

> Wenn die Portneuzuordnung Clientzugriff ermöglicht, konfigurieren Sie den Client neu, sodass er einen anderen Port als Endpunkt des Lastenausgleichs verwendet, um einen Dienstverlust zu vermeiden. Andernfalls führt das Entfernen der Portzuordnung zum Verlust des Clientzugriffs und sollte entsprechend geplant werden.

> Dieses Verfahren funktioniert nicht für ein StorageGRID -System, das als Container auf Bare-Metal-Hosts bereitgestellt wird. Siehe die Anweisungen für"Entfernen von Port-Neuzuordnungen auf Bare-Metal-Hosts" .

Schritte

1. Melden Sie sich beim Knoten an.
   a. Geben Sie den folgenden Befehl ein: `ssh -p 8022 admin@node_IP`

      Port 8022 ist der SSH-Port des Basisbetriebssystems, während Port 22 der SSH-Port der Container-Engine ist, auf der StorageGRID ausgeführt wird.

   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 das folgende Skript aus: `remove-port-remap.sh`
3. Starten Sie den Knoten neu: `reboot`
4. Melden Sie sich von der Befehlsshell ab: `exit`
5. Wiederholen Sie diese Schritte auf jedem Admin-Knoten und Gateway-Knoten, bei dem es zu Konflikten bei der Neuzuordnung der Ports kommt.

Entfernen Sie Port-Neuzuordnungen auf Bare-Metal-Hosts

Wenn Sie einen Endpunkt für den Load Balancer-Dienst konfigurieren und einen Port verwenden möchten, der bereits als Mapped-To-Port einer Port-Neuzuordnung konfiguriert wurde, müssen Sie zuerst die vorhandene Port-Neuzuordnung entfernen, da der Endpunkt sonst nicht wirksam ist.

Informationen zu diesem Vorgang

Wenn Sie StorageGRID auf Bare-Metal-Hosts ausführen, befolgen Sie dieses Verfahren anstelle des allgemeinen Verfahrens zum Entfernen von Port-Neuzuordnungen. Sie müssen die Knotenkonfigurationsdatei für jeden Admin-Knoten und Gateway-Knoten mit widersprüchlichen neu zugeordneten Ports bearbeiten, um alle Port-Neuzuordnungen des Knotens zu entfernen und den Knoten neu zu starten.

Durch dieses Verfahren werden alle Port-Neuzuordnungen entfernt. Wenn Sie einige der Neuzuordnungen behalten müssen, wenden Sie sich an den technischen Support.

Informationen zum Konfigurieren von Load Balancer-Endpunkten finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Dieses Verfahren kann zu einem vorübergehenden Dienstverlust führen, da Knoten neu gestartet werden.

Schritte

1. Melden Sie sich beim Host an, der den Knoten unterstützt. Melden Sie sich als Root oder mit einem Konto mit Sudo-Berechtigung an.
2. Führen Sie den folgenden Befehl aus, um den Knoten vorübergehend zu deaktivieren: `sudo storagegrid node stop node-name`
3. Bearbeiten Sie die Knotenkonfigurationsdatei für den Knoten mit einem Texteditor wie vim oder pico.

   Die Knotenkonfigurationsdatei finden Sie unter `/etc/storagegrid/nodes/node-name.conf` .
4. Suchen Sie den Abschnitt der Knotenkonfigurationsdatei, der die Portneuzuordnungen enthält.

   Siehe die letzten beiden Zeilen im folgenden Beispiel.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. Bearbeiten Sie die Einträge PORT_REMAP und PORT_REMAP_INBOUND, um Port-Neuzuordnungen zu entfernen.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Führen Sie den folgenden Befehl aus, um Ihre Änderungen an der Knotenkonfigurationsdatei für den Knoten zu validieren:`sudo storagegrid node validate node-name`

   Beheben Sie alle Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

7. Führen Sie den folgenden Befehl aus, um den Knoten ohne Portneuzuordnungen neu zu starten: `sudo storagegrid node start node-name`
8. Melden Sie sich als Administrator am Knoten an und verwenden Sie dabei das Passwort, das in der `Passwords.txt` Datei.
9. Überprüfen Sie, ob die Dienste ordnungsgemäß gestartet werden.
   a. Zeigen Sie eine Liste der Status aller Dienste auf dem Server an:`sudo storagegrid-status`

Der Status wird automatisch aktualisiert.

b. Warten Sie, bis alle Dienste den Status „Wird ausgeführt“ oder „Verifiziert“ haben.

c. Verlassen Sie den Statusbildschirm:`Ctrl+C`

10. Wiederholen Sie diese Schritte auf jedem Admin-Knoten und Gateway-Knoten, bei dem es zu Konflikten bei der Neuzuordnung der Ports kommt.

Netzwerkverfahren

Subnetze für Grid-Netzwerke aktualisieren

StorageGRID verwaltet eine Liste der Netzwerk-Subnetze, die zur Kommunikation zwischen Grid-Knoten im Grid-Netzwerk (eth0) verwendet werden. Diese Einträge umfassen die von jedem Standort in Ihrem StorageGRID -System für das Grid-Netzwerk verwendeten Subnetze sowie alle für NTP, DNS, LDAP oder andere externe Server verwendeten Subnetze, auf die über das Grid-Netzwerk-Gateway zugegriffen wird. Wenn Sie Grid-Knoten oder einen neuen Standort in einer Erweiterung hinzufügen, müssen Sie möglicherweise Subnetze zum Grid-Netzwerk aktualisieren oder hinzufügen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben die Bereitstellungspassphrase.
- Sie verfügen über die Netzwerkadressen der Subnetze, die Sie konfigurieren möchten, in CIDR-Notation.

Informationen zu diesem Vorgang

Wenn Sie eine Erweiterungsaktivität durchführen, die das Hinzufügen eines neuen Subnetzes umfasst, müssen Sie der Grid-Netzwerk-Subnetzliste ein neues Subnetz hinzufügen, bevor Sie mit dem Erweiterungsvorgang beginnen. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und die Erweiterung erneut starten.

Verwenden Sie keine Subnetze, die die folgenden IPv4-Adressen für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens enthalten:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Verwenden Sie beispielsweise nicht die folgenden Subnetzbereiche für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens:

- 192.168.130.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.130.101 und 192.168.130.102 enthält
- 192.168.131.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.131.101 und 192.168.131.102 enthält
- 198.51.100.0/24, da dieser Subnetzbereich die IP-Adressen 198.51.100.2 und 198.51.100.4 enthält

Hinzufügen eines Subnetzes

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **Grid-Netzwerk**.
2. Wählen Sie **Weiteres Subnetz hinzufügen**, um ein neues Subnetz in CIDR-Notation hinzuzufügen.

   Geben Sie beispielsweise `10.96.104.0/22` .
3. Geben Sie die Bereitstellungspassphrase ein und wählen Sie **Speichern**.
4. Warten Sie, bis die Änderungen übernommen wurden, und laden Sie dann ein neues Wiederherstellungspaket herunter.
   a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
   b. Geben Sie die **Bereitstellungspassphrase** ein.

Die Datei des Wiederherstellungspakets muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können. Es wird auch verwendet, um den primären Admin-Knoten wiederherzustellen.

Die von Ihnen angegebenen Subnetze werden automatisch für Ihr StorageGRID -System konfiguriert.

Bearbeiten eines Subnetzes

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **Grid-Netzwerk**.
2. Wählen Sie das Subnetz aus, das Sie bearbeiten möchten, und nehmen Sie die erforderlichen Änderungen vor.

3. Geben Sie die Bereitstellungspassphrase ein und wählen Sie **Speichern**.
4. Wählen Sie im Bestätigungsdialogfeld **Ja** aus.
5. Warten Sie, bis die Änderungen übernommen wurden, und laden Sie dann ein neues Wiederherstellungspaket herunter.
   a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
   b. Geben Sie die **Bereitstellungspassphrase** ein.

Löschen eines Subnetzes

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **Grid-Netzwerk**.
2. Wählen Sie das Löschsymbol neben dem Subnetz.
3. Geben Sie die Bereitstellungspassphrase ein und wählen Sie **Speichern**.
4. Wählen Sie im Bestätigungsdialogfeld **Ja** aus.
5. Warten Sie, bis die Änderungen übernommen wurden, und laden Sie dann ein neues Wiederherstellungspaket herunter.
   a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
   b. Geben Sie die **Bereitstellungspassphrase** ein.

Konfigurieren von IP-Adressen

Richtlinien für IP-Adressen

Sie können die Netzwerkkonfiguration durchführen, indem Sie mit dem Tool „IP ändern“ IP-Adressen für Grid-Knoten konfigurieren.

Sie müssen das Tool „IP ändern“ verwenden, um die meisten Änderungen an der Netzwerkkonfiguration vorzunehmen, die ursprünglich während der Grid-Bereitstellung festgelegt wurde. Manuelle Änderungen mithilfe von standardmäßigen Linux-Netzwerkbefehlen und -dateien werden möglicherweise nicht auf alle StorageGRID -Dienste übertragen und bleiben möglicherweise bei Upgrades, Neustarts oder Knotenwiederherstellungsverfahren nicht erhalten.

Das Verfahren zur Änderung der IP-Adresse kann ein störender Vorgang sein. Teile des Rasters sind möglicherweise nicht verfügbar, bis die neue Konfiguration angewendet wird.

Wenn Sie nur Änderungen an der Grid-Netzwerk-Subnetzliste vornehmen, verwenden Sie den Grid-Manager, um die Netzwerkkonfiguration hinzuzufügen oder zu ändern. Verwenden Sie andernfalls das Tool „IP ändern“, wenn auf den Grid Manager aufgrund eines Netzwerkkonfigurationsproblems nicht zugegriffen werden kann oder Sie gleichzeitig eine Änderung der Grid-Netzwerkweiterleitung und andere Netzwerkänderungen durchführen.

Wenn Sie die Grid-Netzwerk-IP-Adresse für alle Knoten im Grid ändern möchten, verwenden Sie die"Sonderverfahren für netzweite Änderungen" .

Ethernet-Schnittstellen

Die eth0 zugewiesene IP-Adresse ist immer die Grid-Netzwerk-IP-Adresse des Grid-Knotens. Die eth1

zugewiesene IP-Adresse ist immer die Admin-Netzwerk-IP-Adresse des Grid-Knotens. Die eth2 zugewiesene IP-Adresse ist immer die Client-Netzwerk-IP-Adresse des Grid-Knotens.

Beachten Sie, dass es sich bei eth0, eth1 und eth2 auf einigen Plattformen, z. B. StorageGRID -Geräten, möglicherweise um aggregierte Schnittstellen handelt, die aus untergeordneten Brücken oder Verbindungen von physischen oder VLAN-Schnittstellen bestehen. Auf diesen Plattformen werden auf der Registerkarte **SSM > Ressourcen** möglicherweise die Grid-, Admin- und Client-Netzwerk-IP-Adressen angezeigt, die zusätzlich zu eth0, eth1 oder eth2 anderen Schnittstellen zugewiesen sind.

DHCP

Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten. Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmasken und Standard-Gateways für einen Grid-Knoten ändern möchten. Durch die Verwendung des Tools „IP ändern“ werden DHCP-Adressen statisch.

Hochverfügbarkeitsgruppen (HA)

- Wenn eine Client-Netzwerkschnittstelle in einer HA-Gruppe enthalten ist, können Sie die Client-Netzwerk-IP-Adresse für diese Schnittstelle nicht in eine Adresse ändern, die außerhalb des für die HA-Gruppe konfigurierten Subnetzes liegt.
- Sie können die Client-Netzwerk-IP-Adresse nicht in den Wert einer vorhandenen virtuellen IP-Adresse ändern, die einer auf der Client-Netzwerkschnittstelle konfigurierten HA-Gruppe zugewiesen ist.
- Wenn eine Grid-Netzwerkschnittstelle in einer HA-Gruppe enthalten ist, können Sie die Grid-Netzwerk-IP-Adresse für diese Schnittstelle nicht in eine Adresse ändern, die außerhalb des für die HA-Gruppe konfigurierten Subnetzes liegt.
- Sie können die Grid-Netzwerk-IP-Adresse nicht in den Wert einer vorhandenen virtuellen IP-Adresse ändern, die einer auf der Grid-Netzwerkschnittstelle konfigurierten HA-Gruppe zugewiesen ist.

Knotennetzwerkkonfiguration ändern

Sie können die Netzwerkkonfiguration eines oder mehrerer Knoten mit dem Tool „IP ändern“ ändern. Sie können die Konfiguration des Grid-Netzwerks ändern oder die Admin- oder Client-Netzwerke hinzufügen, ändern oder entfernen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Linux: Wenn Sie zum ersten Mal einen Grid-Knoten zum Admin-Netzwerk oder Client-Netzwerk hinzufügen und ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET zuvor nicht in der Knotenkonfigurationsdatei konfiguriert haben, müssen Sie dies jetzt tun.

Lesen Sie die StorageGRID -Installationsanweisungen für Ihr Linux-Betriebssystem:

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"

Geräte: Wenn bei StorageGRID -Geräten das Client- oder Admin-Netzwerk während der Erstinstallation nicht im StorageGRID -Geräteinstallationsprogramm konfiguriert wurde, kann das Netzwerk nicht nur mithilfe des Tools „IP ändern“ hinzugefügt werden. Zuerst müssen Sie "Versetzen Sie das Gerät in den Wartungsmodus" , konfigurieren Sie die Links, versetzen Sie die Appliance wieder in den normalen Betriebsmodus und

verwenden Sie dann das Tool „IP ändern“, um die Netzwerkkonfiguration zu ändern. Siehe die "Verfahren zum Konfigurieren von Netzwerkverbindungen" .

Sie können die IP-Adresse, die Subnetzmaske, das Gateway oder den MTU-Wert für einen oder mehrere Knoten in jedem Netzwerk ändern.

Sie können auch einen Knoten zu einem Client-Netzwerk oder einem Admin-Netzwerk hinzufügen oder daraus entfernen:

- Sie können einem Client-Netzwerk oder einem Admin-Netzwerk einen Knoten hinzufügen, indem Sie dem Knoten eine IP-Adresse/Subnetzmaske in diesem Netzwerk hinzufügen.
- Sie können einen Knoten aus einem Client-Netzwerk oder einem Admin-Netzwerk entfernen, indem Sie die IP-Adresse/Subnetzmaske für den Knoten in diesem Netzwerk löschen.

  Knoten können nicht aus dem Grid-Netzwerk entfernt werden.

> Ein Austausch der IP-Adresse ist nicht zulässig. Wenn Sie IP-Adressen zwischen Grid-Knoten austauschen müssen, müssen Sie eine temporäre Zwischen-IP-Adresse verwenden.

> Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist und Sie die IP-Adresse eines Admin-Knotens ändern, beachten Sie, dass alle Vertrauensstellungen der vertrauenden Seite, die mit der IP-Adresse des Admin-Knotens (anstelle des vollqualifizierten Domänennamens, wie empfohlen) konfiguriert wurden, ungültig werden. Sie können sich nicht mehr beim Knoten anmelden. Unmittelbar nach der Änderung der IP-Adresse müssen Sie die Vertrauensstellung der vertrauenden Seite des Knotens in Active Directory Federation Services (AD FS) mit der neuen IP-Adresse aktualisieren oder neu konfigurieren. Siehe die Anweisungen für"Konfigurieren von SSO" .

> Alle Änderungen, die Sie mit dem Tool „IP ändern“ am Netzwerk vornehmen, werden an die Installations-Firmware für die StorageGRID -Geräte weitergegeben. Auf diese Weise ist die Netzwerkkonfiguration korrekt, wenn die StorageGRID -Software auf einem Gerät neu installiert wird oder ein Gerät in den Wartungsmodus versetzt wird.

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.

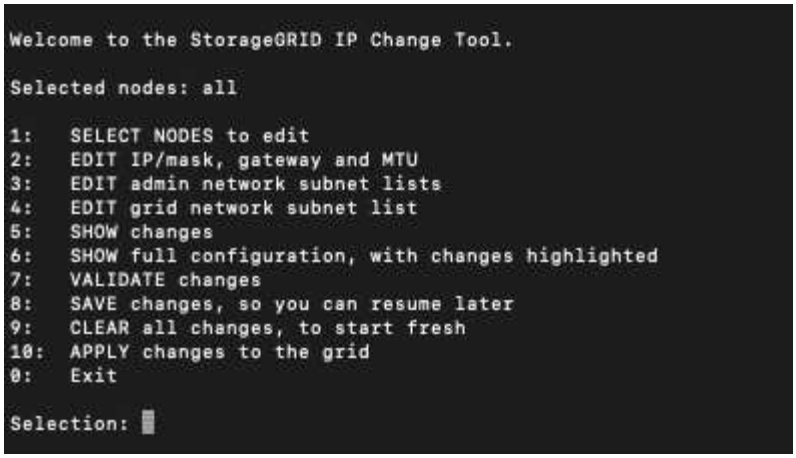
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

   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. Starten Sie das Tool „IP ändern“, indem Sie den folgenden Befehl eingeben: `change-ip`
3. Geben Sie bei der Eingabeaufforderung die Bereitstellungspassphrase ein.

   Das Hauptmenü wird angezeigt.



4. Wählen Sie optional **1** aus, um auszuwählen, welche Knoten aktualisiert werden sollen. Wählen Sie dann eine der folgenden Optionen:

   - **1**: Einzelner Knoten – Auswahl nach Name
   - **2**: Einzelner Knoten – Auswahl nach Site, dann nach Name
   - **3**: Einzelner Knoten – Auswahl nach aktueller IP
   - **4**: Alle Knoten an einem Standort
   - **5**: Alle Knoten im Raster

     Hinweis: Wenn Sie alle Knoten aktualisieren möchten, lassen Sie „alle“ ausgewählt.

   Nachdem Sie Ihre Auswahl getroffen haben, wird das Hauptmenü angezeigt und das Feld **Ausgewählte Knoten** wird entsprechend Ihrer Auswahl aktualisiert. Alle nachfolgenden Aktionen werden nur auf den angezeigten Knoten ausgeführt.

5. Wählen Sie im Hauptmenü Option **2**, um IP/Maske, Gateway und MTU-Informationen für die ausgewählten Knoten zu bearbeiten.
   a. Wählen Sie das Netzwerk aus, in dem Sie Änderungen vornehmen möchten:

      - **1**: Netz
      - **2**: Admin-Netzwerk
      - **3**: Client-Netzwerk
      - **4**: Alle Netzwerke

      Nachdem Sie Ihre Auswahl getroffen haben, zeigt die Eingabeaufforderung den Knotennamen, den Netzwerknamen (Grid, Admin oder Client), den Datentyp (IP/Maske, Gateway oder MTU) und den aktuellen Wert an.

      Durch Bearbeiten der IP-Adresse, Präfixlänge, des Gateways oder der MTU einer DHCP-konfigurierten Schnittstelle wird die Schnittstelle auf statisch geändert. Wenn Sie eine per DHCP konfigurierte Schnittstelle ändern, wird eine Warnung angezeigt, die Sie darüber informiert, dass die Schnittstelle auf statisch geändert wird.

      Schnittstellen konfiguriert als `fixed` kann nicht bearbeitet werden.

   b. Um einen neuen Wert festzulegen, geben Sie ihn im für den aktuellen Wert angezeigten Format ein.

c. Um den aktuellen Wert unverändert zu lassen, drücken Sie **Enter**.

d. Wenn der Datentyp `IP/mask` können Sie das Admin- oder Client-Netzwerk vom Knoten löschen, indem Sie **d** oder **0.0.0.0/0** eingeben.

e. Nachdem Sie alle Knoten bearbeitet haben, die Sie ändern möchten, geben Sie **q** ein, um zum Hauptmenü zurückzukehren.

   Ihre Änderungen werden zurückgehalten, bis sie gelöscht oder angewendet werden.

6. Überprüfen Sie Ihre Änderungen, indem Sie eine der folgenden Optionen auswählen:

   - **5**: Zeigt Bearbeitungen in der Ausgabe an, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe gezeigt:

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

   - **6**: Zeigt Änderungen in der Ausgabe an, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben.

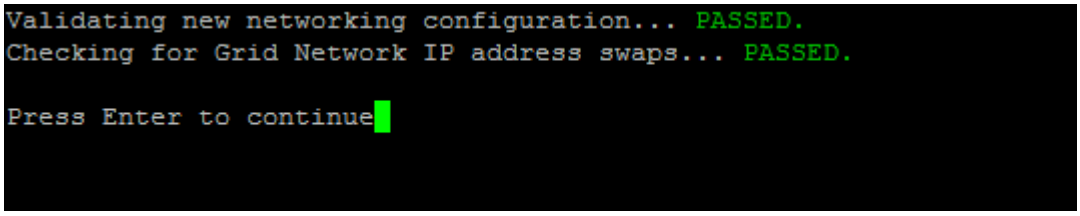
> Bestimmte Befehlszeilenschnittstellen zeigen Hinzufügungen und Löschungen möglicherweise durchgestrichen an. Die korrekte Anzeige hängt davon ab, ob Ihr Terminalclient die erforderlichen VT100-Escapesequenzen unterstützt.

7. Wählen Sie Option **7**, um alle Änderungen zu bestätigen.

   Diese Validierung stellt sicher, dass die Regeln für das Grid-, Admin- und Client-Netzwerk, wie z. B. die Nichtverwendung überlappender Subnetze, nicht verletzt werden.

   In diesem Beispiel hat die Validierung Fehler zurückgegeben.

In diesem Beispiel wurde die Validierung erfolgreich durchgeführt.



8. Wählen Sie nach erfolgreicher Validierung eine der folgenden Optionen:
   - **8**: Nicht angewendete Änderungen speichern.

     Mit dieser Option können Sie das Tool „IP ändern“ beenden und später erneut starten, ohne dass nicht angewendete Änderungen verloren gehen.

   - **10**: Wenden Sie die neue Netzwerkkonfiguration an.
9. Wenn Sie Option **10** ausgewählt haben, wählen Sie eine der folgenden Optionen:
   - **Anwenden**: Wenden Sie die Änderungen sofort an und starten Sie jeden Knoten bei Bedarf automatisch neu.

     Wenn für die neue Netzwerkkonfiguration keine physischen Netzwerkänderungen erforderlich sind, können Sie „Übernehmen“ auswählen, um die Änderungen sofort anzuwenden. Knoten werden bei Bedarf automatisch neu gestartet. Knoten, die neu gestartet werden müssen, werden angezeigt.

   - **Phase**: Wenden Sie die Änderungen beim nächsten manuellen Neustart der Knoten an.

     Wenn Sie Änderungen an der physischen oder virtuellen Netzwerkkonfiguration vornehmen müssen, damit die neue Netzwerkkonfiguration funktioniert, müssen Sie die Option **stage** verwenden, die betroffenen Knoten herunterfahren, die erforderlichen physischen Netzwerkänderungen vornehmen und die betroffenen Knoten neu starten. Wenn Sie „Übernehmen“ auswählen, ohne zuerst diese Netzwerkänderungen vorzunehmen, schlagen die Änderungen normalerweise fehl.

     > Wenn Sie die Option **Stage** verwenden, müssen Sie den Knoten nach der Bereitstellung so schnell wie möglich neu starten, um Störungen zu minimieren.

   - **Abbrechen**: Nehmen Sie derzeit keine Netzwerkänderungen vor.

     Wenn Sie nicht wussten, dass die vorgeschlagenen Änderungen einen Neustart der Knoten erfordern, können Sie die Änderungen verschieben, um die Auswirkungen auf die Benutzer zu minimieren. Wenn Sie „Abbrechen“ auswählen, kehren Sie zum Hauptmenü zurück und Ihre Änderungen bleiben erhalten, sodass Sie sie später anwenden können.

     Wenn Sie **Übernehmen** oder **Stufe** auswählen, wird eine neue Netzwerkkonfigurationsdatei generiert, die Bereitstellung durchgeführt und die Knoten mit neuen Arbeitsinformationen aktualisiert.

Während der Bereitstellung zeigt die Ausgabe den Status an, während Updates angewendet werden.

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

Nachdem Sie Änderungen angewendet oder bereitgestellt haben, wird aufgrund der Änderung der Grid-Konfiguration ein neues Wiederherstellungspaket generiert.

10. Wenn Sie **Phase** ausgewählt haben, führen Sie nach Abschluss der Bereitstellung die folgenden Schritte aus:

    a. Nehmen Sie die erforderlichen physischen oder virtuellen Netzwerkänderungen vor.

    Änderungen am physischen Netzwerk: Nehmen Sie die erforderlichen Änderungen am physischen Netzwerk vor und fahren Sie den Knoten bei Bedarf sicher herunter.

    Linux: Wenn Sie den Knoten zum ersten Mal zu einem Admin-Netzwerk oder Client-Netzwerk hinzufügen, stellen Sie sicher, dass Sie die Schnittstelle wie in beschrieben hinzugefügt haben"Linux: Schnittstellen zum vorhandenen Knoten hinzufügen" .

    a. Starten Sie die betroffenen Knoten neu.

11. Wählen Sie **0**, um das Tool „IP ändern“ nach Abschluss Ihrer Änderungen zu beenden.
12. Laden Sie ein neues Wiederherstellungspaket vom Grid Manager herunter.
    a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
    b. Geben Sie die Bereitstellungspassphrase ein.

Subnetzlisten im Admin-Netzwerk hinzufügen oder ändern

Sie können die Subnetze in der Subnetzliste des Admin-Netzwerks eines oder mehrerer Knoten hinzufügen, löschen oder ändern.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei.

Sie können allen Knoten in der Subnetzliste des Admin-Netzwerks Subnetze hinzufügen, löschen oder ändern.

Verwenden Sie keine Subnetze, die die folgenden IPv4-Adressen für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens enthalten:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Verwenden Sie beispielsweise nicht die folgenden Subnetzbereiche für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens:

- 192.168.130.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.130.101 und 192.168.130.102 enthält
- 192.168.131.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.131.101 und 192.168.131.102 enthält
- 198.51.100.0/24, da dieser Subnetzbereich die IP-Adressen 198.51.100.2 und 198.51.100.4 enthält

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. Starten Sie das Tool „IP ändern“, indem Sie den folgenden Befehl eingeben: `change-ip`
3. Geben Sie bei der Eingabeaufforderung die Bereitstellungspassphrase ein.

   Das Hauptmenü wird angezeigt.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

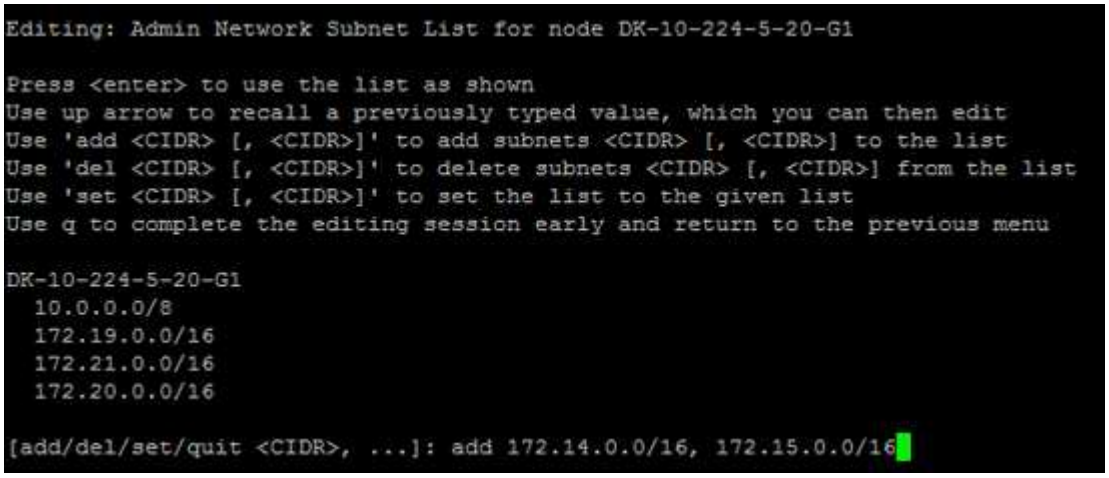
4. Beschränken Sie optional die Netzwerke/Knoten, auf denen Vorgänge ausgeführt werden. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie die zu bearbeitenden Knoten aus, indem Sie **1** wählen, wenn Sie nach bestimmten Knoten filtern möchten, an denen der Vorgang ausgeführt werden soll. Wählen Sie eine der folgenden Optionen:
     - **1**: Einzelner Knoten (Auswahl nach Name)
     - **2**: Einzelner Knoten (Auswahl nach Site, dann nach Name)
     - **3**: Einzelner Knoten (Auswahl nach aktueller IP)
     - **4**: Alle Knoten an einem Standort
     - **5**: Alle Knoten im Raster
     - **0**: Zurück
   - Lassen Sie „Alle“ ausgewählt bleiben. Nachdem die Auswahl getroffen wurde, wird der Hauptmenübildschirm angezeigt. Das Feld „Ausgewählte Knoten“ spiegelt Ihre neue Auswahl wider und jetzt werden alle ausgewählten Vorgänge nur für dieses Element ausgeführt.
5. Wählen Sie im Hauptmenü die Option zum Bearbeiten von Subnetzen für das Admin-Netzwerk (Option **3**).
6. Wählen Sie eine der folgenden Optionen:
   - Fügen Sie ein Subnetz hinzu, indem Sie diesen Befehl eingeben: `add CIDR`
   - Löschen Sie ein Subnetz, indem Sie diesen Befehl eingeben: `del CIDR`
   - Legen Sie die Liste der Subnetze fest, indem Sie diesen Befehl eingeben: `set CIDR`

   Für alle Befehle können Sie mehrere Adressen in diesem Format eingeben: `add CIDR, CIDR`

   Beispiel: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   Sie können den Tippaufwand reduzieren, indem Sie mit der Taste „Pfeil nach oben“ bereits eingegebene Werte in die aktuelle Eingabeaufforderung zurückrufen und diese dann gegebenenfalls bearbeiten.

   Die folgende Beispieleingabe zeigt das Hinzufügen von Subnetzen zur Subnetzliste des Admin-Netzwerks:

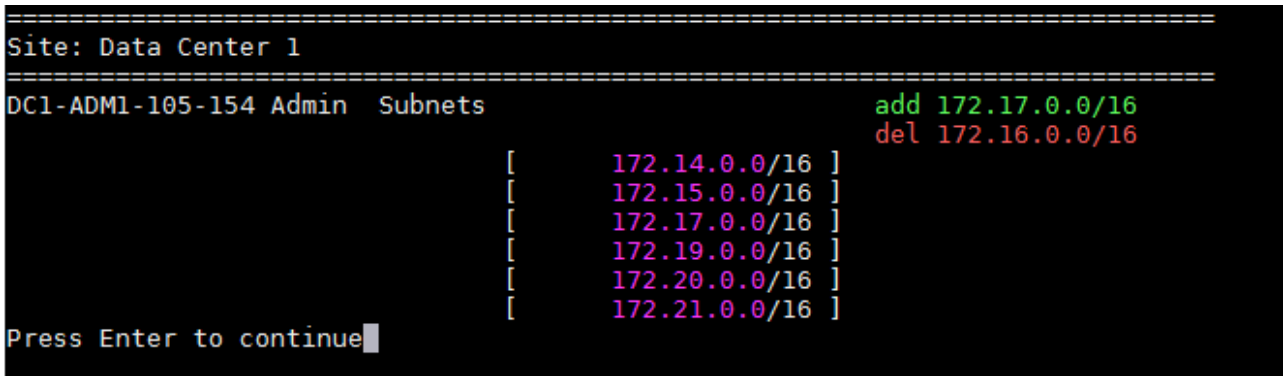


7. Wenn Sie fertig sind, geben Sie **q** ein, um zum Hauptmenübildschirm zurückzukehren. Ihre Änderungen werden zurückgehalten, bis sie gelöscht oder angewendet werden.

> Wenn Sie in Schritt 2 einen der Knotenauswahlmodi „Alle“ ausgewählt haben, drücken Sie **Eingabe** (ohne **q**), um zum nächsten Knoten in der Liste zu gelangen.

8. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie Option **5**, um Änderungen in der Ausgabe anzuzeigen, die isoliert ist, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben, wie in der folgenden Beispielausgabe gezeigt:



   - Wählen Sie Option **6**, um Änderungen in der Ausgabe anzuzeigen, die die vollständige Konfiguration anzeigt. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben. **Hinweis:** Bestimmte Terminalemulatoren zeigen Hinzufügungen und Löschungen möglicherweise durchgestrichen an.

     Wenn Sie versuchen, die Subnetzliste zu ändern, wird die folgende Meldung angezeigt:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

     Wenn Sie die NTP- und DNS-Server-Subnetze nicht speziell einem Netzwerk zugewiesen haben, erstellt StorageGRID automatisch eine Hostroute (/32) für die Verbindung. Wenn Sie beispielsweise lieber eine /16- oder /24-Route für die ausgehende Verbindung zu einem DNS- oder NTP-Server hätten, sollten Sie die automatisch erstellte /32-Route löschen und die gewünschten Routen hinzufügen. Wenn Sie die automatisch erstellte Hostroute nicht löschen, bleibt sie bestehen, nachdem Sie Änderungen an der Subnetzliste vorgenommen haben.

Obwohl Sie diese automatisch erkannten Hostrouten verwenden können, sollten Sie die DNS- und NTP-Routen im Allgemeinen manuell konfigurieren, um die Konnektivität sicherzustellen.

9. Wählen Sie Option **7**, um alle schrittweisen Änderungen zu validieren.

   Diese Validierung stellt sicher, dass die Regeln für die Grid-, Admin- und Client-Netzwerke eingehalten werden, beispielsweise die Verwendung überlappender Subnetze.

10. Wählen Sie optional Option **8** aus, um alle schrittweisen Änderungen zu speichern und später zurückzukehren, um mit den Änderungen fortzufahren.

    Mit dieser Option können Sie das Tool „IP ändern“ beenden und später erneut starten, ohne dass nicht angewendete Änderungen verloren gehen.

11. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie Option **9**, wenn Sie alle Änderungen löschen möchten, ohne die neue Netzwerkkonfiguration zu speichern oder anzuwenden.
    - Wählen Sie Option **10**, wenn Sie bereit sind, Änderungen anzuwenden und die neue Netzwerkkonfiguration bereitzustellen. Während der Bereitstellung zeigt die Ausgabe den Status beim Anwenden von Updates an, wie in der folgenden Beispielausgabe dargestellt:

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

12. Laden Sie ein neues Wiederherstellungspaket vom Grid Manager herunter.
    a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
    b. Geben Sie die Bereitstellungspassphrase ein.

Subnetzlisten im Grid-Netzwerk hinzufügen oder ändern

Mit dem Tool „IP ändern“ können Sie Subnetze im Grid-Netzwerk hinzufügen oder ändern.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei.

Sie können Subnetze in der Grid-Netzwerk-Subnetzliste hinzufügen, löschen oder ändern. Änderungen wirken sich auf das Routing aller Knoten im Raster aus.

Wenn Sie nur Änderungen an der Grid-Netzwerk-Subnetzliste vornehmen, verwenden Sie den Grid-Manager, um die Netzwerkkonfiguration hinzuzufügen oder zu ändern. Verwenden Sie andernfalls das Tool „IP ändern“, wenn auf den Grid Manager aufgrund eines Netzwerkkonfigurationsproblems nicht zugegriffen werden kann oder Sie gleichzeitig eine Änderung der Grid-Netzwerkweiterleitung und andere Netzwerkänderungen durchführen.

Verwenden Sie keine Subnetze, die die folgenden IPv4-Adressen für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens enthalten:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Verwenden Sie beispielsweise nicht die folgenden Subnetzbereiche für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens:

- 192.168.130.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.130.101 und 192.168.130.102 enthält
- 192.168.131.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.131.101 und 192.168.131.102 enthält
- 198.51.100.0/24, da dieser Subnetzbereich die IP-Adressen 198.51.100.2 und 198.51.100.4 enthält

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. Starten Sie das Tool „IP ändern“, indem Sie den folgenden Befehl eingeben: `change-ip`
3. Geben Sie bei der Eingabeaufforderung die Bereitstellungspassphrase ein.

   Das Hauptmenü wird angezeigt.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. Wählen Sie im Hauptmenü die Option zum Bearbeiten von Subnetzen für das Grid-Netzwerk (Option **4**).

   Änderungen an der Grid-Netzwerk-Subnetzliste gelten für das gesamte Grid.

5. Wählen Sie eine der folgenden Optionen:

   - Fügen Sie ein Subnetz hinzu, indem Sie diesen Befehl eingeben: `add CIDR`
   - Löschen Sie ein Subnetz, indem Sie diesen Befehl eingeben: `del CIDR`
   - Legen Sie die Liste der Subnetze fest, indem Sie diesen Befehl eingeben: `set CIDR`

   Für alle Befehle können Sie mehrere Adressen in diesem Format eingeben: `add CIDR, CIDR`

   Beispiel: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

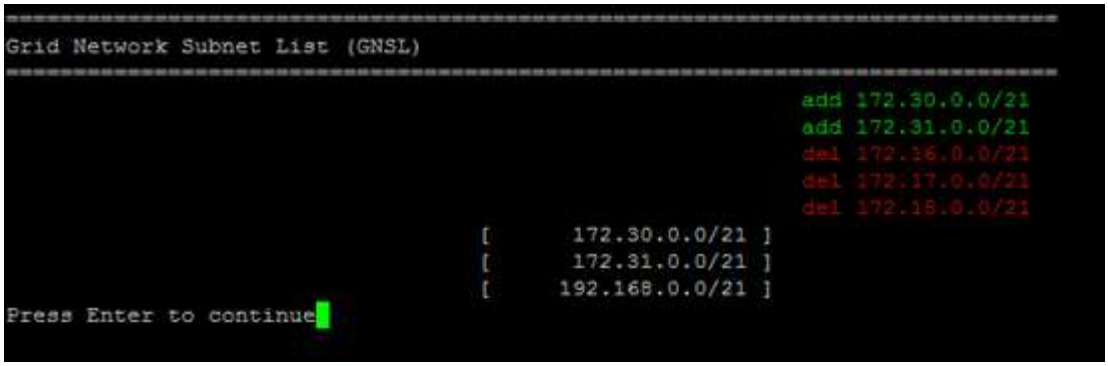
   Sie können den Tippaufwand reduzieren, indem Sie mit der Taste „Pfeil nach oben“ bereits eingegebene Werte in die aktuelle Eingabeaufforderung zurückrufen und diese dann gegebenenfalls bearbeiten.

   Die folgende Beispieleingabe zeigt das Festlegen von Subnetzen für die Grid-Netzwerk-Subnetzliste:

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. Wenn Sie fertig sind, geben Sie **q** ein, um zum Hauptmenübildschirm zurückzukehren. Ihre Änderungen werden zurückgehalten, bis sie gelöscht oder angewendet werden.
7. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie Option **5**, um Änderungen in der Ausgabe anzuzeigen, die isoliert ist, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben, wie in der folgenden Beispielausgabe gezeigt:



- Wählen Sie Option **6**, um Änderungen in der Ausgabe anzuzeigen, die die vollständige Konfiguration anzeigt. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben.

  Bestimmte Befehlszeilenschnittstellen zeigen Hinzufügungen und Löschungen möglicherweise durchgestrichen an.

8. Wählen Sie Option **7**, um alle schrittweisen Änderungen zu validieren.

   Diese Validierung stellt sicher, dass die Regeln für die Grid-, Admin- und Client-Netzwerke eingehalten werden, beispielsweise die Verwendung überlappender Subnetze.

9. Wählen Sie optional Option **8** aus, um alle schrittweisen Änderungen zu speichern und später zurückzukehren, um mit den Änderungen fortzufahren.

   Mit dieser Option können Sie das Tool „IP ändern“ beenden und später erneut starten, ohne dass nicht angewendete Änderungen verloren gehen.

10. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie Option **9**, wenn Sie alle Änderungen löschen möchten, ohne die neue Netzwerkkonfiguration zu speichern oder anzuwenden.
    - Wählen Sie Option **10**, wenn Sie bereit sind, Änderungen anzuwenden und die neue Netzwerkkonfiguration bereitzustellen. Während der Bereitstellung zeigt die Ausgabe den Status beim Anwenden von Updates an, wie in der folgenden Beispielausgabe dargestellt:

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

11. Wenn Sie beim Vornehmen von Grid-Netzwerkänderungen die Option **10** ausgewählt haben, wählen Sie eine der folgenden Optionen:

    - **Anwenden**: Wenden Sie die Änderungen sofort an und starten Sie jeden Knoten bei Bedarf automatisch neu.

      Wenn die neue Netzwerkkonfiguration ohne externe Änderungen gleichzeitig mit der alten Netzwerkkonfiguration funktionieren soll, können Sie die Option **Übernehmen** für eine vollautomatische Konfigurationsänderung verwenden.

- **Phase**: Wenden Sie die Änderungen beim nächsten Neustart der Knoten an.

  Wenn Sie Änderungen an der physischen oder virtuellen Netzwerkkonfiguration vornehmen müssen, damit die neue Netzwerkkonfiguration funktioniert, müssen Sie die Option **stage** verwenden, die betroffenen Knoten herunterfahren, die erforderlichen physischen Netzwerkänderungen vornehmen und die betroffenen Knoten neu starten.

  > Wenn Sie die Option **Stage** verwenden, starten Sie den Knoten nach der Bereitstellung so bald wie möglich neu, um Unterbrechungen zu minimieren.

- **Abbrechen**: Nehmen Sie derzeit keine Netzwerkänderungen vor.

  Wenn Sie nicht wussten, dass die vorgeschlagenen Änderungen einen Neustart der Knoten erfordern, können Sie die Änderungen verschieben, um die Auswirkungen auf die Benutzer zu minimieren. Wenn Sie „Abbrechen“ auswählen, kehren Sie zum Hauptmenü zurück und Ihre Änderungen bleiben erhalten, sodass Sie sie später anwenden können.

Nachdem Sie Änderungen angewendet oder bereitgestellt haben, wird aufgrund der Änderung der Grid-Konfiguration ein neues Wiederherstellungspaket generiert.

12. Wenn die Konfiguration aufgrund von Fehlern abgebrochen wird, stehen folgende Optionen zur Verfügung:
    - Um den IP-Änderungsvorgang abzubrechen und zum Hauptmenü zurückzukehren, geben Sie **a** ein.
    - Um den fehlgeschlagenen Vorgang erneut zu versuchen, geben Sie **r** ein.
    - Um mit der nächsten Operation fortzufahren, geben Sie **c** ein.

      Der fehlgeschlagene Vorgang kann später wiederholt werden, indem Sie im Hauptmenü die Option **10** (Änderungen übernehmen) auswählen. Der IP-Änderungsvorgang ist erst abgeschlossen, wenn alle Vorgänge erfolgreich abgeschlossen wurden.

    - Wenn Sie manuell eingreifen mussten (um beispielsweise einen Knoten neu zu starten) und sicher sind, dass die Aktion, die das Tool für fehlgeschlagen hält, tatsächlich erfolgreich abgeschlossen wurde, geben Sie **f** ein, um sie als erfolgreich zu markieren und mit dem nächsten Vorgang fortzufahren.
13. Laden Sie ein neues Wiederherstellungspaket vom Grid Manager herunter.
    a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
    b. Geben Sie die Bereitstellungspassphrase ein.

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

Ändern Sie die IP-Adressen für alle Knoten im Raster

Wenn Sie die Grid-Netzwerk-IP-Adresse für alle Knoten im Grid ändern müssen, müssen Sie dieses spezielle Verfahren befolgen. Mit dem Verfahren zum Ändern einzelner Knoten können Sie keine netzweite Änderung der Grid-Netzwerk-IP vornehmen.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei.

Um einen erfolgreichen Start des Grids zu gewährleisten, müssen Sie alle Änderungen gleichzeitig vornehmen.

> Dieses Verfahren gilt nur für das Grid-Netzwerk. Sie können dieses Verfahren nicht verwenden, um IP-Adressen in den Admin- oder Client-Netzwerken zu ändern.

Wenn Sie die IP-Adressen und MTU für die Knoten nur an einem Standort ändern möchten, folgen Sie den"Knotennetzwerkkonfiguration ändern" Anweisungen.

Schritte

1. Planen Sie Änderungen, die Sie außerhalb des Tools „IP ändern“ vornehmen müssen, im Voraus, z. B. Änderungen an DNS oder NTP und Änderungen an der Single Sign-On-Konfiguration (SSO), falls verwendet.

   > Wenn die vorhandenen NTP-Server über die neuen IP-Adressen nicht für das Grid zugänglich sind, fügen Sie die neuen NTP-Server hinzu, bevor Sie das Verfahren zum Ändern der IP-Adresse durchführen.

   > Wenn die vorhandenen DNS-Server für das Grid unter den neuen IP-Adressen nicht zugänglich sind, fügen Sie die neuen DNS-Server hinzu, bevor Sie das Verfahren zum Ändern der IP-Adresse durchführen.

   > Wenn SSO für Ihr StorageGRID -System aktiviert ist und alle Vertrauensstellungen der vertrauenden Seite mithilfe von IP-Adressen des Admin-Knotens konfiguriert wurden (anstelle von vollqualifizierten Domänennamen, wie empfohlen), müssen Sie diese Vertrauensstellungen der vertrauenden Seite in Active Directory Federation Services (AD FS) unmittelbar nach der Änderung der IP-Adressen aktualisieren oder neu konfigurieren. Sehen "Konfigurieren der einmaligen Anmeldung" .

   > Fügen Sie bei Bedarf das neue Subnetz für die neuen IP-Adressen hinzu.

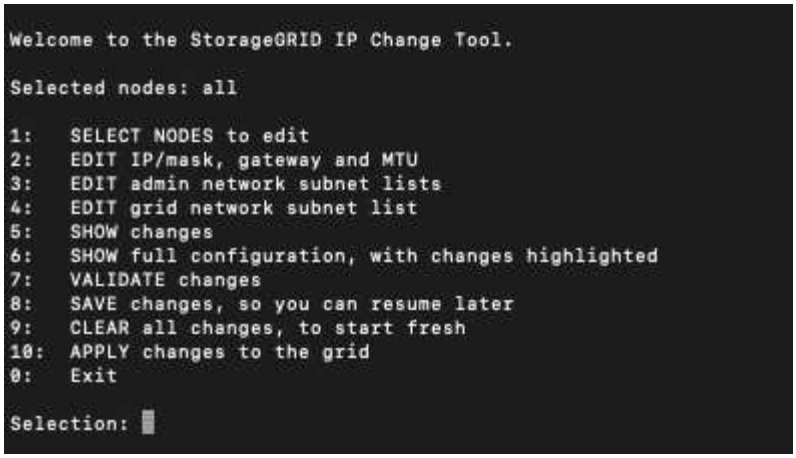
2. Melden Sie sich beim primären Admin-Knoten an:

   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. Starten Sie das Tool „IP ändern“, indem Sie den folgenden Befehl eingeben: `change-ip`
4. Geben Sie bei der Eingabeaufforderung die Bereitstellungspassphrase ein.

   Das Hauptmenü wird angezeigt. Standardmäßig ist die `Selected nodes` Feld ist auf `all` .



5. Wählen Sie im Hauptmenü **2** aus, um die IP-/Subnetzmaske, das Gateway und die MTU-Informationen für alle Knoten zu bearbeiten.

   a. Wählen Sie **1**, um Änderungen am Grid-Netzwerk vorzunehmen.

      Nachdem Sie Ihre Auswahl getroffen haben, zeigt die Eingabeaufforderung die Knotennamen, den Grid-Netzwerknamen, den Datentyp (IP/Maske, Gateway oder MTU) und die aktuellen Werte an.

      Durch Bearbeiten der IP-Adresse, Präfixlänge, des Gateways oder der MTU einer DHCP-konfigurierten Schnittstelle wird die Schnittstelle auf statisch geändert. Vor jeder per DHCP konfigurierten Schnittstelle wird eine Warnung angezeigt.

   Schnittstellen konfiguriert als `fixed` kann nicht bearbeitet werden.

   a. Um einen neuen Wert festzulegen, geben Sie ihn im für den aktuellen Wert angezeigten Format ein.
   b. Nachdem Sie alle Knoten bearbeitet haben, die Sie ändern möchten, geben Sie **q** ein, um zum Hauptmenü zurückzukehren.

      Ihre Änderungen werden zurückgehalten, bis sie gelöscht oder angewendet werden.

6. Überprüfen Sie Ihre Änderungen, indem Sie eine der folgenden Optionen auswählen:
   - **5**: Zeigt Bearbeitungen in der Ausgabe an, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe gezeigt:

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

- **6**: Zeigt Änderungen in der Ausgabe an, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Hinzufügungen) oder rot (Löschungen) hervorgehoben.

> Bestimmte Befehlszeilenschnittstellen zeigen Hinzufügungen und Löschungen möglicherweise durchgestrichen an. Die korrekte Anzeige hängt davon ab, ob Ihr Terminalclient die erforderlichen VT100-Escapesequenzen unterstützt.

7. Wählen Sie Option **7**, um alle Änderungen zu bestätigen.

   Durch diese Validierung wird sichergestellt, dass die Regeln für das Grid-Netzwerk, beispielsweise die Nichtverwendung überlappender Subnetze, nicht verletzt werden.

   In diesem Beispiel hat die Validierung Fehler zurückgegeben.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   In diesem Beispiel wurde die Validierung erfolgreich durchgeführt.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. Wählen Sie nach erfolgreicher Validierung **10** aus, um die neue Netzwerkkonfiguration anzuwenden.
9. Wählen Sie **stage** aus, um die Änderungen beim nächsten Neustart der Knoten anzuwenden.

> Sie müssen **Bühne** auswählen. Führen Sie keinen Rolling Restart durch, weder manuell noch durch Auswahl von **Apply** anstelle von **Stage**; das Grid wird nicht erfolgreich gestartet.

10. Nachdem Sie Ihre Änderungen abgeschlossen haben, wählen Sie **0**, um das Tool „IP ändern“ zu beenden.
11. Fahren Sie alle Knoten gleichzeitig herunter.

> Das gesamte Netz muss heruntergefahren werden, sodass alle Knoten gleichzeitig ausfallen.

12. Nehmen Sie die erforderlichen physischen oder virtuellen Netzwerkänderungen vor.
13. Stellen Sie sicher, dass alle Grid-Knoten ausgefallen sind.
14. Schalten Sie alle Knoten ein.
15. Nach dem erfolgreichen Start des Netzes:
    a. Wenn Sie neue NTP-Server hinzugefügt haben, löschen Sie die alten NTP-Serverwerte.
    b. Wenn Sie neue DNS-Server hinzugefügt haben, löschen Sie die alten DNS-Serverwerte.
16. Laden Sie das neue Wiederherstellungspaket vom Grid Manager herunter.
    a. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
    b. Geben Sie die Bereitstellungspassphrase ein.

Ähnliche Informationen

- "Subnetzlisten im Grid-Netzwerk hinzufügen oder ändern"
- "Grid-Knoten herunterfahren"

Schnittstellen zum vorhandenen Knoten hinzufügen

Linux: Admin- oder Client-Schnittstellen zu einem vorhandenen Knoten hinzufügen

Führen Sie die folgenden Schritte aus, um einem Linux-Knoten nach der Installation eine Schnittstelle im Admin-Netzwerk oder im Client-Netzwerk hinzuzufügen.

Wenn Sie ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET während der Installation nicht in der Knotenkonfigurationsdatei auf dem Linux-Host konfiguriert haben, verwenden Sie dieses Verfahren, um die Schnittstelle hinzuzufügen. Weitere Informationen zur Knotenkonfigurationsdatei finden Sie in den Anweisungen für Ihr Linux-Betriebssystem:

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"

Sie führen dieses Verfahren auf dem Linux-Server aus, auf dem sich der Knoten befindet, der die neue Netzwerkzuweisung benötigt, und nicht innerhalb des Knotens. Bei diesem Verfahren wird dem Knoten nur die Schnittstelle hinzugefügt. Wenn Sie versuchen, andere Netzwerkparameter anzugeben, tritt ein Validierungsfehler auf.

Um Adressinformationen bereitzustellen, müssen Sie das Tool „IP ändern“ verwenden. Sehen

"Knotennetzwerkkonfiguration ändern" .

Schritte

1. Melden Sie sich beim Linux-Server an, auf dem der Knoten gehostet wird.
2. Bearbeiten Sie die Knotenkonfigurationsdatei: `/etc/storagegrid/nodes/node-name.conf` .

   Geben Sie keine anderen Netzwerkparameter an, da sonst ein Validierungsfehler auftritt.

   a. Fügen Sie einen Eintrag für das neue Netzwerkziel hinzu. Beispiel:

   ```
   CLIENT_NETWORK_TARGET = bond0.3206
   ```

   b. Optional: Fügen Sie einen Eintrag für die MAC-Adresse hinzu. Beispiel:

   ```
   CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
   ```

3. Führen Sie den Befehl „Node Validate“ aus:

   ```
   sudo storagegrid node validate node-name
   ```

4. Beheben Sie alle Validierungsfehler.
5. Führen Sie den Befehl zum Neuladen des Knotens aus:

   ```
   sudo storagegrid node reload node-name
   ```

Linux: Trunk oder Zugriffsschnittstellen zu einem Knoten hinzufügen

Sie können einem Linux-Knoten nach der Installation zusätzliche Trunk- oder Zugriffsschnittstellen hinzufügen. Die von Ihnen hinzugefügten Schnittstellen werden auf der Seite „VLAN-Schnittstellen“ und der Seite „HA-Gruppen“ angezeigt.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anweisungen zur Installation von StorageGRID auf Ihrer Linux-Plattform.
  - "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
  - "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- Sie haben die `Passwords.txt` Datei.
- Du hast"spezifische Zugriffsberechtigungen" .

Versuchen Sie nicht, einem Knoten Schnittstellen hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein Erweiterungsverfahren aktiv ist.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um einem Linux-Knoten nach der Installation eine oder mehrere zusätzliche Schnittstellen hinzuzufügen. Sie möchten beispielsweise möglicherweise einem Admin- oder Gateway-Knoten eine Trunk-Schnittstelle hinzufügen, sodass Sie mithilfe von VLAN-Schnittstellen den Datenverkehr verschiedener Anwendungen oder Mandanten trennen können. Oder Sie möchten möglicherweise eine Zugriffsschnittstelle zur Verwendung in einer Hochverfügbarkeitsgruppe (HA) hinzufügen.

Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID

konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt zu einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.

Beim Hinzufügen von Schnittstellen ist der Knoten für kurze Zeit nicht verfügbar. Sie sollten diesen Vorgang jeweils nur auf einem Knoten durchführen.

Schritte

1. Melden Sie sich beim Linux-Server an, auf dem der Knoten gehostet wird.
2. Bearbeiten Sie die Knotenkonfigurationsdatei mit einem Texteditor wie vim oder pico:

   `/etc/storagegrid/nodes/node-name.conf`

3. Fügen Sie der Datei einen Eintrag hinzu, um den Namen und optional die Beschreibung jeder zusätzlichen Schnittstelle anzugeben, die Sie dem Knoten hinzufügen möchten. Verwenden Sie dieses Format.

   `INTERFACE_TARGET_nnnn=value`

   Geben Sie für *nnnn* eine eindeutige Nummer für jeden `INTERFACE_TARGET` Eintrag, den Sie hinzufügen.

   Geben Sie für *Wert* den Namen der physischen Schnittstelle auf dem Bare-Metal-Host an. Fügen Sie dann optional ein Komma hinzu und geben Sie eine Beschreibung der Schnittstelle ein, die auf der Seite „VLAN-Schnittstellen“ und der Seite „HA-Gruppen“ angezeigt wird.

   Beispiel:

   `INTERFACE_TARGET_0001=ens256, Trunk`

   Geben Sie keine anderen Netzwerkparameter an, da sonst ein Validierungsfehler auftritt.

4. Führen Sie den folgenden Befehl aus, um Ihre Änderungen an der Knotenkonfigurationsdatei zu bestätigen:

   `sudo storagegrid node validate node-name`

   Beheben Sie alle Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

5. Führen Sie den folgenden Befehl aus, um die Konfiguration des Knotens zu aktualisieren:

   `sudo storagegrid node reload node-name`

Nach Abschluss

- Wenn Sie eine oder mehrere Trunk-Schnittstellen hinzugefügt haben, gehen Sie zu"VLAN-Schnittstellen konfigurieren" um für jede neue übergeordnete Schnittstelle eine oder mehrere VLAN-Schnittstellen zu konfigurieren.
- Wenn Sie eine oder mehrere Zugriffsschnittstellen hinzugefügt haben, gehen Sie zu"Konfigurieren von Hochverfügbarkeitsgruppen" um die neuen Schnittstellen direkt zu HA-Gruppen hinzuzufügen.

VMware: Trunk- oder Zugriffsschnittstellen zu einem Knoten hinzufügen

Sie können einem VM-Knoten nach der Installation des Knotens einen Trunk oder eine Zugriffsschnittstelle hinzufügen. Die von Ihnen hinzugefügten Schnittstellen werden auf

der Seite „VLAN-Schnittstellen“ und der Seite „HA-Gruppen“ angezeigt.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anleitungen für"Installieren von StorageGRID auf Ihrer VMware-Plattform" .
- Sie verfügen über virtuelle VMware-Maschinen mit Admin-Knoten und Gateway-Knoten.
- Sie haben ein Netzwerk-Subnetz, das nicht als Grid-, Admin- oder Client-Netzwerk verwendet wird.
- Sie haben die `Passwords.txt` Datei.
- Du hast"spezifische Zugriffsberechtigungen" .

> Versuchen Sie nicht, einem Knoten Schnittstellen hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein Erweiterungsverfahren aktiv ist.

Informationen zu diesem Vorgang

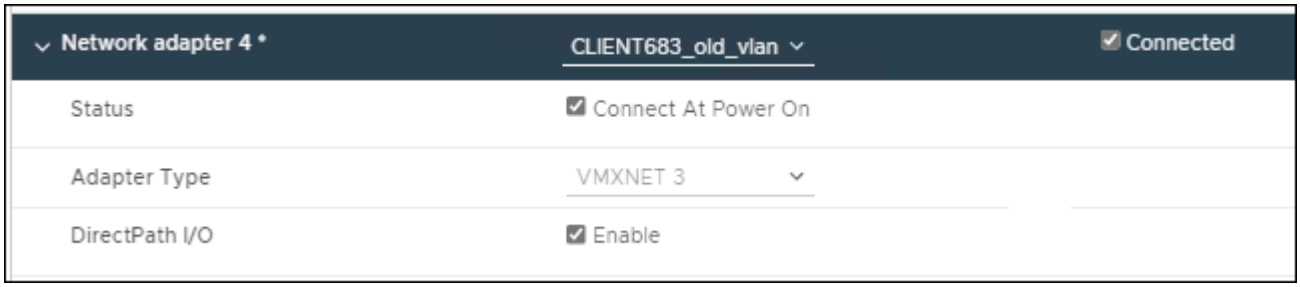
Führen Sie die folgenden Schritte aus, um einem VMware-Knoten nach der Installation des Knotens eine oder mehrere zusätzliche Schnittstellen hinzuzufügen. Sie möchten beispielsweise möglicherweise einem Admin- oder Gateway-Knoten eine Trunk-Schnittstelle hinzufügen, sodass Sie mithilfe von VLAN-Schnittstellen den Datenverkehr verschiedener Anwendungen oder Mandanten trennen können. Oder Sie möchten möglicherweise eine Zugriffsschnittstelle zur Verwendung in einer Hochverfügbarkeitsgruppe (HA) hinzufügen.

Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt zu einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.

Beim Hinzufügen von Schnittstellen ist der Knoten möglicherweise für kurze Zeit nicht verfügbar.

Schritte

1. Fügen Sie in vCenter einem Admin-Knoten und einem Gateway-Knoten-VM einen neuen Netzwerkadapter (Typ VMXNET3) hinzu. Aktivieren Sie die Kontrollkästchen **Verbunden** und **Beim Einschalten verbinden**.



2. Verwenden Sie SSH, um sich beim Admin-Knoten oder Gateway-Knoten anzumelden.
3. Verwenden `ip link show` um zu bestätigen, dass die neue Netzwerkschnittstelle ens256 erkannt wurde.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Nach Abschluss

- Wenn Sie eine oder mehrere Trunk-Schnittstellen hinzugefügt haben, gehen Sie zu"VLAN-Schnittstellen konfigurieren" um für jede neue übergeordnete Schnittstelle eine oder mehrere VLAN-Schnittstellen zu konfigurieren.
- Wenn Sie eine oder mehrere Zugriffsschnittstellen hinzugefügt haben, gehen Sie zu"Konfigurieren von Hochverfügbarkeitsgruppen" um die neuen Schnittstellen direkt zu HA-Gruppen hinzuzufügen.

Konfigurieren von DNS-Servern

Sie können DNS-Server hinzufügen, aktualisieren und entfernen, sodass Sie vollständig qualifizierte Domänennamen (FQDN) als Hostnamen anstelle von IP-Adressen verwenden können.

Um beim Angeben von Hostnamen für externe Ziele vollqualifizierte Domänennamen (FQDNs) anstelle von IP-Adressen zu verwenden, geben Sie die IP-Adresse jedes DNS-Servers an, den Sie verwenden möchten. Diese Einträge werden für AutoSupport, Warn-E-Mails, SNMP-Benachrichtigungen, Plattformdienst-Endpunkte, Cloud-Speicherpools und mehr verwendet.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie müssen die IP-Adressen der DNS-Server konfigurieren.

Informationen zu diesem Vorgang

Um einen ordnungsgemäßen Betrieb sicherzustellen, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, ist es möglich, dass aufgrund bekannter Betriebssystembeschränkungen auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie"Passen Sie die DNS-Serverliste an" für einzelne Knoten (normalerweise alle Knoten an einem Standort), einen anderen Satz von bis zu drei DNS-Servern zu verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein isolierter Standort die FQDNs für externe Ziele auflösen kann.

Hinzufügen eines DNS-Servers

Befolgen Sie diese Schritte, um einen DNS-Server hinzuzufügen.

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **DNS-Server**.
2. Wählen Sie **Weiteren Server hinzufügen**, um einen DNS-Server hinzuzufügen.
3. Wählen Sie **Speichern**.

Ändern eines DNS-Servers

Befolgen Sie diese Schritte, um einen DNS-Server zu ändern.

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **DNS-Server**.
2. Wählen Sie die IP-Adresse des Servernamens aus, den Sie bearbeiten möchten, und nehmen Sie die erforderlichen Änderungen vor.
3. Wählen Sie **Speichern**.

Löschen eines DNS-Servers

Befolgen Sie diese Schritte, um eine IP-Adresse eines DNS-Servers zu löschen.

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **DNS-Server**.
2. Wählen Sie das Löschsymbol neben der IP-Adresse.
3. Wählen Sie **Speichern**.

DNS-Konfiguration für einzelnen Grid-Knoten ändern

Anstatt das DNS global für die gesamte Bereitstellung zu konfigurieren, können Sie ein Skript ausführen, um das DNS für jeden Grid-Knoten anders zu konfigurieren.

Im Allgemeinen sollten Sie zum Konfigurieren von DNS-Servern die Option **WARTUNG** > **Netzwerk** > **DNS-Server** im Grid Manager verwenden. Verwenden Sie das folgende Skript nur, wenn Sie für verschiedene Grid-Knoten unterschiedliche DNS-Server verwenden müssen.

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 `#` .

e. Fügen Sie dem SSH-Agenten den privaten SSH-Schlüssel hinzu. Eingeben: `ssh-add`

f. Geben Sie das SSH-Zugriffskennwort ein, das im `Passwords.txt` Datei.

2. Melden Sie sich bei dem Knoten an, den Sie mit einer benutzerdefinierten DNS-Konfiguration aktualisieren möchten: `ssh node_IP_address`

3. Führen Sie das DNS-Setup-Skript aus: `setup_resolv.rb.`

   Das Skript antwortet mit der Liste der unterstützten Befehle.

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. Fügen Sie die IPv4-Adresse eines Servers hinzu, der den Domänennamendienst für Ihr Netzwerk bereitstellt: `add <nameserver IP_address>`

5. Wiederholen Sie die `add nameserver` Befehl zum Hinzufügen von Nameservern.
6. Befolgen Sie die Anweisungen für andere Befehle.
7. Speichern Sie Ihre Änderungen und beenden Sie die Anwendung: `save`
8. Schließen Sie die Befehlsshell auf dem Server: `exit`
9. Wiederholen Sie für jeden Rasterknoten die Schritte vonAnmelden am Knoten durchSchließen der Befehlsshell .
10. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel aus dem SSH-Agenten. Eingeben: `ssh-add -D`

NTP-Server verwalten

Sie können Network Time Protocol (NTP)-Server hinzufügen, aktualisieren oder entfernen, um sicherzustellen, dass die Daten zwischen den Grid-Knoten in Ihrem StorageGRID System genau synchronisiert werden.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben die Bereitstellungspassphrase.
- Sie müssen die IPv4-Adressen der NTP-Server konfigurieren.

Wie StorageGRID NTP verwendet

Das StorageGRID -System verwendet das Network Time Protocol (NTP), um die Zeit zwischen allen Grid-Knoten im Grid zu synchronisieren.

An jedem Standort wird mindestens zwei Knoten im StorageGRID -System die primäre NTP-Rolle zugewiesen. Sie synchronisieren sich mit mindestens vier und höchstens sechs externen Zeitquellen und untereinander. Jeder Knoten im StorageGRID -System, der kein primärer NTP-Knoten ist, fungiert als NTP-Client und synchronisiert sich mit diesen primären NTP-Knoten.

Die externen NTP-Server stellen eine Verbindung zu den Knoten her, denen Sie zuvor primäre NTP-Rollen zugewiesen haben. Aus diesem Grund wird empfohlen, mindestens zwei Knoten mit primären NTP-Rollen anzugeben.

NTP-Server-Richtlinien

Befolgen Sie diese Richtlinien, um sich vor Zeitproblemen zu schützen:

- Die externen NTP-Server stellen eine Verbindung zu den Knoten her, denen Sie zuvor primäre NTP-Rollen zugewiesen haben. Aus diesem Grund wird empfohlen, mindestens zwei Knoten mit primären NTP-Rollen anzugeben.
- Stellen Sie sicher, dass mindestens zwei Knoten an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn an einem Standort nur ein Knoten die NTP-Quellen erreichen kann, treten bei einem Ausfall dieses Knotens Zeitprobleme auf. Darüber hinaus gewährleistet die Festlegung von zwei Knoten pro Site als primäre NTP-Quellen eine genaue Zeitmessung, wenn eine Site vom Rest des Netzes isoliert ist.
- Die angegebenen externen NTP-Server müssen das NTP-Protokoll verwenden. Sie müssen NTP-

Serverreferenzen von Stratum 3 oder besser angeben, um Probleme mit Zeitabweichungen zu vermeiden.

> Wenn Sie die externe NTP-Quelle für eine StorageGRID Installation auf Produktionsebene angeben, verwenden Sie den Windows-Zeitdienst (W32Time) nicht auf einer Windows-Version vor Windows Server 2016. Der Zeitdienst früherer Windows-Versionen ist nicht genau genug und wird von Microsoft für die Verwendung in Umgebungen mit hoher Genauigkeit, einschließlich StorageGRID, nicht unterstützt. Weitere Einzelheiten finden Sie unter "Supportgrenze zum Konfigurieren des Windows-Zeitdienstes für Umgebungen mit hoher Genauigkeit" .

Konfigurieren von NTP-Servern

Befolgen Sie diese Schritte, um NTP-Server hinzuzufügen, zu aktualisieren oder zu entfernen.

Schritte

1. Wählen Sie **WARTUNG** > **Netzwerk** > **NTP-Server**.
2. Fügen Sie im Abschnitt „Server“ nach Bedarf NTP-Servereinträge hinzu, aktualisieren oder entfernen Sie sie.

   Sie sollten mindestens vier NTP-Server einschließen und können bis zu sechs Server angeben.

3. Geben Sie die Bereitstellungspassphrase für Ihr StorageGRID -System ein und wählen Sie dann **Speichern**.

   Die Seite ist deaktiviert, bis die Konfigurationsaktualisierungen abgeschlossen sind.

   > Wenn alle Ihre NTP-Server den Verbindungstest nicht bestehen, nachdem Sie die neuen NTP-Server gespeichert haben, fahren Sie nicht fort. Wenden Sie sich an den technischen Support.

Beheben von NTP-Serverproblemen

Wenn Probleme mit der Stabilität oder Verfügbarkeit der ursprünglich während der Installation angegebenen NTP-Server auftreten, können Sie die Liste der externen NTP-Quellen, die das StorageGRID -System verwendet, aktualisieren, indem Sie zusätzliche Server hinzufügen oder vorhandene Server aktualisieren oder entfernen.

Wiederherstellen der Netzwerkkonnektivität für isolierte Knoten

Unter bestimmten Umständen können eine oder mehrere Knotengruppen möglicherweise keinen Kontakt zum Rest des Grids herstellen. Beispielsweise können standort- oder netzweite IP-Adressänderungen zu isolierten Knoten führen.

Informationen zu diesem Vorgang

Die Knotenisolation wird durch Folgendes angezeigt:

- Warnungen, wie z. B. **Kommunikation mit Knoten nicht möglich** (**Warnungen** > **Aktuell**)
- Konnektivitätsbezogene Diagnose (**SUPPORT** > **Tools** > **Diagnose**)

Zu den Folgen isolierter Knoten zählen unter anderem die folgenden:

- Wenn mehrere Knoten isoliert sind, können Sie sich möglicherweise nicht beim Grid Manager anmelden oder darauf zugreifen.
- Wenn mehrere Knoten isoliert sind, sind die im Dashboard für den Mandantenmanager angezeigten Werte für Speichernutzung und Kontingent möglicherweise veraltet. Die Gesamtsummen werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

Um das Isolationsproblem zu lösen, führen Sie auf jedem isolierten Knoten oder auf einem Knoten in einer Gruppe (alle Knoten in einem Subnetz, das nicht den primären Admin-Knoten enthält) ein Befehlszeilenprogramm aus, der vom Grid isoliert ist. Das Dienstprogramm stellt den Knoten die IP-Adresse eines nicht isolierten Knotens im Grid zur Verfügung, wodurch der isolierte Knoten oder die Gruppe von Knoten wieder Kontakt zum gesamten Grid aufnehmen kann.

> Wenn das Multicast Domain Name System (mDNS) in den Netzwerken deaktiviert ist, müssen Sie möglicherweise das Befehlszeilenprogramm auf jedem isolierten Knoten ausführen.

Schritte

Dieses Verfahren gilt nicht, wenn nur einige Dienste offline sind oder Kommunikationsfehler melden.

1. Greifen Sie auf den Knoten zu und überprüfen Sie `/var/local/log/dynip.log` für Isolationsmeldungen.

   Beispiel:

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action might be required.
   ```

   Wenn Sie die VMware-Konsole verwenden, enthält diese eine Meldung, dass der Knoten möglicherweise isoliert ist.

   Bei Linux-Bereitstellungen erscheinen Isolationsmeldungen in `/var/log/storagegrid/node/<nodename>.log` Dateien.

2. Wenn die Isolationsmeldungen wiederholt und dauerhaft auftreten, führen Sie den folgenden Befehl aus:

   `add_node_ip.py <address>`

   Wo `<address>` ist die IP-Adresse eines Remote-Knotens, der mit dem Grid verbunden ist.

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. Überprüfen Sie Folgendes für jeden Knoten, der zuvor isoliert wurde:
   - Die Dienste des Knotens wurden gestartet.

- Der Status des Dynamic IP-Dienstes lautet "Wird ausgeführt", nachdem Sie den `storagegrid-status` Befehl.
- Auf der Seite „Knoten“ wird der Knoten nicht mehr als vom Rest des Rasters getrennt angezeigt.

> Wenn Sie den `add_node_ip.py` Wenn der Befehl das Problem nicht löst, können andere Netzwerkprobleme vorliegen, die behoben werden müssen.

Host- und Middleware-Verfahren

Linux: Grid-Knoten auf neuen Host migrieren

Sie können einen oder mehrere StorageGRID Knoten von einem Linux-Host (dem *Quellhost*) auf einen anderen Linux-Host (den *Zielhost*) migrieren, um die Hostwartung durchzuführen, ohne die Funktionalität oder Verfügbarkeit Ihres Grids zu beeinträchtigen.

Beispielsweise möchten Sie möglicherweise einen Knoten migrieren, um Betriebssystem-Patches durchzuführen und einen Neustart durchzuführen.

Bevor Sie beginnen

- Sie haben Ihre StorageGRID -Bereitstellung so geplant, dass sie Migrationsunterstützung umfasst.
  - "Anforderungen für die Node-Container-Migration für Red Hat Enterprise Linux"
  - "Anforderungen für die Node-Containermigration für Ubuntu oder Debian"
- Der Zielhost ist bereits für die Verwendung von StorageGRID vorbereitet.
- Für alle Speichervolumes pro Knoten wird gemeinsam genutzter Speicher verwendet.
- Netzwerkschnittstellen haben auf allen Hosts einheitliche Namen.

> Führen Sie bei einer Produktionsbereitstellung nicht mehr als einen Speicherknoten auf einem einzelnen Host aus. Durch die Verwendung eines dedizierten Hosts für jeden Speicherknoten wird eine isolierte Fehlerdomäne bereitgestellt.
>
> Andere Knotentypen, wie etwa Admin-Knoten oder Gateway-Knoten, können auf demselben Host bereitgestellt werden. Wenn Sie jedoch mehrere Knoten desselben Typs haben (z. B. zwei Gateway-Knoten), installieren Sie nicht alle Instanzen auf demselben Host.

Knoten vom Quellhost exportieren

Fahren Sie als ersten Schritt den Grid-Knoten herunter und exportieren Sie ihn vom Linux-Quellhost.

Führen Sie die folgenden Befehle auf dem *Quellhost* aus.

Schritte

1. Rufen Sie den Status aller Knoten ab, die derzeit auf dem Quellhost ausgeführt werden.

   ```
   sudo storagegrid node status all
   ```

   Beispielausgabe:

```
Name Config-State Run-State
DC1-ADM1 Configured Running
DC1-ARC1 Configured Running
DC1-GW1 Configured Running
DC1-S1 Configured Running
DC1-S2 Configured Running
DC1-S3 Configured Running
```

2. Identifizieren Sie den Namen des Knotens, den Sie migrieren möchten, und stoppen Sie ihn, wenn sein Ausführungsstatus „Ausführen“ lautet.

   ```
   sudo storagegrid node stop DC1-S3
   ```

   Beispielausgabe:

   ```
   Stopping node DC1-S3
   Waiting up to 630 seconds for node shutdown
   ```

3. Exportieren Sie den Knoten vom Quellhost.

   ```
   sudo storagegrid node export DC1-S3
   ```

   Beispielausgabe:

   ```
   Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
   Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
   want to import it again.
   ```

4. Notieren Sie sich die `import` in der Ausgabe vorgeschlagener Befehl.

   Sie führen diesen Befehl im nächsten Schritt auf dem Zielhost aus.

Knoten auf Zielhost importieren

Nachdem Sie den Knoten vom Quellhost exportiert haben, importieren und validieren Sie den Knoten auf dem Zielhost. Durch die Validierung wird bestätigt, dass der Knoten Zugriff auf dieselben Blockspeicher- und Netzwerkschnittstellengeräte hat wie auf dem Quellhost.

Führen Sie die folgenden Befehle auf dem *Zielhost* aus.

Schritte

1. Importieren Sie den Knoten auf dem Zielhost.

   ```
   sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
   ```

   Beispielausgabe:

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
You should run 'storagegrid node validate DC1-S3'
```

2. Validieren Sie die Knotenkonfiguration auf dem neuen Host.

   ```
   sudo storagegrid node validate DC1-S3
   ```

   Beispielausgabe:

   ```
   Confirming existence of node DC1-S3... PASSED
   Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
   DC1-S3... PASSED
   Checking for duplication of unique values... PASSED
   ```

3. Wenn Validierungsfehler auftreten, beheben Sie diese, bevor Sie den migrierten Knoten starten.

   Informationen zur Fehlerbehebung finden Sie in den StorageGRID -Installationsanweisungen für Ihr Linux-Betriebssystem.

   - "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
   - "Installieren Sie StorageGRID unter Ubuntu oder Debian"

Migrierten Knoten starten

Nachdem Sie den migrierten Knoten validiert haben, starten Sie den Knoten, indem Sie einen Befehl auf dem *Zielhost* ausführen.

Schritte

1. Starten Sie den Knoten auf dem neuen Host.

   ```
   sudo storagegrid node start DC1-S3
   ```

2. Sign in und überprüfen Sie, ob der Status des Knotens grün ist und keine Warnung vorliegt.

   > Durch die Überprüfung, ob der Status des Knotens grün ist, wird sichergestellt, dass der migrierte Knoten vollständig neu gestartet wurde und sich wieder dem Grid angeschlossen hat. Wenn der Status nicht grün ist, migrieren Sie keine weiteren Knoten, damit nicht mehr als ein Knoten außer Betrieb ist.

3. Wenn Sie nicht auf den Grid Manager zugreifen können, warten Sie 10 Minuten und führen Sie dann den folgenden Befehl aus:

   ```
   sudo storagegrid node status _node-name
   ```

   Bestätigen Sie, dass der migrierte Knoten den Ausführungsstatus „Wird ausgeführt“ hat.

VMware: Virtuelle Maschine für automatischen Neustart konfigurieren

Wenn die virtuelle Maschine nach dem Neustart von VMware vSphere Hypervisor nicht neu gestartet wird, müssen Sie die virtuelle Maschine möglicherweise für den automatischen Neustart konfigurieren.

Sie sollten dieses Verfahren durchführen, wenn Sie feststellen, dass eine virtuelle Maschine nicht neu gestartet wird, während Sie einen Grid-Knoten wiederherstellen oder ein anderes Wartungsverfahren durchführen.

Schritte

1. Wählen Sie in der VMware vSphere-Clientstruktur die virtuelle Maschine aus, die nicht gestartet ist.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einschalten**.
3. Konfigurieren Sie VMware vSphere Hypervisor so, dass die virtuelle Maschine in Zukunft automatisch neu gestartet wird.

Knoten wiederherstellen oder ersetzen

Warnungen und Hinweise zur Wiederherstellung von Grid-Knoten

Wenn ein Grid-Knoten ausfällt, müssen Sie ihn so schnell wie möglich wiederherstellen. Sie müssen alle Warnungen und Hinweise zur Knotenwiederherstellung lesen, bevor Sie beginnen.

> StorageGRID ist ein verteiltes System, das aus mehreren Knoten besteht, die miteinander arbeiten. Verwenden Sie keine Festplatten-Snapshots, um Grid-Knoten wiederherzustellen. Lesen Sie stattdessen die Wiederherstellungs- und Wartungsverfahren für jeden Knotentyp.

> Wenn eine gesamte StorageGRID -Site ausgefallen ist, wenden Sie sich an den technischen Support. Der technische Support arbeitet mit Ihnen zusammen, um einen Site-Wiederherstellungsplan zu entwickeln und umzusetzen, der die wiederherzustellende Datenmenge maximiert und Ihre Geschäftsziele erfüllt. Sehen "So stellt der technische Support eine Site wieder her" .

Zu den Gründen für die schnellstmögliche Wiederherstellung eines ausgefallenen Grid-Knotens gehören unter anderem die folgenden:

- Ein ausgefallener Grid-Knoten kann die Redundanz von System- und Objektdaten verringern, sodass Sie dem Risiko eines dauerhaften Datenverlusts ausgesetzt sind, wenn ein anderer Knoten ausfällt.
- Ein ausgefallener Netzknoten kann die Effizienz des täglichen Betriebs beeinträchtigen.
- Ein ausgefallener Grid-Knoten kann Ihre Fähigkeit zur Überwachung des Systembetriebs einschränken.
- Ein ausgefallener Grid-Knoten kann einen internen Serverfehler 500 verursachen, wenn strenge ILM-Regeln gelten.
- Wenn ein Grid-Knoten nicht umgehend wiederhergestellt wird, kann sich die Wiederherstellungszeit verlängern. Beispielsweise können sich Warteschlangen bilden, die vor Abschluss der Wiederherstellung gelöscht werden müssen.

Befolgen Sie immer das Wiederherstellungsverfahren für den spezifischen Typ des Grid-Knotens, den Sie wiederherstellen. Die Wiederherstellungsverfahren variieren für primäre und nicht primäre Admin-Knoten, Gateway-Knoten, Appliance-Knoten und Speicherknoten.

Voraussetzungen für die Wiederherstellung von Netzknoten

Bei der Wiederherstellung von Grid-Knoten werden alle der folgenden Bedingungen vorausgesetzt:

- Die ausgefallene physische oder virtuelle Hardware wurde ersetzt und konfiguriert.
- Die Version des StorageGRID Appliance Installers auf dem Ersatzgerät entspricht der Softwareversion Ihres StorageGRID -Systems, wie in beschrieben "Überprüfen und aktualisieren Sie die Version des StorageGRID Appliance Installer" .
- Wenn Sie einen anderen Grid-Knoten als den primären Admin-Knoten wiederherstellen, besteht eine Verbindung zwischen dem wiederherzustellenden Grid-Knoten und dem primären Admin-Knoten.
- Wenn Sie einen Appliance-Speicherknoten wiederherstellen, müssen Sie während der Appliance-

Installation denselben Speichertyp wie bei der ursprünglichen Appliance angeben (Kombiniert, Nur Metadaten oder Nur Daten). Wenn Sie einen anderen Speichertyp angeben, schlägt die Wiederherstellung fehl und erfordert eine Neuinstallation der Appliance mit dem richtigen angegebenen Speichertyp.

Reihenfolge der Knotenwiederherstellung, wenn ein Server, auf dem mehr als ein Grid-Knoten gehostet wird, ausfällt

Wenn ein Server ausfällt, auf dem mehr als ein Grid-Knoten gehostet wird, können Sie die Knoten in beliebiger Reihenfolge wiederherstellen. Wenn der ausgefallene Server jedoch den primären Admin-Knoten hostet, müssen Sie diesen Knoten zuerst wiederherstellen. Durch die Wiederherstellung des primären Admin-Knotens wird zunächst verhindert, dass die Wiederherstellung anderer Knoten angehalten wird, während diese auf die Kontaktaufnahme mit dem primären Admin-Knoten warten.

IP-Adressen für wiederhergestellte Knoten

Versuchen Sie nicht, einen Knoten mit einer IP-Adresse wiederherzustellen, die derzeit einem anderen Knoten zugewiesen ist. Wenn Sie den neuen Knoten bereitstellen, verwenden Sie die aktuelle IP-Adresse des ausgefallenen Knotens oder eine nicht verwendete IP-Adresse.

Wenn Sie zum Bereitstellen des neuen Knotens eine neue IP-Adresse verwenden und den Knoten dann wiederherstellen, wird die neue IP-Adresse weiterhin für den wiederhergestellten Knoten verwendet. Wenn Sie zur ursprünglichen IP-Adresse zurückkehren möchten, verwenden Sie nach Abschluss der Wiederherstellung das Tool „IP ändern“.

Sammeln Sie die erforderlichen Materialien für die Wiederherstellung des Netzknotens

Bevor Sie Wartungsarbeiten durchführen, müssen Sie sicherstellen, dass Sie über die erforderlichen Materialien verfügen, um einen ausgefallenen Grid-Knoten wiederherzustellen.

Artikel	Hinweise
StorageGRID -Installationsarchiv	Wenn Sie einen Grid-Knoten wiederherstellen müssen, müssen SieLaden Sie die StorageGRID Installationsdateien herunter für Ihre Plattform. **Hinweis:** Sie müssen keine Dateien herunterladen, wenn Sie ausgefallene Speichervolumes auf einem Speicherknoten wiederherstellen.
Service-Laptop	Der Dienstlaptop muss über folgendes verfügen: • Netzwerkanschluss • SSH-Client (z. B. PuTTY) • "Unterstützte Webbrowser"

Artikel	Hinweise
Wiederherstellungspaket `.zip` Datei	Erhalten Sie eine Kopie des aktuellsten Wiederherstellungspakets `.zip` Datei: `sgws-recovery-package-id-revision.zip` Der Inhalt der `.zip` Die Datei wird bei jeder Änderung des Systems aktualisiert. Sie werden angewiesen, nach der Durchführung solcher Änderungen die aktuellste Version des Wiederherstellungspakets an einem sicheren Ort aufzubewahren. Verwenden Sie zur Wiederherstellung nach Netzausfällen die aktuellste Kopie. Wenn der primäre Admin-Knoten normal funktioniert, können Sie das Wiederherstellungspaket vom Grid Manager herunterladen. Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**. Wenn Sie nicht auf den Grid Manager zugreifen können, finden Sie verschlüsselte Kopien des Wiederherstellungspakets auf einigen Speicherknoten, die den ADC-Dienst enthalten. Suchen Sie auf jedem Speicherknoten an diesem Speicherort nach dem Wiederherstellungspaket: `/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg` Verwenden Sie das Wiederherstellungspaket mit der höchsten Revisionsnummer.
`Passwords.txt`Datei	Enthält die Passwörter, die für den Zugriff auf Grid-Knoten über die Befehlszeile erforderlich sind. Im Wiederherstellungspaket enthalten.
Bereitstellungspassphrase	Die Passphrase wird bei der Erstinstallation des StorageGRID -Systems erstellt und dokumentiert. Die Bereitstellungspassphrase ist nicht in der `Passwords.txt` Datei.
Aktuelle Dokumentation für Ihre Plattform	Gehen Sie für die Dokumentation auf die Website des Plattformanbieters. Die aktuell unterstützten Versionen Ihrer Plattform finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Laden Sie die Software herunter und extrahieren Sie die Dateien, es sei denn, Sie sind"Wiederherstellen ausgefallener Speichervolumes auf einem Speicherknoten" .

Sie müssen die Version von StorageGRID verwenden, die derzeit im Grid ausgeführt wird.

Schritte

1. Ermitteln Sie, welche Version der Software aktuell installiert ist. Wählen Sie oben im Grid Manager das Hilfesymbol und dann **Info** aus.
2. Gehen Sie zum "NetApp -Downloadseite für StorageGRID" .
3. Wählen Sie die Version von StorageGRID aus, die derzeit im Grid ausgeführt wird.

Die Softwareversionen von StorageGRID haben dieses Format: `11.x.y` .

4. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Ihr NetApp -Konto an .
5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.
6. Wählen Sie in der Spalte **Install StorageGRID** der Download-Seite die `.tgz` oder `.zip` Datei für Ihre Plattform.

   Die in der Installationsarchivdatei angezeigte Version muss mit der Version der aktuell installierten Software übereinstimmen.

   Verwenden Sie die `.zip` Datei, wenn Sie Windows verwenden.

Plattform	Installationsarchiv
Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu oder Debian oder Appliances	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

7. Laden Sie die Archivdatei herunter und extrahieren Sie sie.
8. Befolgen Sie die entsprechenden Schritte für Ihre Plattform, um die benötigten Dateien basierend auf Ihrer Plattform und den Grid-Knoten auszuwählen, die Sie wiederherstellen müssen.

   Die im Schritt für jede Plattform aufgeführten Pfade beziehen sich auf das von der Archivdatei installierte Verzeichnis der obersten Ebene.

9. Wenn Sie eine"Red Hat Enterprise Linux-System" , wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet.
	RPM-Paket zum Installieren der StorageGRID -Knotenimages auf Ihren RHEL-Hosts.
	RPM-Paket zum Installieren des StorageGRID Hostdienstes auf Ihren RHEL-Hosts.
Bereitstellungsskripttool	Beschreibung

Pfad und Dateiname	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Beispiel für eine Ansible-Rolle und ein Playbook zum Konfigurieren von RHEL-Hosts für die Bereitstellung von StorageGRID Containern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

1. Wenn Sie eine"Ubuntu- oder Debian-System" , wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine nicht für die Produktion NetApp -Lizenzdatei, die Sie für Tests und Proof-of-Concept-Bereitstellungen verwenden können.
	DEB-Paket zum Installieren der StorageGRID -Knotenimages auf Ubuntu- oder Debian-Hosts.
	MD5-Prüfsumme für die Datei `/debs/storagegrid-webscale-images-version-SHA.deb` .
	DEB-Paket zum Installieren des StorageGRID -Hostdienstes auf Ubuntu- oder Debian-Hosts.
Bereitstellungsskripttool	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Beispiel für eine Ansible-Rolle und ein Playbook zum Konfigurieren von Ubuntu- oder Debian-Hosts für die Bereitstellung von StorageGRID Containern. Sie können die Rolle oder das Playbook nach Bedarf anpassen.

Pfad und Dateiname	Beschreibung
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

1. Wenn Sie eine"VMware-System" , wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID Downloaddatei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Anspruch auf Support für das Produkt bietet.
	Die Festplattendatei der virtuellen Maschine, die als Vorlage zum Erstellen virtueller Grid-Knotenmaschinen verwendet wird.
	Die Open Virtualization Format-Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen des primären Admin-Knotens.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen nicht primärer Admin-Knoten.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Gateway-Knoten.
	Die Vorlagendatei(`.ovf`) und Manifestdatei(`.mf`) zum Bereitstellen von Speicherknoten auf Basis virtueller Maschinen.

Pfad und Dateiname	Beschreibung
Bereitstellungsskripttool	Beschreibung
	Ein Bash-Shell-Skript zur Automatisierung der Bereitstellung virtueller Grid-Knoten.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `deploy-vsphere-ovftool.sh` Skript.
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID -Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Geräten.
	Ein Beispiel-Python-Skript, das Sie verwenden können, um sich bei der Grid Management API anzumelden, wenn Single Sign-On (SSO) aktiviert ist. Sie können dieses Skript auch für die Ping Federate-Integration verwenden.
	Eine Beispielkonfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Eine leere Konfigurationsdatei zur Verwendung mit dem `configure-storagegrid.py` Skript.
	Ein Beispiel-Python-Skript, das Sie zum Anmelden bei der Grid Management API verwenden können, wenn Single Sign-On (SSO) mit Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfsskript, das vom Begleiter aufgerufen wird `storagegrid-ssoauth-azure.py` Python-Skript zum Durchführen von SSO-Interaktionen mit Azure.
	API-Schemas für StorageGRID. **Hinweis**: Bevor Sie ein Upgrade durchführen, können Sie diese Schemata verwenden, um zu bestätigen, dass der gesamte Code, den Sie zur Verwendung der StorageGRID Verwaltungs-APIs geschrieben haben, mit der neuen StorageGRID Version kompatibel ist, wenn Sie keine nicht produktive StorageGRID Umgebung zum Testen der Upgrade-Kompatibilität haben.

1. Wenn Sie ein auf einem StorageGRID -Gerät basierendes System wiederherstellen, wählen Sie die

entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	DEB-Paket zum Installieren der StorageGRID -Knotenimages auf Ihren Geräten.
	MD5-Prüfsumme für die Datei `/debs/storagegridwebscale-images-version-SHA.deb` .

Für die Installation der Appliance sind diese Dateien nur erforderlich, wenn Sie Netzwerkverkehr vermeiden müssen. Das Gerät kann die erforderlichen Dateien vom primären Admin-Knoten herunterladen.

Verfahren zur Knotenwiederherstellung auswählen

Sie müssen das richtige Wiederherstellungsverfahren für den Typ des ausgefallenen Knotens auswählen.

Rasterknoten	Wiederherstellungsverfahren
Mehr als ein Speicherknoten	Wenden Sie sich an den technischen Support. Wenn mehr als ein Speicherknoten ausgefallen ist, muss der technische Support bei der Wiederherstellung helfen, um Datenbankinkonsistenzen zu vermeiden, die zu Datenverlust führen könnten. Möglicherweise ist ein Site-Wiederherstellungsverfahren erforderlich. "So stellt der technische Support eine Site wieder her"
Ein einzelner Speicherknoten	Das Wiederherstellungsverfahren für den Speicherknoten hängt von der Art und Dauer des Fehlers ab. "Wiederherstellung nach Speicherknotenfehlern"
Admin-Knoten	Das Admin-Knoten-Verfahren hängt davon ab, ob Sie den primären Admin-Knoten oder einen nicht primären Admin-Knoten wiederherstellen müssen. "Wiederherstellung nach Admin-Knoten-Fehlern"
Gateway-Knoten	"Wiederherstellung nach Gateway-Knotenfehlern"
Archivknoten	"Wiederherstellung nach Archivknotenfehlern (StorageGRID 11.8-Dokumentationssite)"

Wenn ein Server ausfällt, auf dem mehr als ein Grid-Knoten gehostet wird, können Sie die Knoten in beliebiger Reihenfolge wiederherstellen. Wenn der ausgefallene Server jedoch den primären Admin-Knoten hostet, müssen Sie diesen Knoten zuerst wiederherstellen. Durch die Wiederherstellung des primären Admin-Knotens wird zunächst verhindert, dass die Wiederherstellung anderer Knoten angehalten wird, während diese auf die Kontaktaufnahme mit dem primären Admin-Knoten warten.

Wiederherstellung nach Speicherknotenfehlern

Wiederherstellung nach Speicherknotenfehlern

Das Verfahren zur Wiederherstellung eines ausgefallenen Speicherknotens hängt von der Art des Fehlers und dem Typ des ausgefallenen Speicherknotens ab.

Verwenden Sie diese Tabelle, um das Wiederherstellungsverfahren für einen ausgefallenen Speicherknoten auszuwählen.

Ausgabe	Aktion	Hinweise
• Mehr als ein Speicherknoten ist ausgefallen. • Ein zweiter Speicherknoten ist weniger als 15 Tage nach einem Speicherknotenausfall oder einer Wiederherstellung ausgefallen. Dies gilt auch für den Fall, dass ein Speicherknoten ausfällt, während die Wiederherstellung eines anderen Speicherknotens noch läuft.	Wenden Sie sich an den technischen Support.	Die Wiederherstellung von mehr als einem Speicherknoten (oder mehr als einem Speicherknoten innerhalb von 15 Tagen) kann die Integrität der Cassandra-Datenbank beeinträchtigen, was zu Datenverlust führen kann. Der technische Support kann feststellen, wann die Wiederherstellung eines zweiten Speicherknotens sicher beginnen kann. **Hinweis**: Wenn an einem Standort mehr als ein Speicherknoten ausfällt, der den ADC-Dienst enthält, gehen alle ausstehenden Plattformdienstanforderungen für diesen Standort verloren.
An einem Standort ist mehr als ein Speicherknoten ausgefallen oder ein ganzer Standort ist ausgefallen.	Wenden Sie sich an den technischen Support. Möglicherweise muss ein Site-Wiederherstellungsverfahren durchgeführt werden.	Der technische Support wird Ihre Situation beurteilen und einen Wiederherstellungsplan entwickeln. Sehen "So stellt der technische Support eine Site wieder her" .
Ein Appliance-Speicherknoten ist ausgefallen.	"Wiederherstellen des Appliance-Speicherknotens"	Das Wiederherstellungsverfahren für Appliance-Speicherknoten ist bei allen Fehlern gleich.

Ausgabe	Aktion	Hinweise
Ein oder mehrere Speichervolumes sind ausgefallen, aber das Systemlaufwerk ist intakt	"Wiederherstellung nach einem Speichervolume-Fehler, wenn das Systemlaufwerk intakt ist"	Dieses Verfahren wird für softwarebasierte Storage Nodes verwendet.
Das Systemlaufwerk ist ausgefallen.	"Wiederherstellung nach einem Systemlaufwerksfehler"	Das Verfahren zum Ersetzen des Knotens hängt von der Bereitstellungsplattform und davon ab, ob auch Speichervolumes ausgefallen sind.

Einige StorageGRID Wiederherstellungsverfahren verwenden Reaper zur Durchführung von Cassandra-Reparaturen. Reparaturen erfolgen automatisch, sobald die entsprechenden bzw. erforderlichen Leistungen begonnen haben. Möglicherweise bemerken Sie eine Skriptausgabe, in der „Reaper“ oder „Cassandra-Reparatur“ erwähnt wird. Wenn eine Fehlermeldung angezeigt wird, die darauf hinweist, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

Wiederherstellen des Appliance-Speicherknotens

Warnungen zur Wiederherstellung von Appliance-Speicherknoten

Das Verfahren zum Wiederherstellen eines ausgefallenen StorageGRID -Geräte -Speicherknotens ist dasselbe, unabhängig davon, ob Sie die Wiederherstellung nach dem Verlust des Systemlaufwerks oder nur nach dem Verlust von Speichervolumes durchführen.

Wenn mehr als ein Speicherknoten ausgefallen ist (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es könnte zu Datenverlust kommen.

Wenn dies der zweite Speicherknotenausfall innerhalb von weniger als 15 Tagen nach einem Speicherknotenausfall oder einer Wiederherstellung ist, wenden Sie sich an den technischen Support. Der Wiederaufbau von Cassandra auf zwei oder mehr Speicherknoten innerhalb von 15 Tagen kann zu Datenverlust führen.

Wenn an einem Standort mehr als ein Speicherknoten ausgefallen ist, ist möglicherweise ein Standortwiederherstellungsverfahren erforderlich. Sehen "So stellt der technische Support eine Site wieder her" .

Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und die Kopie auf einem ausgefallenen Speichervolume vorhanden ist, können Sie das Objekt nicht wiederherstellen.

Informationen zur Hardware-Wartung, wie z. B. Anweisungen zum Austausch eines Controllers oder zur Neuinstallation von SANtricity OS, finden Sie im "Wartungsanweisungen für Ihr Speichergerät" .

Bereiten Sie den Speicherknoten des Geräts für die Neuinstallation vor

Wenn Sie einen Appliance-Speicherknoten wiederherstellen, müssen Sie die Appliance zunächst für die Neuinstallation der StorageGRID -Software vorbereiten.

Schritte

1. Melden Sie sich beim ausgefallenen Speicherknoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Bereiten Sie den Storage Node des Geräts für die Installation der StorageGRID -Software vor. `sgareinstall`

3. Wenn Sie aufgefordert werden, fortzufahren, geben Sie Folgendes ein: `y`

   Das Gerät wird neu gestartet und Ihre SSH-Sitzung wird beendet. Normalerweise dauert es etwa 5 Minuten, bis das StorageGRID Appliance Installer verfügbar ist. In einigen Fällen kann es jedoch bis zu 30 Minuten dauern.

   > Versuchen Sie nicht, den Neustart durch Aus- und Wiedereinschalten des Geräts oder durch anderweitiges Zurücksetzen zu beschleunigen. Sie könnten automatische BIOS-, BMC oder andere Firmware-Upgrades unterbrechen.

   Der Storage Node des StorageGRID -Geräts wird zurückgesetzt und auf die Daten auf dem Storage Node kann nicht mehr zugegriffen werden. Während des ursprünglichen Installationsvorgangs konfigurierte IP-Adressen sollten erhalten bleiben. Es wird jedoch empfohlen, dies nach Abschluss des Vorgangs zu bestätigen.

   Nach der Ausführung des `sgareinstall` Befehl werden alle von StorageGRID bereitgestellten Konten, Kennwörter und SSH-Schlüssel entfernt und neue Hostschlüssel generiert.

Starten Sie die Installation der StorageGRID -Appliance

Um StorageGRID auf einem Appliance-Speicherknoten zu installieren, verwenden Sie den StorageGRID Appliance Installer, der auf der Appliance enthalten ist.

Bevor Sie beginnen

- Das Gerät wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Netzwerkverbindungen und IP-Adressen wurden für das Gerät mithilfe des StorageGRID Appliance Installer konfiguriert.
- Sie kennen die IP-Adresse des primären Admin-Knotens für das StorageGRID Grid.
- Alle auf der IP-Konfigurationsseite des StorageGRID Appliance Installer aufgeführten Grid-Netzwerk-Subnetze wurden in der Grid-Netzwerk-Subnetzliste auf dem primären Admin-Knoten definiert.
- Sie haben diese erforderlichen Aufgaben abgeschlossen, indem Sie die Installationsanweisungen für Ihr

Speichergerät befolgt haben. Sehen "Schnellstart für die Hardwareinstallation" .

- Sie verwenden eine"unterstützter Webbrowser" .
- Sie kennen eine der dem Compute-Controller im Gerät zugewiesenen IP-Adressen. Sie können die IP-Adresse für das Admin-Netzwerk (Verwaltungsport 1 am Controller), das Grid-Netzwerk oder das Client-Netzwerk verwenden.

Informationen zu diesem Vorgang

So installieren Sie StorageGRID auf einem Appliance-Speicherknoten:

- Sie geben die IP-Adresse des primären Admin-Knotens und den Hostnamen (Systemnamen) des Knotens an oder bestätigen diese.
- Sie starten die Installation und warten, während die Volumes konfiguriert und die Software installiert wird.

> Wenn Sie einen Appliance-Speicherknoten wiederherstellen, installieren Sie ihn mit demselben Speichertyp wie die ursprüngliche Appliance neu (Kombiniert, Nur Metadaten oder Nur Daten). Wenn Sie einen anderen Speichertyp angeben, schlägt die Wiederherstellung fehl und erfordert eine Neuinstallation der Appliance mit dem richtigen angegebenen Speichertyp.

- Während des Vorgangs wird die Installation unterbrochen. Um die Installation fortzusetzen, müssen Sie sich beim Grid Manager anmelden und den ausstehenden Speicherknoten als Ersatz für den ausgefallenen Knoten konfigurieren.
- Nachdem Sie den Knoten konfiguriert haben, wird der Installationsprozess der Appliance abgeschlossen und die Appliance neu gestartet.

Schritte

1. Öffnen Sie einen Browser und geben Sie eine der IP-Adressen für den Compute Controller im Gerät ein.

   `https://Controller_IP:8443`

   Die Startseite des StorageGRID Appliance-Installationsprogramms wird angezeigt.

2. Legen Sie im Abschnitt „Verbindung zum primären Admin-Knoten“ fest, ob Sie die IP-Adresse für den primären Admin-Knoten angeben müssen.

   Das StorageGRID Appliance Installer kann diese IP-Adresse automatisch erkennen, vorausgesetzt, der primäre Admin-Knoten oder mindestens ein anderer Grid-Knoten mit konfigurierter ADMIN_IP ist im selben Subnetz vorhanden.

3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

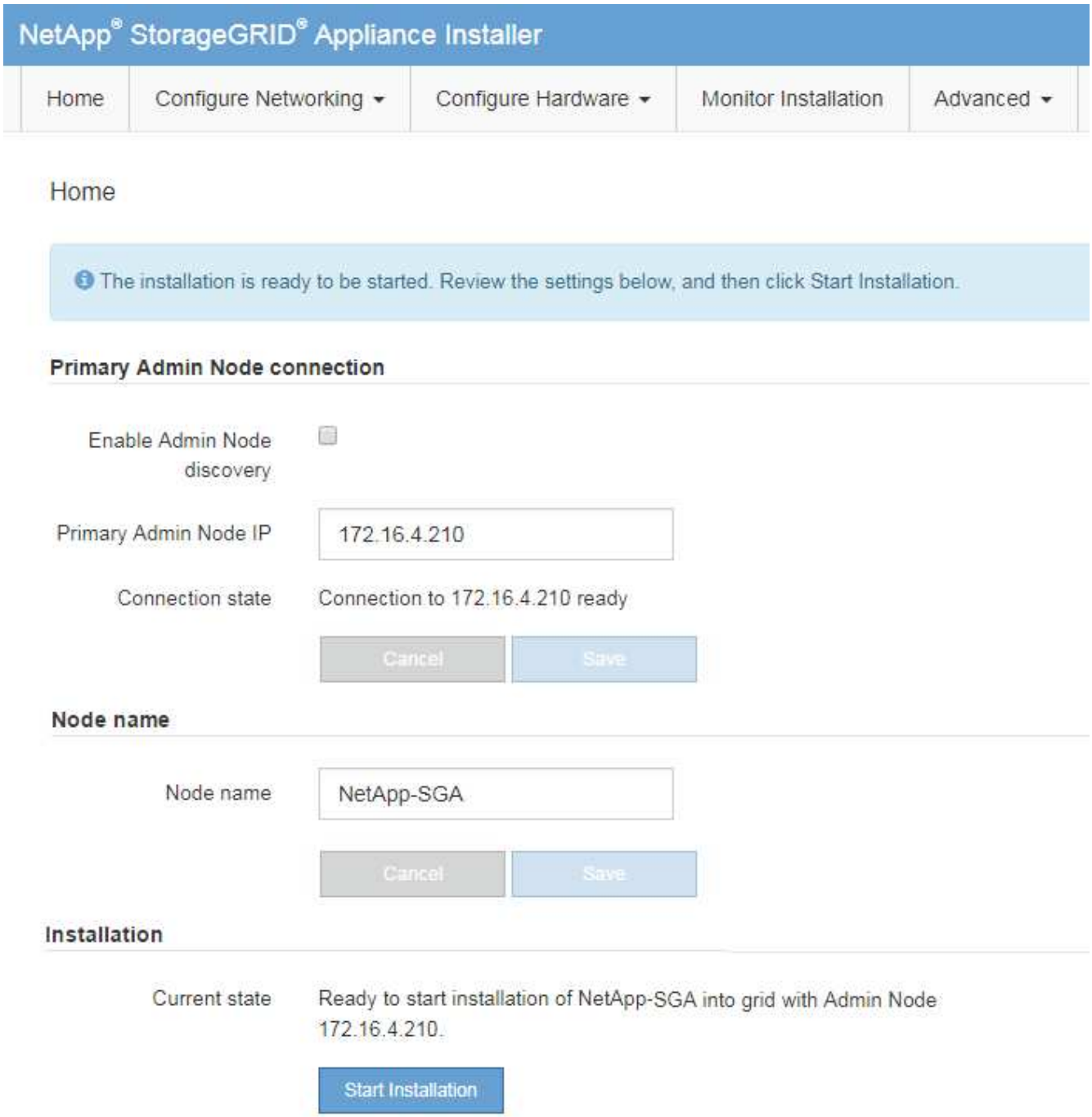
Option	Schritte
Manuelle IP-Eingabe	a. Deaktivieren Sie das Kontrollkästchen **Admin-Knotenerkennung aktivieren**. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie auf **Speichern**. d. Warten Sie, bis der Verbindungsstatus für die neue IP-Adresse „Bereit“ lautet.

Option	Schritte
Automatische Erkennung aller verbundenen primären Admin-Knoten	a. Aktivieren Sie das Kontrollkästchen **Admin-Knotenerkennung aktivieren**. b. Wählen Sie aus der Liste der erkannten IP-Adressen den primären Admin-Knoten für das Grid aus, in dem dieser Appliance-Speicherknoten bereitgestellt wird. c. Klicken Sie auf **Speichern**. d. Warten Sie, bis der Verbindungsstatus für die neue IP-Adresse „Bereit“ lautet.

4. Geben Sie im Feld **Knotenname** denselben Hostnamen (Systemnamen) ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.
5. Bestätigen Sie im Abschnitt Installation, dass der aktuelle Status „Bereit zum Starten der Installation von `node name` in das Grid mit dem primären Admin-Knoten „*admin_ip*“ und dass die Schaltfläche „Installation starten“ aktiviert ist.

   Wenn die Schaltfläche **Installation starten** nicht aktiviert ist, müssen Sie möglicherweise die Netzwerkkonfiguration oder die Porteinstellungen ändern. Anweisungen hierzu finden Sie in der Wartungsanleitung Ihres Geräts.

6. Klicken Sie auf der Startseite des StorageGRID Appliance Installer auf **Installation starten**.



Der aktuelle Status ändert sich in „Installation läuft“ und die Seite „Monitorinstallation“ wird angezeigt.

Wenn Sie manuell auf die Seite „Monitorinstallation“ zugreifen müssen, klicken Sie in der Menüleiste auf „Monitorinstallation“. Sehen "Überwachen Sie die Installation der Appliance" .

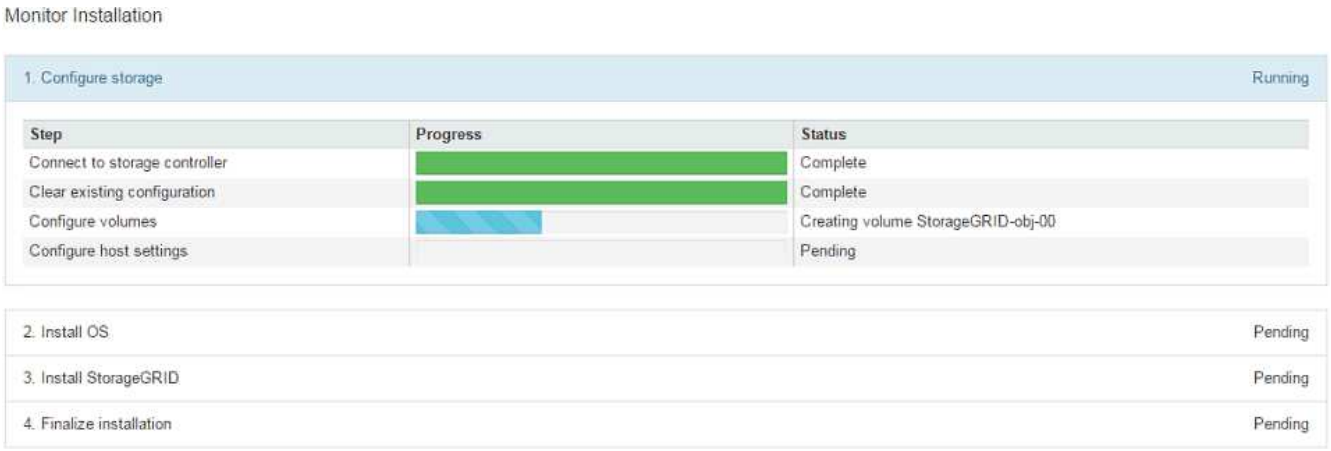
Überwachen Sie die Installation der StorageGRID -Appliance

Der StorageGRID Appliance Installer zeigt den Status an, bis die Installation abgeschlossen ist. Wenn die Softwareinstallation abgeschlossen ist, wird das Gerät neu gestartet.

Schritte

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

   Auf der Seite „Installation überwachen“ wird der Installationsfortschritt angezeigt.



   Die blaue Statusleiste zeigt an, welche Aufgabe gerade ausgeführt wird. Grüne Statusbalken zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.

   > Das Installationsprogramm stellt sicher, dass Aufgaben, die bei einer vorherigen Installation abgeschlossen wurden, nicht erneut ausgeführt werden. Wenn Sie eine Installation erneut ausführen, werden alle Aufgaben, die nicht erneut ausgeführt werden müssen, mit einer grünen Statusleiste und dem Status „Übersprungen“ angezeigt.

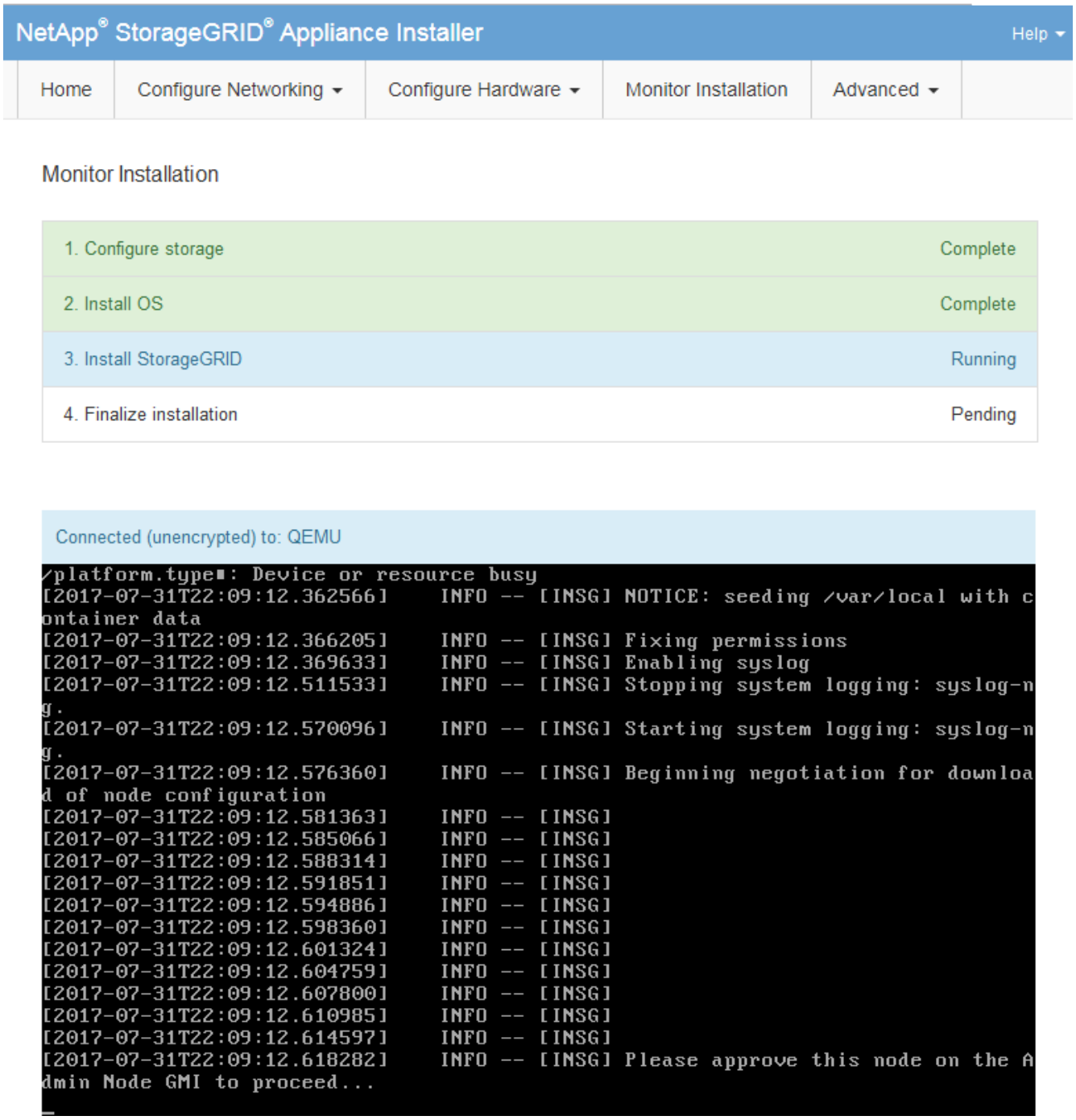
2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.
   - **1. Speicher konfigurieren**

     Während dieser Phase stellt das Installationsprogramm eine Verbindung zum Speichercontroller her, löscht alle vorhandenen Konfigurationen, kommuniziert mit SANtricity OS, um Volumes zu konfigurieren, und konfiguriert die Hosteinstellungen.

   - **2. Betriebssystem installieren**

     Während dieser Phase kopiert das Installationsprogramm das Basis-Betriebssystem-Image für StorageGRID auf das Gerät.

3. Überwachen Sie den Installationsfortschritt weiter, bis die Phase * StorageGRID installieren* angehalten wird und auf der eingebetteten Konsole eine Meldung angezeigt wird, in der Sie aufgefordert werden, diesen Knoten mithilfe des Grid Managers auf dem Admin-Knoten zu genehmigen.



4. Gehe zu"Wählen Sie „Wiederherstellung starten“, um den Speicherknoten des Geräts zu konfigurieren." .

Wählen Sie „Wiederherstellung starten“, um den Speicherknoten des Geräts zu konfigurieren.

Sie müssen im Grid Manager „Wiederherstellung starten“ auswählen, um einen Appliance-Speicherknoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Bevor Sie beginnen

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

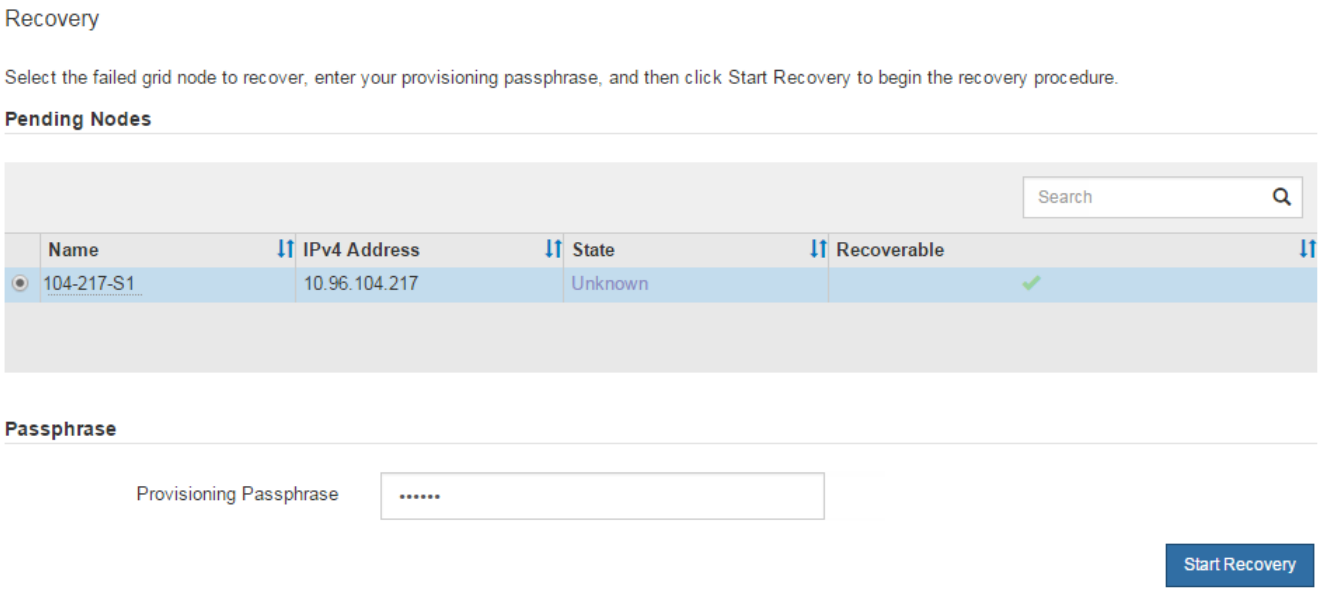
- Sie haben einen Speicherknoten für die Wiederherstellungs-Appliance bereitgestellt.
- Sie verfügen über das Startdatum aller Reparaturaufträge für löschcodierte Daten.
- Sie haben überprüft, dass der Speicherknoten innerhalb der letzten 15 Tage nicht neu erstellt wurde.

Schritte

1. Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Wiederherstellung**.
2. Wählen Sie in der Liste „Ausstehende Knoten“ den Grid-Knoten aus, den Sie wiederherstellen möchten.

   Knoten werden in der Liste angezeigt, nachdem sie ausgefallen sind. Sie können einen Knoten jedoch erst auswählen, wenn er neu installiert wurde und zur Wiederherstellung bereit ist.

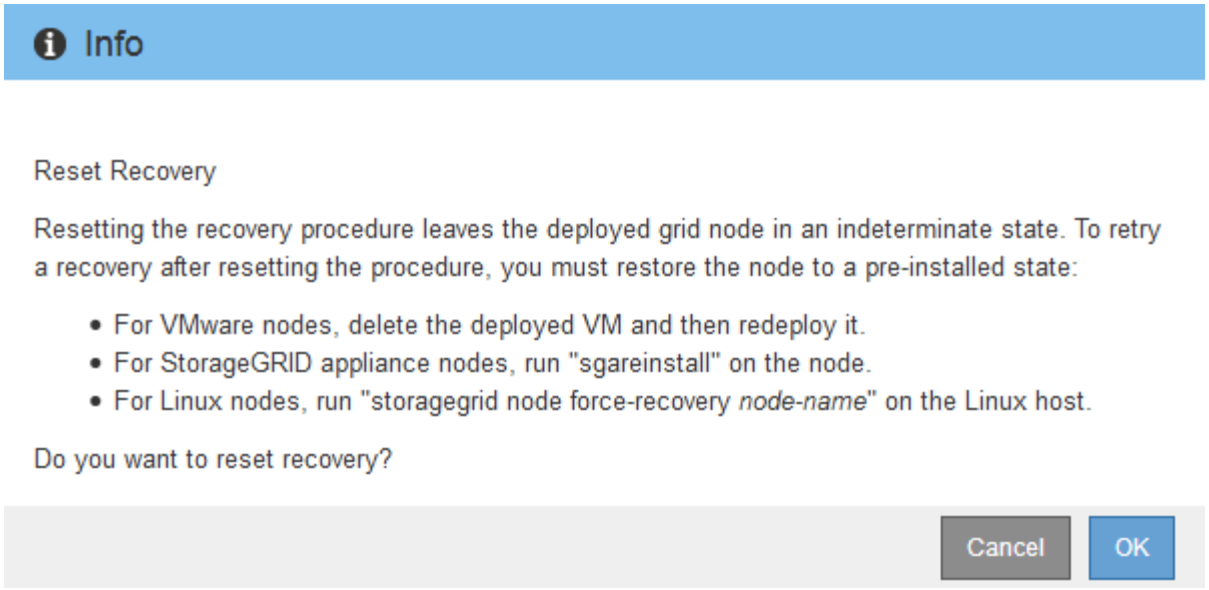
3. Geben Sie die **Bereitstellungspassphrase** ein.
4. Klicken Sie auf **Wiederherstellung starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Grid-Knoten wird wiederhergestellt“.

   Wenn der Grid-Knoten die Phase „Warten auf manuelle Schritte“ erreicht, fahren Sie mit dem nächsten Thema fort und führen Sie die manuellen Schritte aus, um die Appliance-Speichervolumes erneut zu mounten und neu zu formatieren.

> Sie können während der Wiederherstellung jederzeit auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das darauf hinweist, dass der Knoten in einem unbestimmten Zustand verbleibt, wenn Sie die Prozedur zurücksetzen.



Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Vorgangs erneut versuchen möchten, müssen Sie den Appliance-Knoten in einen vorinstallierten Zustand zurückversetzen, indem Sie Folgendes ausführen: `sgareinstall` auf dem Knoten.

Appliance-Speichervolumes erneut mounten und neu formatieren (manuelle Schritte)

Sie müssen zwei Skripte manuell ausführen, um die beibehaltenen Speichervolumes erneut zu mounten und alle ausgefallenen Speichervolumes neu zu formatieren. Das erste Skript stellt Volumes erneut bereit, die ordnungsgemäß als StorageGRID Speichervolumes formatiert sind. Das zweite Skript formatiert alle nicht gemounteten Volumes neu, erstellt die Cassandra-Datenbank bei Bedarf neu und startet die Dienste.

Bevor Sie beginnen

- Sie haben die Hardware aller ausgefallenen Speichervolumes, von denen Sie wissen, dass sie ersetzt werden müssen, bereits ausgetauscht.

  Ausführen des `sn-remount-volumes` Skript kann Ihnen dabei helfen, weitere ausgefallene Speichervolumes zu identifizieren.

- Sie haben überprüft, dass keine Außerbetriebnahme eines Speicherknotens im Gange ist, oder Sie haben den Vorgang zur Außerbetriebnahme des Knotens angehalten. (Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Außerbetriebnahme**.)
- Sie haben überprüft, dass keine Erweiterung im Gange ist. (Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Erweiterung**.)

> ⚠ Wenden Sie sich an den technischen Support, wenn mehr als ein Speicherknoten offline ist oder wenn ein Speicherknoten in diesem Raster in den letzten 15 Tagen neu erstellt wurde. Führen Sie nicht die `sn-recovery-postinstall.sh` Skript. Der Wiederaufbau von Cassandra auf zwei oder mehr Speicherknoten innerhalb von 15 Tagen kann zu Datenverlust führen.

Informationen zu diesem Vorgang

Um dieses Verfahren abzuschließen, führen Sie die folgenden übergeordneten Aufgaben aus:

- Melden Sie sich beim wiederhergestellten Speicherknoten an.
- Führen Sie den `sn-remount-volumes` Skript zum erneuten Mounten ordnungsgemäß formatierter Speichervolumes. Wenn dieses Skript ausgeführt wird, geschieht Folgendes:
  - Mountet und unmountet jedes Speichervolume, um das XFS-Journal wiederzugeben.
  - Führt eine Konsistenzprüfung der XFS-Datei durch.
  - Wenn das Dateisystem konsistent ist, wird ermittelt, ob es sich bei dem Speichervolume um ein ordnungsgemäß formatiertes StorageGRID -Speichervolume handelt.
  - Wenn das Speichervolume richtig formatiert ist, wird das Speichervolume erneut bereitgestellt. Alle vorhandenen Daten auf dem Datenträger bleiben erhalten.
- Überprüfen Sie die Skriptausgabe und beheben Sie alle Probleme.
- Führen Sie den `sn-recovery-postinstall.sh` Skript. Wenn dieses Skript ausgeführt wird, geschieht Folgendes.

> Starten Sie einen Storage Node während der Wiederherstellung nicht neu, bevor Sie `sn-recovery-postinstall.sh` (Schritt 4), um die ausgefallenen Speichervolumes neu zu formatieren und die Objektmetadaten wiederherzustellen. Neustart des Speicherknotens vor `sn-recovery-postinstall.sh` „completes“ verursacht Fehler bei Diensten, die zu starten versuchen, und führt dazu, dass StorageGRID Appliance-Knoten den Wartungsmodus verlassen.

  - Formatiert alle Speichervolumes neu, die der `sn-remount-volumes` Das Skript konnte nicht gemountet werden oder war falsch formatiert.

> Wenn ein Speichervolume neu formatiert wird, gehen alle Daten auf diesem Volume verloren. Sie müssen ein zusätzliches Verfahren ausführen, um Objektdaten von anderen Speicherorten im Grid wiederherzustellen, vorausgesetzt, dass ILM-Regeln zum Speichern von mehr als einer Objektkopie konfiguriert wurden.

  - Baut die Cassandra-Datenbank auf dem Knoten bei Bedarf neu auf.
  - Startet die Dienste auf dem Speicherknoten.

Schritte

1. Melden Sie sich beim wiederhergestellten Speicherknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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 das erste Skript aus, um alle ordnungsgemäß formatierten Speichervolumes erneut zu mounten.

> Wenn alle Speichervolumes neu sind und formatiert werden müssen oder wenn alle Speichervolumes ausgefallen sind, können Sie diesen Schritt überspringen und das zweite Skript ausführen, um alle nicht gemounteten Speichervolumes neu zu formatieren.

a. Führen Sie das Skript aus: `sn-remount-volumes`

   Die Ausführung dieses Skripts auf Speichervolumes mit Daten kann Stunden dauern.

b. Überprüfen Sie während der Ausführung des Skripts die Ausgabe und beantworten Sie alle Eingabeaufforderungen.

   > Bei Bedarf können Sie die `tail -f` Befehl zum Überwachen des Inhalts der Protokolldatei des Skripts(`/var/local/log/sn-remount-volumes.log`) . Die Protokolldatei enthält detailliertere Informationen als die Befehlszeilenausgabe.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
```

```
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

In der Beispielausgabe wurde ein Speichervolume erfolgreich erneut bereitgestellt und bei drei Speichervolumes traten Fehler auf.

- `/dev/sdb`hat die Konsistenzprüfung des XFS-Dateisystems bestanden und verfügte über eine gültige Volumestruktur, sodass es erfolgreich erneut gemountet werden konnte. Daten auf Geräten, die durch das Skript erneut gemountet werden, bleiben erhalten.
- `/dev/sdc`Die Konsistenzprüfung des XFS-Dateisystems ist fehlgeschlagen, da das Speichervolume neu oder beschädigt war.
- `/dev/sdd`konnte nicht gemountet werden, da die Festplatte nicht initialisiert wurde oder der Superblock der Festplatte beschädigt war. Wenn das Skript ein Speichervolume nicht mounten

kann, werden Sie gefragt, ob Sie die Konsistenzprüfung des Dateisystems ausführen möchten.

- Wenn das Speichervolume an eine neue Festplatte angeschlossen ist, antworten Sie mit **N** auf die Eingabeaufforderung. Sie müssen das Dateisystem auf einer neuen Festplatte nicht überprüfen.
- Wenn das Speichervolume an eine vorhandene Festplatte angeschlossen ist, antworten Sie mit **J** auf die Eingabeaufforderung. Mithilfe der Ergebnisse der Dateisystemprüfung können Sie die Ursache der Beschädigung ermitteln. Die Ergebnisse werden gespeichert im `/var/local/log/sn-remount-volumes.log` Protokolldatei.

- `/dev/sde`die Konsistenzprüfung des XFS-Dateisystems bestanden und eine gültige Volumestruktur hatten; die LDR-Knoten-ID im `volID` Datei stimmte nicht mit der ID für diesen Speicherknoten überein (die `configured LDR noid` oben angezeigt). Diese Meldung zeigt an, dass dieses Volume zu einem anderen Speicherknoten gehört.

3. Überprüfen Sie die Skriptausgabe und beheben Sie alle Probleme.

> Wenn ein Speichervolume die Konsistenzprüfung des XFS-Dateisystems nicht bestanden hat oder nicht gemountet werden konnte, überprüfen Sie die Fehlermeldungen in der Ausgabe sorgfältig. Sie müssen die Auswirkungen der Ausführung des `sn-recovery-postinstall.sh` Skript auf diesen Datenträgern.

a. Überprüfen Sie, ob die Ergebnisse einen Eintrag für alle von Ihnen erwarteten Bände enthalten. Wenn Volumes nicht aufgeführt sind, führen Sie das Skript erneut aus.

b. Überprüfen Sie die Nachrichten für alle gemounteten Geräte. Stellen Sie sicher, dass keine Fehler vorliegen, die darauf hinweisen, dass ein Speichervolume nicht zu diesem Speicherknoten gehört.

   Im Beispiel enthält die Ausgabe für /dev/sde die folgende Fehlermeldung:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Wenn ein Speichervolume als zu einem anderen Speicherknoten gehörend gemeldet wird, wenden Sie sich an den technischen Support. Wenn Sie das `sn-recovery-postinstall.sh` Skript wird das Speichervolume neu formatiert, was zu Datenverlust führen kann.

c. Wenn Speichergeräte nicht gemountet werden konnten, notieren Sie sich den Gerätenamen und reparieren oder ersetzen Sie das Gerät.

> Sie müssen alle Speichergeräte reparieren oder ersetzen, die nicht gemountet werden konnten.

   Sie verwenden den Gerätenamen, um die Volume-ID zu suchen, die beim Ausführen des `repair-data` Skript zum Wiederherstellen von Objektdaten auf dem Volume (nächstes Verfahren).

d. Nachdem Sie alle nicht einhängbaren Geräte repariert oder ersetzt haben, führen Sie den `sn-remount-volumes` Skript erneut, um zu bestätigen, dass alle Speichervolumes, die erneut gemountet werden können, erneut gemountet wurden.

Wenn ein Speichervolume nicht gemountet werden kann oder nicht richtig formatiert ist und Sie mit dem nächsten Schritt fortfahren, werden das Volume und alle darauf befindlichen Daten gelöscht. Wenn Sie zwei Kopien der Objektdaten hatten, verfügen Sie bis zum Abschluss des nächsten Vorgangs (Wiederherstellen der Objektdaten) nur über eine einzige Kopie.

Führen Sie nicht die `sn-recovery-postinstall.sh` Skript, wenn Sie der Meinung sind, dass die auf einem ausgefallenen Speichervolume verbleibenden Daten nicht von einer anderen Stelle im Grid wiederhergestellt werden können (z. B. wenn Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie erstellt, oder wenn Volumes auf mehreren Knoten ausgefallen sind). Wenden Sie sich stattdessen an den technischen Support, um zu erfahren, wie Sie Ihre Daten wiederherstellen können.

4. Führen Sie den `sn-recovery-postinstall.sh` Skript: `sn-recovery-postinstall.sh`

   Dieses Skript formatiert alle Speichervolumes neu, die nicht gemountet werden konnten oder bei denen festgestellt wurde, dass sie nicht richtig formatiert waren. Es erstellt bei Bedarf die Cassandra-Datenbank auf dem Knoten neu und startet die Dienste auf dem Speicherknoten.

   Beachten Sie Folgendes:

   - Die Ausführung des Skripts kann Stunden dauern.
   - Im Allgemeinen sollten Sie die SSH-Sitzung in Ruhe lassen, während das Skript ausgeführt wird.
   - Drücken Sie nicht **Strg+C**, während die SSH-Sitzung aktiv ist.
   - Das Skript wird im Hintergrund ausgeführt, wenn eine Netzwerkstörung auftritt und die SSH-Sitzung beendet, aber Sie können den Fortschritt auf der Wiederherstellungsseite verfolgen.
   - Wenn der Speicherknoten den RSM-Dienst verwendet, kann es vorkommen, dass das Skript 5 Minuten lang blockiert, während die Knotendienste neu gestartet werden. Diese 5-minütige Verzögerung ist immer dann zu erwarten, wenn der RSM-Dienst zum ersten Mal gestartet wird.

     Der RSM-Dienst ist auf Speicherknoten vorhanden, die den ADC-Dienst enthalten.

   Einige StorageGRID Wiederherstellungsverfahren verwenden Reaper zur Durchführung von Cassandra-Reparaturen. Reparaturen erfolgen automatisch, sobald die entsprechenden bzw. erforderlichen Leistungen begonnen haben. Möglicherweise bemerken Sie eine Skriptausgabe, in der „Reaper“ oder „Cassandra-Reparatur“ erwähnt wird. Wenn eine Fehlermeldung angezeigt wird, die darauf hinweist, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

5. Als `sn-recovery-postinstall.sh` Skript ausgeführt wird, überwachen Sie die Wiederherstellungsseite im Grid Manager.

   Der Fortschrittsbalken und die Spalte „Phase“ auf der Wiederherstellungsseite bieten einen allgemeinen Status der `sn-recovery-postinstall.sh` Skript.

6. Nach dem `sn-recovery-postinstall.sh` Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speichervolumes wiederherstellen, die vom Skript formatiert wurden.

   Das Skript fragt, ob Sie den Volume-Wiederherstellungsprozess des Grid Managers verwenden möchten.

- In den meisten Fällen sollten Sie"Wiederherstellen von Objektdaten mit Grid Manager" . Antwort `y` um den Grid Manager zu verwenden.
- In seltenen Fällen, beispielsweise wenn Sie vom technischen Support dazu aufgefordert werden oder wenn Sie wissen, dass der Ersatzknoten weniger Volumes für die Objektspeicherung zur Verfügung hat als der ursprüngliche Knoten, müssen Sie"Objektdaten manuell wiederherstellen" mithilfe der `repair-data` Skript. Wenn einer dieser Fälle zutrifft, antworten Sie `n` .

> Wenn Sie antworten `n` zur Verwendung des Volume-Wiederherstellungsprozesses des Grid Managers (manuelle Wiederherstellung der Objektdaten):
>
> - Sie können Objektdaten mit Grid Manager nicht wiederherstellen.
> - Sie können den Fortschritt manueller Wiederherstellungsaufträge mit Grid Manager überwachen.

Nachdem Sie Ihre Auswahl getroffen haben, wird das Skript abgeschlossen und die nächsten Schritte zur Wiederherstellung der Objektdaten werden angezeigt. Nachdem Sie diese Schritte überprüft haben, drücken Sie eine beliebige Taste, um zur Befehlszeile zurückzukehren.

Stellen Sie Objektdaten auf dem Speichervolume für die Appliance wieder her

Nachdem Sie die Speichervolumes für den Storage Node der Appliance wiederhergestellt haben, können Sie die replizierten oder erasure-coded Objektdaten wiederherstellen, die beim Ausfall des Storage Node verloren gegangen sind.

Welches Verfahren soll ich anwenden?

Stellen Sie Objektdaten nach Möglichkeit mithilfe der Seite **Volume-Wiederherstellung** im Grid Manager wieder her.

- Wenn die Volumes unter **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** aufgelistet sind, stellen Sie die Objektdaten mithilfe des"Seite zur Volume-Wiederherstellung im Grid Manager" .
- Wenn die Volumes nicht unter **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** aufgeführt sind, befolgen Sie die folgenden Schritte zur Verwendung des `repair-data` Skript zum Wiederherstellen von Objektdaten.

  Wenn der wiederhergestellte Storage Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie die `repair-data` Skript.

> Das Skript „repair-data“ ist veraltet und wird in einer zukünftigen Version entfernt. Verwenden Sie nach Möglichkeit die"Volume-Wiederherstellungsverfahren im Grid Manager" .

Verwenden Sie die `repair-data` Skript zum Wiederherstellen von Objektdaten

Bevor Sie beginnen

- Sie haben bestätigt, dass der wiederhergestellte Speicherknoten den Verbindungsstatus **Verbunden** hat. auf der Registerkarte **KNOTEN** > **Übersicht** im Grid Manager.

Informationen zu diesem Vorgang

Objektdaten können von anderen Speicherknoten oder einem Cloud-Speicherpool wiederhergestellt werden, vorausgesetzt, die ILM-Regeln des Grids wurden so konfiguriert, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und diese Kopie auf einem Speichervolume vorhanden war, das ausgefallen ist, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, muss StorageGRID mehrere Anfragen an den Endpunkt des Cloud-Speicherpools senden, um die Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Wiederherstellungszeitraums und der damit verbundenen Kosten zu erhalten.

Über die `repair-data` Skript

Um Objektdaten wiederherzustellen, führen Sie den `repair-data` Skript. Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans, um sicherzustellen, dass die ILM-Regeln eingehalten werden.

Wählen Sie unten **Replizierte Daten** oder **Erasure-coded (EC) Daten**, um die verschiedenen Optionen für die `repair-data` Skript, je nachdem, ob Sie replizierte Daten oder erasure-coded Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssätze ausführen.

> Weitere Informationen zum `repair-data` Skript, geben Sie `repair-data --help` von der Befehlszeile des primären Admin-Knotens.

> Das Skript „repair-data“ ist veraltet und wird in einer zukünftigen Version entfernt. Verwenden Sie nach Möglichkeit die"Volume-Wiederherstellungsverfahren im Grid Manager" .

Replizierte Daten

Zum Wiederherstellen replizierter Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Sie können Reparaturen replizierter Daten mit diesem Befehl verfolgen:

```
repair-data show-replicated-repair-status
```

Löschcodierte (EC) Daten

Zum Wiederherstellen von Erasure-Code-Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Sie können die Reparatur von Erasure-Codierten Daten mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```

> Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Wenn jedoch nicht alle löschcodierten Daten berücksichtigt werden können, kann die Reparatur nicht abgeschlossen werden. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

> Der EC-Reparaturauftrag reserviert vorübergehend viel Speicherplatz. Möglicherweise werden Speicherwarnungen ausgelöst, die jedoch nach Abschluss der Reparatur behoben werden. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturjob abgeschlossen ist, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Hostnamen für Speicherknoten suchen

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. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicherknotens für die wiederhergestellten Speichervolumes zu finden. Um eine Liste aller Knoten im Raster anzuzeigen, geben

Sie Folgendes ein: `cat /etc/hosts` .

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Speichervolumes ausgefallen sind, reparieren Sie den gesamten Knoten. Befolgen Sie die Anweisungen für **replizierte Daten**, **löschcodierte (EC) Daten** oder beides, je nachdem, ob Sie replizierte Daten, löschcodierte (EC) Daten oder beides verwenden.

Wenn nur einige Volumes ausgefallen sind, gehen Sie zuwenn nur einige Volumes ausgefallen sind .

> Du kannst nicht rennen `repair-data` Operationen für mehr als einen Knoten gleichzeitig. Um mehrere Knoten wiederherzustellen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Raster replizierte Daten enthält, verwenden Sie die `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option, wobei `--nodes` ist der Hostname (Systemname), um den gesamten Speicherknoten zu reparieren.

Dieser Befehl repariert die replizierten Daten auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Beim Wiederherstellen von Objektdaten wird die Warnung „Objekte verloren“ ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Speicherknoten im gesamten System können Warnungen ausgelöst werden. Sie sollten die Ursache des Verlusts ermitteln und feststellen, ob eine Wiederherstellung möglich ist. Sehen "Untersuchen Sie verlorene Gegenstände" .

Löschcodierte (EC) Daten

Wenn Ihr Grid Erasure-Coding-Daten enthält, verwenden Sie die `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option, wobei `--nodes` ist der Hostname (Systemname), um den gesamten Speicherknoten zu reparieren.

Dieser Befehl repariert die erasure-coded Daten auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Die Operation gibt einen eindeutigen `repair ID` das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese `repair ID` um den Fortschritt und das Ergebnis der `repair_data` Betrieb. Nach Abschluss des Wiederherstellungsprozesses wird keine weitere Rückmeldung zurückgegeben.

Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige der Volumes ausgefallen sind, reparieren Sie die betroffenen Volumes. Befolgen Sie die Anweisungen für **replizierte Daten**, **löschcodierte (EC) Daten** oder beides, je nachdem, ob Sie replizierte Daten, löschcodierte (EC) Daten oder beides verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zuwenn alle Volumes ausgefallen sind .

Geben Sie die Volume-IDs im Hexadezimalformat ein. Zum Beispiel, `0000` ist der erste Band und `000F` ist der sechzehnte Band. Sie können ein Volume, einen Volumebereich oder mehrere Volumes angeben, die nicht in einer Sequenz stehen.

Alle Volumes müssen sich auf demselben Speicherknoten befinden. Wenn Sie Volumes für mehr als einen Speicherknoten wiederherstellen müssen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Grid replizierte Daten enthält, verwenden Sie die `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wo `--nodes` ist der Hostname des Knotens). Fügen Sie dann entweder die `--volumes` oder `--volume-range` Option, wie in den folgenden Beispielen gezeigt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf dem Volume wieder her `0002` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf allen Volumes im Bereich wieder her `0003` Zu `0009` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Mehrere Volumes, nicht in einer Sequenz: Dieser Befehl stellt replizierte Daten auf Volumes wieder her `0001` , `0005` , Und `0008` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Beim Wiederherstellen von Objektdaten wird die Warnung „Objekte verloren“ ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Speicherknoten im gesamten System können Warnungen ausgelöst werden. Beachten Sie die Alarmbeschreibung und die empfohlenen Maßnahmen, um die Ursache des Verlusts zu ermitteln und festzustellen, ob eine Wiederherstellung möglich ist.

Löschcodierte (EC) Daten

Wenn Ihr Grid Erasure-Coding-Daten enthält, verwenden Sie die `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wo `--nodes` ist der Hostname des Knotens). Fügen Sie dann entweder die `--volumes` oder `--volume-range` Option, wie in den folgenden Beispielen gezeigt.

Einzelnes Volume: Dieser Befehl stellt löschcodierte Daten auf dem Volume wieder her `0007` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt die löschcodierten Daten auf allen Volumes im Bereich wieder her `0004` Zu `0006` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Mehrere Volumes, nicht in einer Sequenz: Dieser Befehl stellt erased-coded Daten auf Volumes wieder her `000A` , `000C` , Und `000E` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Operation gibt einen eindeutigen `repair ID` das identifiziert dies `repair_data`

Betrieb. Verwenden Sie diese `repair ID` um den Fortschritt und das Ergebnis der `repair_data` Betrieb. Nach Abschluss des Wiederherstellungsprozesses wird keine weitere Rückmeldung zurückgegeben.

> Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

Monitorreparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **löschcodierte (EC) Daten** oder beides verwenden.

Sie können auch den Status der laufenden Volume-Wiederherstellungsaufträge überwachen und einen Verlauf der abgeschlossenen Wiederherstellungsaufträge anzeigen."Grid-Manager" .

Replizierte Daten

- Um einen geschätzten Prozentsatz der Fertigstellung der replizierten Reparatur zu erhalten, addieren Sie die `show-replicated-repair-status` Option zum Befehl „repair-data“.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob die Reparaturen abgeschlossen sind:
  a. Wählen Sie **NODES** > ***Speicherknoten wird repariert*** > **ILM**.
  b. Überprüfen Sie die Attribute im Abschnitt „Bewertung“. Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut **Warten – Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
  a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
  b. Wählen Sie ***grid*** > ***Reparierter Speicherknoten*** > **LDR** > **Datenspeicher**.
  c. Verwenden Sie eine Kombination der folgenden Attribute, um so gut wie möglich zu bestimmen, ob replizierte Reparaturen abgeschlossen sind.

> ⓘ Möglicherweise liegen Cassandra-Inkonsistenzen vor und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

  - **Reparaturversuche (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt replizierter Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Speicherknoten versucht, ein Hochrisikoobjekt zu reparieren. Wenn dieses Attribut über einen Zeitraum, der länger ist als der aktuelle Scanzeitraum (bereitgestellt durch das Attribut **Scanzeitraum – Geschätzt**), nicht ansteigt, bedeutet dies, dass beim ILM-Scan auf keinem Knoten ein Hochrisikoobjekt gefunden wurde, das repariert werden muss.

> ⓘ Hochrisikoobjekte sind Objekte, bei denen die Gefahr eines vollständigen Verlusts besteht. Dies schließt keine Objekte ein, die ihrer ILM-Konfiguration nicht entsprechen.

  - **Scan-Zeitraum – Geschätzt (XSCM)**: Verwenden Sie dieses Attribut, um abzuschätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn das Attribut **Reparaturversuche** über einen Zeitraum, der länger als der aktuelle Scanzeitraum ist, nicht ansteigt, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt wurden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period – Estimated (XSCM)** gilt für das gesamte Raster und ist das Maximum aller Knoten-Scan-Perioden. Sie können den Attributverlauf **Scan-Zeitraum – Geschätzt** für das Raster abfragen, um einen geeigneten Zeitrahmen zu bestimmen.

Löschcodierte (EC) Daten

So überwachen Sie die Reparatur von Erasure-Code-Daten und wiederholen alle möglicherweise fehlgeschlagenen Anfragen:

1. Bestimmen Sie den Status der Datenreparaturen mit Erasure Code:
   - Wählen Sie **SUPPORT** > **Tools** > **Metriken**, um die geschätzte Zeit bis zur Fertigstellung und den Fertigstellungsgrad für den aktuellen Auftrag anzuzeigen. Wählen Sie dann im Abschnitt „Grafana“ die Option „EC-Übersicht“ aus. Sehen Sie sich die Dashboards **Geschätzte Zeit bis zur Fertigstellung des Grid EC-Jobs** und **Prozentsatz der Fertigstellung des Grid EC-Jobs**

an.

- Verwenden Sie diesen Befehl, um den Status eines bestimmten `repair-data` Betrieb:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

  ```
  repair-data show-ec-repair-status
  ```

Die Ausgabe listet Informationen auf, einschließlich `repair ID` , für alle bisherigen und laufenden Reparaturen.

2. Wenn die Ausgabe zeigt, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie die `--repair-id` Option zum erneuten Versuch der Reparatur.

   Mit diesem Befehl wird eine fehlgeschlagene Knotenreparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Mit diesem Befehl wird eine fehlgeschlagene Volumereparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung des Appliance-Speicherknotens

Nach der Wiederherstellung eines Appliance-Speicherknotens müssen Sie überprüfen, ob der gewünschte Status des Appliance-Speicherknotens auf „Online“ eingestellt ist, und sicherstellen, dass der Status standardmäßig „Online“ ist, wenn der Speicherknotenserver neu gestartet wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Überprüfen Sie die Werte von **Wiederhergestellter Speicherknoten** > **LDR** > **Speicher** > **Speicherstatus – Gewünscht** und **Speicherstatus – Aktuell**.

   Der Wert beider Attribute sollte „Online“ sein.

3. Wenn „Speicherstatus – Gewünscht“ auf „Schreibgeschützt“ eingestellt ist, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf die Registerkarte **Konfiguration**.
   b. Wählen Sie aus der Dropdown-Liste **Speicherstatus – Gewünscht** die Option **Online** aus.
   c. Klicken Sie auf **Änderungen übernehmen**.

d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherstatus – Gewünscht** und **Speicherstatus – Aktuell** auf „Online“ aktualisiert wurden.

Wiederherstellung nach einem Speichervolume-Fehler, wenn das Systemlaufwerk intakt ist

Wiederherstellung nach einem Speichervolume-Fehler, wenn das Systemlaufwerk intakt ist

Sie müssen eine Reihe von Aufgaben ausführen, um einen softwarebasierten Speicherknoten wiederherzustellen, bei dem ein oder mehrere Speichervolumes auf dem Speicherknoten ausgefallen sind, das Systemlaufwerk jedoch intakt ist. Wenn nur Speichervolumes ausgefallen sind, steht der Speicherknoten dem StorageGRID -System weiterhin zur Verfügung.

> Dieses Wiederherstellungsverfahren gilt nur für softwarebasierte Speicherknoten. Wenn Speichervolumes auf einem Appliance-Speicherknoten ausgefallen sind, verwenden Sie stattdessen das Appliance-Verfahren:"Wiederherstellen des Appliance-Speicherknotens" .

Dieses Wiederherstellungsverfahren umfasst die folgenden Aufgaben:

- "Überprüfen Sie die Warnungen zur Wiederherstellung des Speichervolumes"
- "Identifizieren und Unmounten fehlerhafter Speichervolumes"
- "Stellen Sie die Volumes wieder her und erstellen Sie die Cassandra-Datenbank neu"
- "Objektdaten wiederherstellen"
- "Überprüfen Sie den Speicherstatus"

Warnungen zur Wiederherstellung von Speichervolumes

Lesen Sie die folgenden Warnungen, bevor Sie ausgefallene Speichervolumes für einen Speicherknoten wiederherstellen.

Die Speichervolumes (oder Rangedbs) in einem Speicherknoten werden durch eine Hexadezimalzahl identifiziert, die als Volume-ID bezeichnet wird. Beispielsweise ist 0000 der erste Band und 000F der sechzehnte Band. Der erste Objektspeicher (Volume 0) auf jedem Speicherknoten verwendet bis zu 4 TB Speicherplatz für Objektmetadaten und Cassandra-Datenbankvorgänge. Der verbleibende Speicherplatz auf diesem Volume wird für Objektdaten verwendet. Alle anderen Speichervolumes werden ausschließlich für Objektdaten verwendet.

Wenn Volume 0 ausfällt und wiederhergestellt werden muss, kann die Cassandra-Datenbank im Rahmen des Volume-Wiederherstellungsverfahrens neu erstellt werden. Cassandra kann auch unter folgenden Umständen neu erstellt werden:

- Ein Speicherknoten wird wieder online gebracht, nachdem er länger als 15 Tage offline war.
- Das Systemlaufwerk und ein oder mehrere Speichervolumes fallen aus und werden wiederhergestellt.

Beim Neuaufbau von Cassandra verwendet das System Informationen von anderen Speicherknoten. Wenn zu viele Speicherknoten offline sind, sind einige Cassandra-Daten möglicherweise nicht verfügbar. Wenn Cassandra vor Kurzem neu erstellt wurde, sind die Cassandra-Daten im gesamten Grid möglicherweise noch nicht konsistent. Es kann zu Datenverlust kommen, wenn Cassandra neu erstellt wird, während zu viele Speicherknoten offline sind, oder wenn zwei oder mehr Speicherknoten innerhalb von 15 Tagen neu erstellt

werden.

> Wenn mehr als ein Speicherknoten ausgefallen ist (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es könnte zu Datenverlust kommen.

> Wenn dies der zweite Speicherknotenausfall innerhalb von weniger als 15 Tagen nach einem Speicherknotenausfall oder einer Wiederherstellung ist, wenden Sie sich an den technischen Support. Der Wiederaufbau von Cassandra auf zwei oder mehr Speicherknoten innerhalb von 15 Tagen kann zu Datenverlust führen.

> Wenn an einem Standort mehr als ein Speicherknoten ausgefallen ist, ist möglicherweise ein Standortwiederherstellungsverfahren erforderlich. Sehen "So stellt der technische Support eine Site wieder her" .

> Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und die Kopie auf einem ausgefallenen Speichervolume vorhanden ist, können Sie das Objekt nicht wiederherstellen.

Ähnliche Informationen

"Warnungen und Hinweise zur Wiederherstellung von Grid-Knoten"

Identifizieren und Unmounten fehlerhafter Speichervolumes

Wenn Sie einen Speicherknoten mit ausgefallenen Speichervolumes wiederherstellen, müssen Sie die ausgefallenen Volumes identifizieren und aushängen. Sie müssen sicherstellen, dass im Rahmen des Wiederherstellungsverfahrens nur die ausgefallenen Speichervolumes neu formatiert werden.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Sie sollten ausgefallene Speichervolumes so schnell wie möglich wiederherstellen.

Der erste Schritt des Wiederherstellungsprozesses besteht darin, Volumes zu erkennen, die getrennt wurden, ausgehängt werden müssen oder E/A-Fehler aufweisen. Wenn ausgefallene Volumes noch angeschlossen sind, aber ein zufällig beschädigtes Dateisystem aufweisen, erkennt das System möglicherweise keine Beschädigung in nicht verwendeten oder nicht zugewiesenen Teilen der Festplatte.

> Sie müssen diesen Vorgang abschließen, bevor Sie manuelle Schritte zur Wiederherstellung der Volumes durchführen, z. B. das Hinzufügen oder erneute Anschließen der Datenträger, das Stoppen des Knotens, das Starten des Knotens oder ein Neustart. Andernfalls, wenn Sie die `reformat_storage_block_devices.rb` Skripts kann ein Dateisystemfehler auftreten, der dazu führt, dass das Skript hängen bleibt oder fehlschlägt.

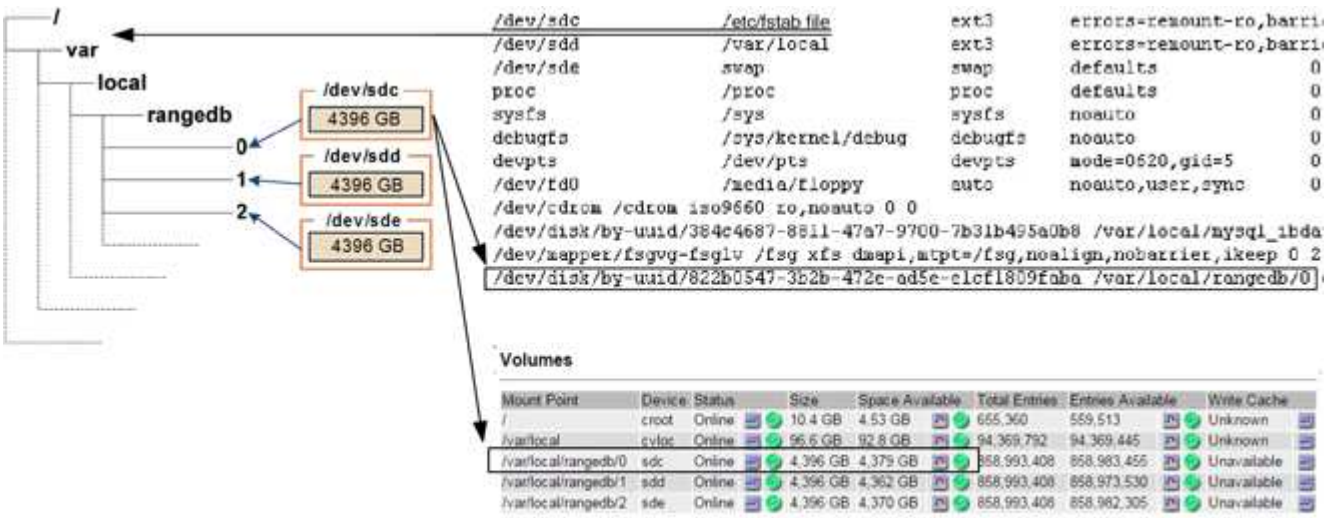
> Reparieren Sie die Hardware und schließen Sie die Festplatten ordnungsgemäß an, bevor Sie den `reboot` Befehl.

Identifizieren Sie ausgefallene Speichervolumes sorgfältig. Anhand dieser Informationen können Sie überprüfen, welche Datenträger neu formatiert werden müssen. Nachdem ein Volume neu formatiert wurde, können die Daten auf dem Volume nicht wiederhergestellt werden.

Um ausgefallene Speichervolumes korrekt wiederherzustellen, müssen Sie sowohl die Gerätenamen der ausgefallenen Speichervolumes als auch deren Volume-IDs kennen.

Bei der Installation wird jedem Speichergerät eine universelle eindeutige Kennung (UUID) für das Dateisystem zugewiesen und es wird mithilfe dieser zugewiesenen Dateisystem-UUID in ein rangedb-Verzeichnis auf dem Speicherknoten eingebunden. Die Dateisystem-UUID und das rangedb-Verzeichnis sind in der `/etc/fstab` Datei. Der Gerätename, das Rangedb-Verzeichnis und die Größe des gemounteten Volumes werden im Grid Manager angezeigt.

Im folgenden Beispiel wird das Gerät `/dev/sdc` hat eine Volume-Größe von 4 TB, ist gemountet auf `/var/local/rangedb/0` , unter Verwendung des Gerätenamens `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` im`/etc/fstab` Datei:



Schritte

1. Führen Sie die folgenden Schritte aus, um die ausgefallenen Speichervolumes und ihre Gerätenamen aufzuzeichnen:

   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.

   b. Wählen Sie **Site** > **Fehlerhafter Speicherknoten** > **LDR** > **Speicher** > **Übersicht** > **Haupt** und suchen Sie nach Objektspeichern mit Alarmen.

   Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

   c. Wählen Sie **Site** > **Fehlerhafter Speicherknoten** > **SSM** > **Ressourcen** > **Übersicht** > **Haupt**. Bestimmen Sie den Bereitstellungspunkt und die Volumegröße jedes im vorherigen Schritt identifizierten ausgefallenen Speichervolumes.

Objektspeicher werden in Hexadezimalnotation nummeriert. Beispielsweise ist 0000 der erste Band und 000F der sechzehnte Band. Im Beispiel entspricht der Objektspeicher mit der ID 0000 `/var/local/rangedb/0` mit dem Gerätenamen sdc und einer Größe von 107 GB.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. Melden Sie sich beim ausgefallenen Speicherknoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Führen Sie das folgende Skript aus, um die Bereitstellung eines ausgefallenen Speichervolumes aufzuheben:

   ```
   sn-unmount-volume object_store_ID
   ```

   Der `object_store_ID` ist die ID des ausgefallenen Speichervolumes. Geben Sie beispielsweise `0` im Befehl für einen Objektspeicher mit der ID 0000.

4. Drücken Sie bei entsprechender Aufforderung **y**, um den Cassandra-Dienst abhängig vom Speichervolumen 0 zu stoppen.

   Wenn der Cassandra-Dienst bereits gestoppt ist, werden Sie nicht dazu aufgefordert. Der Cassandra-Dienst wird nur für Volume 0 gestoppt.

   ```
   root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
   Services depending on storage volume 0 (cassandra) aren't down.
   Services depending on storage volume 0 must be stopped before running
   this script.
   Stop services that require storage volume 0 [y/N]? y
   Shutting down services that require storage volume 0.
   Services requiring storage volume 0 stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

   Innerhalb weniger Sekunden wird das Volume ausgehängt. Es werden Meldungen angezeigt, die jeden Schritt des Vorgangs anzeigen. Die letzte Meldung zeigt an, dass das Volume ausgehängt ist.

5. Wenn das Unmounten fehlschlägt, weil das Volume belegt ist, können Sie ein Unmounten erzwingen, indem Sie `--use-umountof` Option:

> Erzwingen einer Aushängung mit dem `--use-umountof` Die Option kann dazu führen, dass Prozesse oder Dienste, die das Volume verwenden, sich unerwartet verhalten oder abstürzen.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

Wiederherstellen ausgefallener Speichervolumes und Neuaufbau der Cassandra-Datenbank

Sie müssen ein Skript ausführen, das den Speicher auf ausgefallenen Speichervolumes neu formatiert und neu bereitstellt und die Cassandra-Datenbank auf dem Speicherknoten neu erstellt, wenn das System feststellt, dass dies erforderlich ist.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei.
- Die Systemlaufwerke auf dem Server sind intakt.
- Die Ursache des Ausfalls wurde ermittelt und gegebenenfalls wurde bereits Ersatzspeicherhardware angeschafft.
- Die Gesamtgröße des Ersatzspeichers entspricht der des Originals.
- Sie haben überprüft, dass keine Außerbetriebnahme eines Speicherknotens im Gange ist, oder Sie haben den Vorgang zur Außerbetriebnahme des Knotens angehalten. (Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Außerbetriebnahme**.)
- Sie haben überprüft, dass keine Erweiterung im Gange ist. (Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Erweiterung**.)
- Du hast"die Warnungen zur Speichervolumenwiederherstellung überprüft" .

Schritte

1. Ersetzen Sie bei Bedarf den ausgefallenen physischen oder virtuellen Speicher, der mit den ausgefallenen Speichervolumes verknüpft ist, die Sie zuvor identifiziert und ausgehängt haben.

   Mounten Sie die Volumes in diesem Schritt nicht erneut. Der Speicher wird neu gemountet und hinzugefügt zu `/etc/fstab` in einem späteren Schritt.

2. Gehen Sie im Grid Manager zu **NODES** > **`appliance Storage Node`** > **Hardware**. Überprüfen Sie im Abschnitt „StorageGRID Appliance“ der Seite, ob der Storage-RAID-Modus fehlerfrei ist.
3. Melden Sie sich beim ausgefallenen Speicherknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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 `#` .

4. Verwenden Sie einen Texteditor (vi oder vim), um fehlerhafte Volumes aus dem `/etc/fstab` Datei und speichern Sie die Datei anschließend.

> Auskommentieren eines fehlerhaften Datenträgers im `/etc/fstab` Datei ist unzureichend. Das Volume muss gelöscht werden aus `fstab` während der Wiederherstellungsprozess überprüft, ob alle Zeilen in der `fstab` Datei stimmt mit den gemounteten Dateisystemen überein.

5. Formatieren Sie alle ausgefallenen Speichervolumes neu und erstellen Sie die Cassandra-Datenbank neu, falls erforderlich. Eingeben: `reformat_storage_block_devices.rb`

   - Wenn Speichervolume 0 ausgehängt wird, weisen Eingabeaufforderungen und Meldungen darauf hin, dass der Cassandra-Dienst gestoppt wird.
   - Sie werden aufgefordert, die Cassandra-Datenbank bei Bedarf neu zu erstellen.
     - Überprüfen Sie die Warnungen. Wenn keines davon zutrifft, erstellen Sie die Cassandra-Datenbank neu. Geben Sie ein: **y**
     - Wenn mehr als ein Speicherknoten offline ist oder wenn ein anderer Speicherknoten in den letzten 15 Tagen neu erstellt wurde. Geben Sie ein: **n**

       Das Skript wird beendet, ohne Cassandra neu zu erstellen. Wenden Sie sich an den technischen Support.
   - Wenn Sie für jedes RangeDB-Laufwerk auf dem Speicherknoten gefragt werden: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?` , geben Sie eine der folgenden Antworten ein:
     - **y**, um ein Laufwerk mit Fehlern neu zu formatieren. Dadurch wird das Speichervolume neu formatiert und dem `/etc/fstab` Datei.
     - **n**, wenn das Laufwerk keine Fehler enthält und Sie es nicht neu formatieren möchten.

       > Durch Auswahl von **n** wird das Skript beendet. Entweder mounten Sie das Laufwerk (wenn Sie meinen, dass die Daten auf dem Laufwerk erhalten bleiben sollten und das Laufwerk irrtümlicherweise ausgehängt wurde) oder Sie entfernen das Laufwerk. Führen Sie dann den `reformat_storage_block_devices.rb` Befehl erneut.

       > Einige StorageGRID Wiederherstellungsverfahren verwenden Reaper zur Durchführung von Cassandra-Reparaturen. Reparaturen erfolgen automatisch, sobald die entsprechenden bzw. erforderlichen Leistungen begonnen haben. Möglicherweise bemerken Sie eine Skriptausgabe, in der „Reaper“ oder „Cassandra-Reparatur“ erwähnt wird. Wenn eine Fehlermeldung angezeigt wird, die darauf hinweist, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

   In der folgenden Beispielausgabe wird das Laufwerk `/dev/sdf` muss neu formatiert werden, und

Cassandra musste nicht neu erstellt werden:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

Nachdem die Speichervolumes neu formatiert und neu gemountet wurden und die erforderlichen Cassandra-Operationen abgeschlossen sind, können Sie"Wiederherstellen von Objektdaten mit Grid Manager" .

Stellen Sie die Objektdaten auf einem Speichervolume wieder her, auf dem das Systemlaufwerk intakt ist.

Nachdem Sie ein Speichervolume auf einem Speicherknoten wiederhergestellt haben, dessen Systemlaufwerk intakt ist, können Sie die replizierten oder erasure-coded Objektdaten wiederherstellen, die beim Ausfall des Speichervolumes verloren gegangen sind.

Welches Verfahren soll ich anwenden?

Stellen Sie Objektdaten nach Möglichkeit mithilfe der Seite **Volume-Wiederherstellung** im Grid Manager wieder her.

- Wenn die Volumes unter **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** aufgelistet sind, stellen Sie die Objektdaten mithilfe des"Seite zur Volume-Wiederherstellung im Grid Manager" .
- Wenn die Volumes nicht unter **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** aufgeführt sind, befolgen Sie die folgenden Schritte zur Verwendung des `repair-data` Skript zum Wiederherstellen von Objektdaten.

  Wenn der wiederhergestellte Storage Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie die `repair-data` Skript.

> ⓘ Das Skript „repair-data“ ist veraltet und wird in einer zukünftigen Version entfernt. Verwenden Sie nach Möglichkeit die"Volume-Wiederherstellungsverfahren im Grid Manager" .

Verwenden Sie die `repair-data` Skript zum Wiederherstellen von Objektdaten

Bevor Sie beginnen

- Sie haben bestätigt, dass der wiederhergestellte Speicherknoten den Verbindungsstatus **Verbunden** hat. auf der Registerkarte **KNOTEN** > **Übersicht** im Grid Manager.

Informationen zu diesem Vorgang

Objektdaten können von anderen Speicherknoten oder einem Cloud-Speicherpool wiederhergestellt werden, vorausgesetzt, die ILM-Regeln des Grids wurden so konfiguriert, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und diese Kopie auf einem Speichervolume vorhanden war, das ausgefallen ist, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, muss StorageGRID mehrere Anfragen an den Endpunkt des Cloud-Speicherpools senden, um die Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Wiederherstellungszeitraums und der damit verbundenen Kosten zu erhalten.

Über die `repair-data` Skript

Um Objektdaten wiederherzustellen, führen Sie den `repair-data` Skript. Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans, um sicherzustellen, dass die ILM-Regeln eingehalten werden.

Wählen Sie unten **Replizierte Daten** oder **Erasure-coded (EC) Daten**, um die verschiedenen Optionen für die `repair-data` Skript, je nachdem, ob Sie replizierte Daten oder erasure-coded Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssätze ausführen.

> Weitere Informationen zum `repair-data` Skript, geben Sie `repair-data --help` von der Befehlszeile des primären Admin-Knotens.

> Das Skript „repair-data“ ist veraltet und wird in einer zukünftigen Version entfernt. Verwenden Sie nach Möglichkeit die"Volume-Wiederherstellungsverfahren im Grid Manager" .

Replizierte Daten

Zum Wiederherstellen replizierter Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Sie können Reparaturen replizierter Daten mit diesem Befehl verfolgen:

```
repair-data show-replicated-repair-status
```

Löschcodierte (EC) Daten

Zum Wiederherstellen von Erasure-Code-Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Sie können die Reparatur von Erasure-Codierten Daten mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```

Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Wenn jedoch nicht alle löschcodierten Daten berücksichtigt werden können, kann die Reparatur nicht abgeschlossen werden. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

Der EC-Reparaturauftrag reserviert vorübergehend viel Speicherplatz. Möglicherweise werden Speicherwarnungen ausgelöst, die jedoch nach Abschluss der Reparatur behoben werden. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturjob abgeschlossen ist, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Hostnamen für Speicherknoten suchen

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. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicherknotens für die wiederhergestellten Speichervolumes zu finden. Um eine Liste aller Knoten im Raster anzuzeigen, geben

Sie Folgendes ein: `cat /etc/hosts` .

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Speichervolumes ausgefallen sind, reparieren Sie den gesamten Knoten. Befolgen Sie die Anweisungen für **replizierte Daten**, **löschcodierte (EC) Daten** oder beides, je nachdem, ob Sie replizierte Daten, löschcodierte (EC) Daten oder beides verwenden.

Wenn nur einige Volumes ausgefallen sind, gehen Sie zuwenn nur einige Volumes ausgefallen sind .

> Du kannst nicht rennen `repair-data` Operationen für mehr als einen Knoten gleichzeitig. Um mehrere Knoten wiederherzustellen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Raster replizierte Daten enthält, verwenden Sie die `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option, wobei `--nodes` ist der Hostname (Systemname), um den gesamten Speicherknoten zu reparieren.

Dieser Befehl repariert die replizierten Daten auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Beim Wiederherstellen von Objektdaten wird die Warnung „Objekte verloren“ ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Speicherknoten im gesamten System können Warnungen ausgelöst werden. Sie sollten die Ursache des Verlusts ermitteln und feststellen, ob eine Wiederherstellung möglich ist. Sehen "Untersuchen Sie verlorene Gegenstände" .

Löschcodierte (EC) Daten

Wenn Ihr Grid Erasure-Coding-Daten enthält, verwenden Sie die `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option, wobei `--nodes` ist der Hostname (Systemname), um den gesamten Speicherknoten zu reparieren.

Dieser Befehl repariert die erasure-coded Daten auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Die Operation gibt einen eindeutigen `repair ID` das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese `repair ID` um den Fortschritt und das Ergebnis der `repair_data` Betrieb. Nach Abschluss des Wiederherstellungsprozesses wird keine weitere Rückmeldung zurückgegeben.

Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige der Volumes ausgefallen sind, reparieren Sie die betroffenen Volumes. Befolgen Sie die Anweisungen für **replizierte Daten**, **löschcodierte (EC) Daten** oder beides, je nachdem, ob Sie replizierte Daten, löschcodierte (EC) Daten oder beides verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zuwenn alle Volumes ausgefallen sind .

Geben Sie die Volume-IDs im Hexadezimalformat ein. Zum Beispiel, `0000` ist der erste Band und `000F` ist der sechzehnte Band. Sie können ein Volume, einen Volumebereich oder mehrere Volumes angeben, die nicht in einer Sequenz stehen.

Alle Volumes müssen sich auf demselben Speicherknoten befinden. Wenn Sie Volumes für mehr als einen Speicherknoten wiederherstellen müssen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Grid replizierte Daten enthält, verwenden Sie die `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wo `--nodes` ist der Hostname des Knotens). Fügen Sie dann entweder die `--volumes` oder `--volume-range` Option, wie in den folgenden Beispielen gezeigt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf dem Volume wieder her `0002` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf allen Volumes im Bereich wieder her `0003` Zu `0009` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Mehrere Volumes, nicht in einer Sequenz: Dieser Befehl stellt replizierte Daten auf Volumes wieder her `0001` , `0005` , Und `0008` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Beim Wiederherstellen von Objektdaten wird die Warnung „Objekte verloren“ ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Speicherknoten im gesamten System können Warnungen ausgelöst werden. Beachten Sie die Alarmbeschreibung und die empfohlenen Maßnahmen, um die Ursache des Verlusts zu ermitteln und festzustellen, ob eine Wiederherstellung möglich ist.

Löschcodierte (EC) Daten

Wenn Ihr Grid Erasure-Coding-Daten enthält, verwenden Sie die `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wo `--nodes` ist der Hostname des Knotens). Fügen Sie dann entweder die `--volumes` oder `--volume-range` Option, wie in den folgenden Beispielen gezeigt.

Einzelnes Volume: Dieser Befehl stellt löschcodierte Daten auf dem Volume wieder her `0007` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt die löschcodierten Daten auf allen Volumes im Bereich wieder her `0004` Zu `0006` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Mehrere Volumes, nicht in einer Sequenz: Dieser Befehl stellt erased-coded Daten auf Volumes wieder her `000A` , `000C` , Und `000E` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Operation gibt einen eindeutigen `repair ID` das identifiziert dies `repair_data`

Betrieb. Verwenden Sie diese `repair ID` um den Fortschritt und das Ergebnis der `repair_data` Betrieb. Nach Abschluss des Wiederherstellungsprozesses wird keine weitere Rückmeldung zurückgegeben.

> Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

Monitorreparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **löschcodierte (EC) Daten** oder beides verwenden.

Sie können auch den Status der laufenden Volume-Wiederherstellungsaufträge überwachen und einen Verlauf der abgeschlossenen Wiederherstellungsaufträge anzeigen."Grid-Manager" .

Replizierte Daten

- Um einen geschätzten Prozentsatz der Fertigstellung der replizierten Reparatur zu erhalten, addieren Sie die `show-replicated-repair-status` Option zum Befehl „repair-data“.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob die Reparaturen abgeschlossen sind:
  a. Wählen Sie **NODES** > ***Speicherknoten wird repariert*** > **ILM**.
  b. Überprüfen Sie die Attribute im Abschnitt „Bewertung“. Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut **Warten – Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
  a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
  b. Wählen Sie ***grid*** > ***Reparierter Speicherknoten*** > **LDR** > **Datenspeicher**.
  c. Verwenden Sie eine Kombination der folgenden Attribute, um so gut wie möglich zu bestimmen, ob replizierte Reparaturen abgeschlossen sind.

> ⓘ Möglicherweise liegen Cassandra-Inkonsistenzen vor und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

    - **Reparaturversuche (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt replizierter Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Speicherknoten versucht, ein Hochrisikoobjekt zu reparieren. Wenn dieses Attribut über einen Zeitraum, der länger ist als der aktuelle Scanzeitraum (bereitgestellt durch das Attribut **Scanzeitraum – Geschätzt**), nicht ansteigt, bedeutet dies, dass beim ILM-Scan auf keinem Knoten ein Hochrisikoobjekt gefunden wurde, das repariert werden muss.

> ⓘ Hochrisikoobjekte sind Objekte, bei denen die Gefahr eines vollständigen Verlusts besteht. Dies schließt keine Objekte ein, die ihrer ILM-Konfiguration nicht entsprechen.

    - **Scan-Zeitraum – Geschätzt (XSCM)**: Verwenden Sie dieses Attribut, um abzuschätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn das Attribut **Reparaturversuche** über einen Zeitraum, der länger als der aktuelle Scanzeitraum ist, nicht ansteigt, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt wurden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period – Estimated (XSCM)** gilt für das gesamte Raster und ist das Maximum aller Knoten-Scan-Perioden. Sie können den Attributverlauf **Scan-Zeitraum – Geschätzt** für das Raster abfragen, um einen geeigneten Zeitrahmen zu bestimmen.

Löschcodierte (EC) Daten

So überwachen Sie die Reparatur von Erasure-Code-Daten und wiederholen alle möglicherweise fehlgeschlagenen Anfragen:

1. Bestimmen Sie den Status der Datenreparaturen mit Erasure Code:
   - Wählen Sie **SUPPORT** > **Tools** > **Metriken**, um die geschätzte Zeit bis zur Fertigstellung und den Fertigstellungsgrad für den aktuellen Auftrag anzuzeigen. Wählen Sie dann im Abschnitt „Grafana“ die Option „EC-Übersicht“ aus. Sehen Sie sich die Dashboards **Geschätzte Zeit bis zur Fertigstellung des Grid EC-Jobs** und **Prozentsatz der Fertigstellung des Grid EC-Jobs**

an.

- Verwenden Sie diesen Befehl, um den Status eines bestimmten `repair-data` Betrieb:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

  ```
  repair-data show-ec-repair-status
  ```

Die Ausgabe listet Informationen auf, einschließlich `repair ID` , für alle bisherigen und laufenden Reparaturen.

2. Wenn die Ausgabe zeigt, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie die `--repair-id` Option zum erneuten Versuch der Reparatur.

   Mit diesem Befehl wird eine fehlgeschlagene Knotenreparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Mit diesem Befehl wird eine fehlgeschlagene Volumereparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Überprüfen des Speicherstatus nach der Wiederherstellung von Speichervolumes

Nach der Wiederherstellung der Speichervolumes müssen Sie überprüfen, ob der gewünschte Status des Speicherknotens auf „Online“ eingestellt ist, und sicherstellen, dass der Status standardmäßig „Online“ ist, wenn der Speicherknotenserver neu gestartet wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Überprüfen Sie die Werte von **Wiederhergestellter Speicherknoten** > **LDR** > **Speicher** > **Speicherstatus – Gewünscht** und **Speicherstatus – Aktuell**.

   Der Wert beider Attribute sollte „Online“ sein.

3. Wenn „Speicherstatus – Gewünscht“ auf „Schreibgeschützt“ eingestellt ist, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf die Registerkarte **Konfiguration**.
   b. Wählen Sie aus der Dropdown-Liste **Speicherstatus – Gewünscht** die Option **Online** aus.
   c. Klicken Sie auf **Änderungen übernehmen**.

d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherstatus – Gewünscht** und **Speicherstatus – Aktuell** auf „Online“ aktualisiert wurden.

Wiederherstellung nach einem Systemlaufwerksfehler

Warnungen zur Wiederherstellung des Storage Node-Systemlaufwerks

Bevor Sie ein ausgefallenes Systemlaufwerk eines Storage Node wiederherstellen, lesen Sie die allgemeinen"Warnungen und Überlegungen zur Wiederherstellung von Grid-Knoten" und die folgenden spezifischen Warnungen.

Speicherknoten verfügen über eine Cassandra-Datenbank, die Objektmetadaten enthält. Die Cassandra-Datenbank kann unter folgenden Umständen neu erstellt werden:

- Ein Speicherknoten wird wieder online gebracht, nachdem er länger als 15 Tage offline war.
- Ein Speichervolume ist ausgefallen und wurde wiederhergestellt.
- Das Systemlaufwerk und ein oder mehrere Speichervolumes fallen aus und werden wiederhergestellt.

Beim Neuaufbau von Cassandra verwendet das System Informationen von anderen Speicherknoten. Wenn zu viele Speicherknoten offline sind, sind einige Cassandra-Daten möglicherweise nicht verfügbar. Wenn Cassandra vor Kurzem neu erstellt wurde, sind die Cassandra-Daten im gesamten Grid möglicherweise noch nicht konsistent. Es kann zu Datenverlust kommen, wenn Cassandra neu erstellt wird, während zu viele Speicherknoten offline sind, oder wenn zwei oder mehr Speicherknoten innerhalb von 15 Tagen neu erstellt werden.

Wenn mehr als ein Speicherknoten ausgefallen ist (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es könnte zu Datenverlust kommen.

Wenn dies der zweite Speicherknotenausfall innerhalb von weniger als 15 Tagen nach einem Speicherknotenausfall oder einer Wiederherstellung ist, wenden Sie sich an den technischen Support. Der Wiederaufbau von Cassandra auf zwei oder mehr Speicherknoten innerhalb von 15 Tagen kann zu Datenverlust führen.

Wenn an einem Standort mehr als ein Speicherknoten ausgefallen ist, ist möglicherweise ein Standortwiederherstellungsverfahren erforderlich. Sehen "So stellt der technische Support eine Site wieder her" .

Wenn sich dieser Speicherknoten im schreibgeschützten Wartungsmodus befindet, um das Abrufen von Objekten durch einen anderen Speicherknoten mit ausgefallenen Speichervolumes zu ermöglichen, stellen Sie Volumes auf dem Speicherknoten mit ausgefallenen Speichervolumes wieder her, bevor Sie diesen ausgefallenen Speicherknoten wiederherstellen. Siehe die Anweisungen zu"Wiederherstellung nach einem Speicherdatenträgerfehler, wenn das Systemlaufwerk intakt ist" .

Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und die Kopie auf einem ausgefallenen Speichervolume vorhanden ist, können Sie das Objekt nicht wiederherstellen.

Ersetzen des Speicherknotens

Wenn das Systemlaufwerk ausgefallen ist, müssen Sie zuerst den Speicherknoten ersetzen.

Sie müssen das Knotenaustauschverfahren für Ihre Plattform auswählen. Die Schritte zum Ersetzen eines Knotens sind für alle Arten von Rasterknoten gleich.

> Dieses Verfahren gilt nur für softwarebasierte Speicherknoten. Sie müssen ein anderes Verfahren befolgen, um"Wiederherstellen eines Appliance-Speicherknotens" .

Linux: Wenn Sie nicht sicher sind, ob Ihr Systemlaufwerk ausgefallen ist, befolgen Sie die Anweisungen zum Ersetzen des Knotens, um festzustellen, welche Wiederherstellungsschritte erforderlich sind.

Plattform	Verfahren
VMware	"Ersetzen eines VMware-Knotens"
Linux	"Ersetzen eines Linux-Knotens"
OpenStack	Von NetApp bereitgestellte Festplattendateien und Skripts für virtuelle Maschinen für OpenStack werden für Wiederherstellungsvorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Bereitstellung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann die Anweisungen für"Ersetzen eines Linux-Knotens" .

Wählen Sie „Wiederherstellung starten“, um den Speicherknoten zu konfigurieren.

Nachdem Sie einen Speicherknoten ersetzt haben, müssen Sie im Grid Manager „Wiederherstellung starten“ auswählen, um den neuen Knoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben die Bereitstellungspassphrase.
- Sie haben den Ersatzknoten bereitgestellt und konfiguriert.
- Sie verfügen über das Startdatum aller Reparaturaufträge für löschcodierte Daten.
- Sie haben überprüft, dass der Speicherknoten innerhalb der letzten 15 Tage nicht neu erstellt wurde.

Informationen zu diesem Vorgang

Wenn der Speicherknoten als Container auf einem Linux-Host installiert ist, müssen Sie diesen Schritt nur ausführen, wenn einer der folgenden Punkte zutrifft:

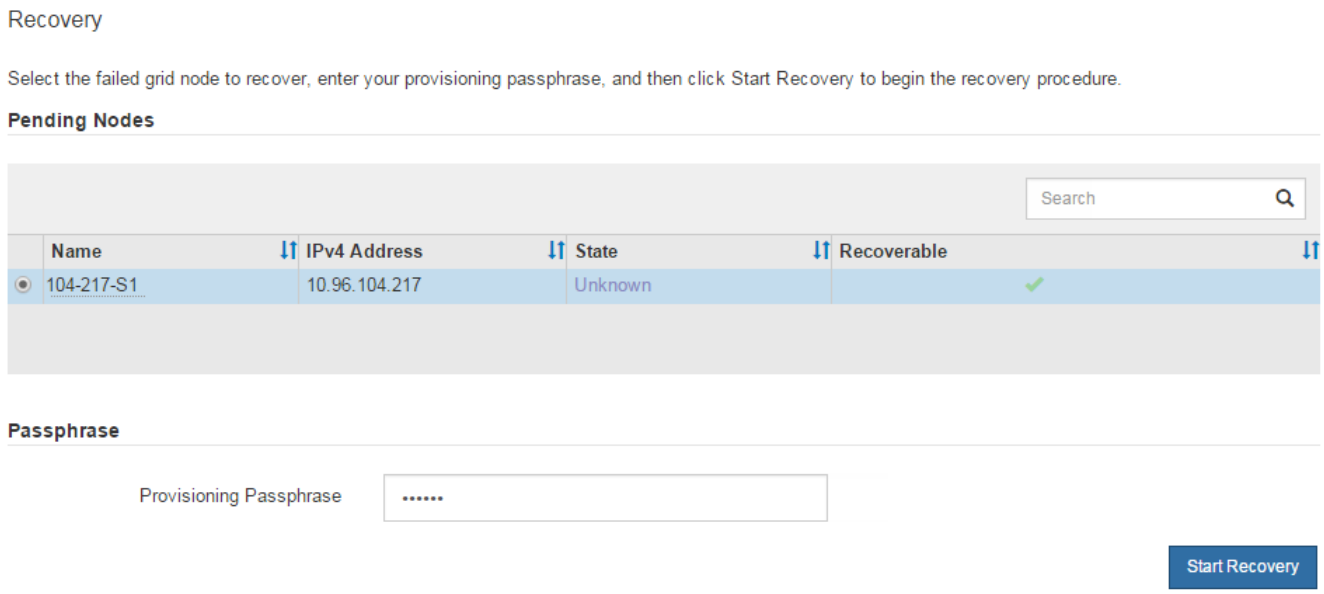
- Sie mussten die `--force` Flag zum Importieren des Knotens, oder Sie haben `storagegrid node force-recovery` *`node-name`*
- Sie mussten eine vollständige Neuinstallation des Knotens durchführen oder /var/local wiederherstellen.

Schritte

1. Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Wiederherstellung**.
2. Wählen Sie in der Liste „Ausstehende Knoten“ den Grid-Knoten aus, den Sie wiederherstellen möchten.

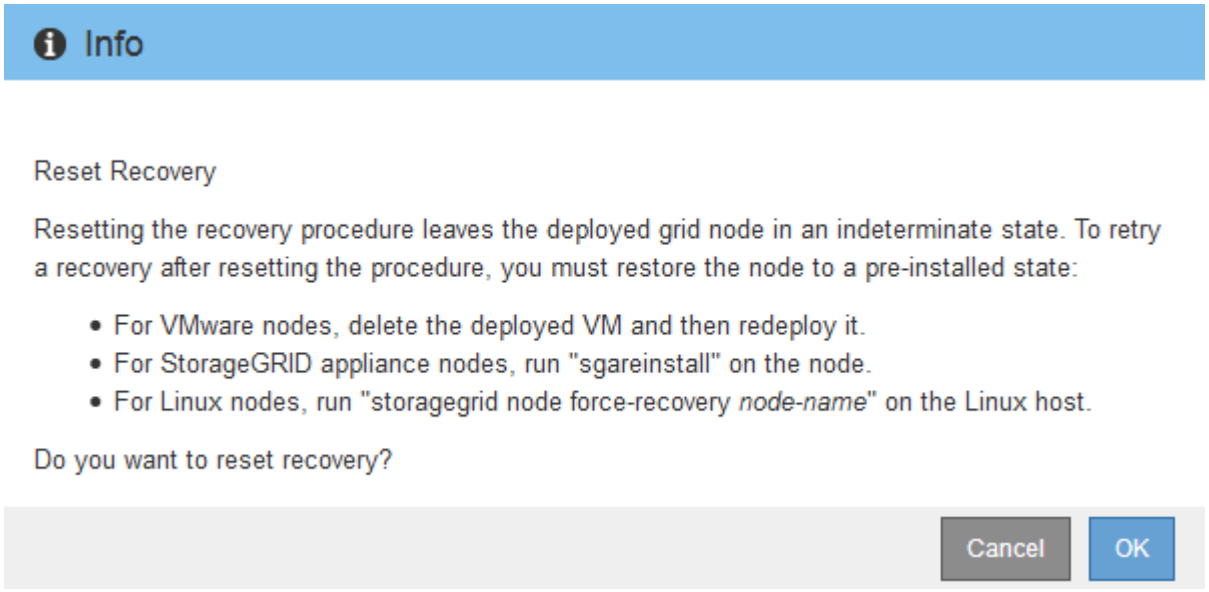
   Knoten werden in der Liste angezeigt, nachdem sie ausgefallen sind. Sie können einen Knoten jedoch erst auswählen, wenn er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Bereitstellungspassphrase** ein.
4. Klicken Sie auf **Wiederherstellung starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Grid-Knoten wird wiederhergestellt“.

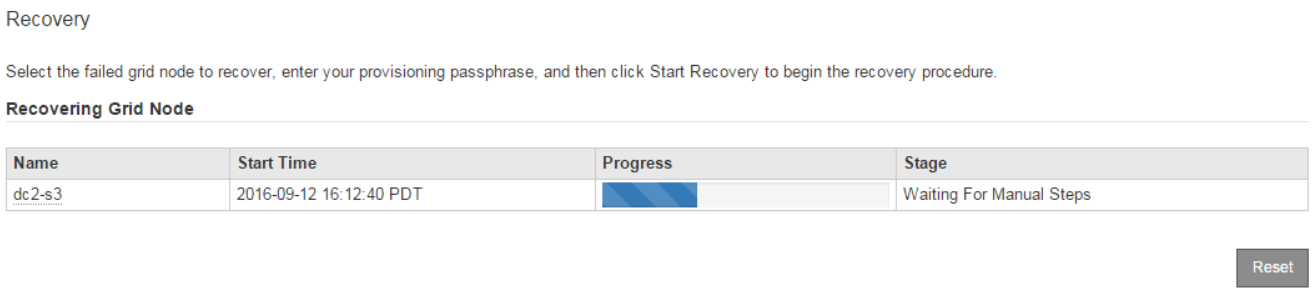
> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das darauf hinweist, dass der Knoten in einem unbestimmten Zustand verbleibt, wenn Sie die Prozedur zurücksetzen.



Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Verfahrens wiederholen möchten, müssen Sie den Knoten wie folgt in einen vorinstallierten Zustand zurückversetzen:

- **VMware**: Löschen Sie den bereitgestellten virtuellen Grid-Knoten. Wenn Sie dann bereit sind, die Wiederherstellung neu zu starten, stellen Sie den Knoten erneut bereit.
- **Linux**: Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen: `storagegrid node force-recovery node-name`

6. Wenn der Speicherknoten die Phase „Warten auf manuelle Schritte“ erreicht, gehen Sie zu"Speichervolumes erneut mounten und neu formatieren (manuelle Schritte)" .



Speichervolumes erneut mounten und neu formatieren (manuelle Schritte)

Sie müssen zwei Skripte manuell ausführen, um beibehaltene Speichervolumes erneut bereitzustellen und alle ausgefallenen Speichervolumes neu zu formatieren. Das erste Skript stellt Volumes erneut bereit, die ordnungsgemäß als StorageGRID Speichervolumes formatiert sind. Das zweite Skript formatiert alle nicht gemounteten Volumes neu, erstellt Cassandra bei Bedarf neu und startet die Dienste.

Bevor Sie beginnen

- Sie haben die Hardware aller ausgefallenen Speichervolumes, von denen Sie wissen, dass sie ersetzt werden müssen, bereits ausgetauscht.

  Ausführen des `sn-remount-volumes` Skript kann Ihnen dabei helfen, weitere ausgefallene Speichervolumes zu identifizieren.

- Sie haben überprüft, dass keine Außerbetriebnahme eines Speicherknotens im Gange ist, oder Sie haben den Vorgang zur Außerbetriebnahme des Knotens angehalten. (Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Außerbetriebnahme**.)
- Sie haben überprüft, dass keine Erweiterung im Gange ist. (Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Erweiterung**.)
- Du hast"die Warnungen zur Wiederherstellung des Storage Node-Systemlaufwerks überprüft" .

> Wenden Sie sich an den technischen Support, wenn mehr als ein Speicherknoten offline ist oder wenn ein Speicherknoten in diesem Raster in den letzten 15 Tagen neu erstellt wurde. Führen Sie nicht die `sn-recovery-postinstall.sh` Skript. Der Wiederaufbau von Cassandra auf zwei oder mehr Speicherknoten innerhalb von 15 Tagen kann zu Datenverlust führen.

Informationen zu diesem Vorgang

Um dieses Verfahren abzuschließen, führen Sie die folgenden übergeordneten Aufgaben aus:

- Melden Sie sich beim wiederhergestellten Speicherknoten an.
- Führen Sie den `sn-remount-volumes` Skript zum erneuten Mounten ordnungsgemäß formatierter Speichervolumes. Wenn dieses Skript ausgeführt wird, geschieht Folgendes:
  - Mountet und unmountet jedes Speichervolume, um das XFS-Journal wiederzugeben.
  - Führt eine Konsistenzprüfung der XFS-Datei durch.
  - Wenn das Dateisystem konsistent ist, wird ermittelt, ob es sich bei dem Speichervolume um ein ordnungsgemäß formatiertes StorageGRID -Speichervolume handelt.
  - Wenn das Speichervolume richtig formatiert ist, wird das Speichervolume erneut bereitgestellt. Alle vorhandenen Daten auf dem Datenträger bleiben erhalten.
- Überprüfen Sie die Skriptausgabe und beheben Sie alle Probleme.
- Führen Sie den `sn-recovery-postinstall.sh` Skript. Wenn dieses Skript ausgeführt wird, geschieht Folgendes.

> Starten Sie einen Storage Node während der Wiederherstellung nicht neu, bevor Sie `sn-recovery-postinstall.sh` um die ausgefallenen Speichervolumes neu zu formatieren und Objektmetadaten wiederherzustellen. Neustart des Speicherknotens vor `sn-recovery-postinstall.sh` „completes“ verursacht Fehler bei Diensten, die versuchen zu starten, und führt dazu, dass die Knoten der StorageGRID Appliance den Wartungsmodus verlassen. Siehe den Schritt fürPost-Installationsskript .

  - Formatiert alle Speichervolumes neu, die der `sn-remount-volumes` Das Skript konnte nicht gemountet werden oder war falsch formatiert.

> Wenn ein Speichervolume neu formatiert wird, gehen alle Daten auf diesem Volume verloren. Sie müssen ein zusätzliches Verfahren ausführen, um Objektdaten von anderen Speicherorten im Grid wiederherzustellen, vorausgesetzt, dass ILM-Regeln zum Speichern von mehr als einer Objektkopie konfiguriert wurden.

  - Baut die Cassandra-Datenbank auf dem Knoten bei Bedarf neu auf.
  - Startet die Dienste auf dem Speicherknoten.

Schritte

1. Melden Sie sich beim wiederhergestellten Speicherknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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 das erste Skript aus, um alle ordnungsgemäß formatierten Speichervolumes erneut zu mounten.

> Wenn alle Speichervolumes neu sind und formatiert werden müssen oder wenn alle Speichervolumes ausgefallen sind, können Sie diesen Schritt überspringen und das zweite Skript ausführen, um alle nicht gemounteten Speichervolumes neu zu formatieren.

a. Führen Sie das Skript aus: `sn-remount-volumes`

   Die Ausführung dieses Skripts auf Speichervolumes mit Daten kann Stunden dauern.

b. Überprüfen Sie während der Ausführung des Skripts die Ausgabe und beantworten Sie alle Eingabeaufforderungen.

   > Bei Bedarf können Sie die `tail -f` Befehl zum Überwachen des Inhalts der Protokolldatei des Skripts(`/var/local/log/sn-remount-volumes.log`) . Die Protokolldatei enthält detailliertere Informationen als die Befehlszeilenausgabe.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
```

```
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
```

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

In der Beispielausgabe wurde ein Speichervolume erfolgreich erneut bereitgestellt und bei drei Speichervolumes traten Fehler auf.

- `/dev/sdb`hat die Konsistenzprüfung des XFS-Dateisystems bestanden und verfügte über eine gültige Volumestruktur, sodass es erfolgreich erneut gemountet werden konnte. Daten auf Geräten, die durch das Skript erneut gemountet werden, bleiben erhalten.
- `/dev/sdc`Die Konsistenzprüfung des XFS-Dateisystems ist fehlgeschlagen, da das Speichervolume neu oder beschädigt war.
- `/dev/sdd`konnte nicht gemountet werden, da die Festplatte nicht initialisiert wurde oder der Superblock der Festplatte beschädigt war. Wenn das Skript ein Speichervolume nicht mounten kann, werden Sie gefragt, ob Sie die Konsistenzprüfung des Dateisystems ausführen möchten.
  - Wenn das Speichervolume an eine neue Festplatte angeschlossen ist, antworten Sie mit **N** auf die Eingabeaufforderung. Sie müssen das Dateisystem auf einer neuen Festplatte nicht überprüfen.
  - Wenn das Speichervolume an eine vorhandene Festplatte angeschlossen ist, antworten Sie mit **J** auf die Eingabeaufforderung. Mithilfe der Ergebnisse der Dateisystemprüfung können Sie die Ursache der Beschädigung ermitteln. Die Ergebnisse werden gespeichert im `/var/local/log/sn-remount-volumes.log` Protokolldatei.
- `/dev/sde`hat die Konsistenzprüfung des XFS-Dateisystems bestanden und hatte eine gültige Volume-Struktur; die LDR-Knoten-ID in der VolID-Datei stimmte jedoch nicht mit der ID für diesen Speicherknoten überein (die `configured LDR noid` oben angezeigt). Diese Meldung zeigt an, dass dieses Volume zu einem anderen Speicherknoten gehört.

3. Überprüfen Sie die Skriptausgabe und beheben Sie alle Probleme.

> Wenn ein Speichervolume die Konsistenzprüfung des XFS-Dateisystems nicht bestanden hat oder nicht gemountet werden konnte, überprüfen Sie die Fehlermeldungen in der Ausgabe sorgfältig. Sie müssen die Auswirkungen der Ausführung des `sn-recovery-postinstall.sh` Skript auf diesen Datenträgern.

a. Überprüfen Sie, ob die Ergebnisse einen Eintrag für alle von Ihnen erwarteten Bände enthalten. Wenn Volumes nicht aufgeführt sind, führen Sie das Skript erneut aus.

b. Überprüfen Sie die Nachrichten für alle gemounteten Geräte. Stellen Sie sicher, dass keine Fehler vorliegen, die darauf hinweisen, dass ein Speichervolume nicht zu diesem Speicherknoten gehört.

   Im Beispiel wird die Ausgabe für `/dev/sde` enthält die folgende Fehlermeldung:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Wenn ein Speichervolume als zu einem anderen Speicherknoten gehörend gemeldet wird, wenden Sie sich an den technischen Support. Wenn Sie das `sn-recovery-postinstall.sh` Skript wird das Speichervolume neu formatiert, was zu Datenverlust führen kann.

c. Wenn Speichergeräte nicht gemountet werden konnten, notieren Sie sich den Gerätenamen und reparieren oder ersetzen Sie das Gerät.

Sie müssen alle Speichergeräte reparieren oder ersetzen, die nicht gemountet werden konnten.

Sie verwenden den Gerätenamen, um die Volume-ID zu suchen, die beim Ausführen des `repair-data` Skript zum Wiederherstellen von Objektdaten auf dem Volume (nächstes Verfahren).

d. Nachdem Sie alle nicht einhängbaren Geräte repariert oder ersetzt haben, führen Sie den `sn-remount-volumes` Skript erneut, um zu bestätigen, dass alle Speichervolumes, die erneut gemountet werden können, erneut gemountet wurden.

Wenn ein Speichervolume nicht gemountet werden kann oder nicht richtig formatiert ist und Sie mit dem nächsten Schritt fortfahren, werden das Volume und alle darauf befindlichen Daten gelöscht. Wenn Sie zwei Kopien der Objektdaten hatten, verfügen Sie bis zum Abschluss des nächsten Vorgangs (Wiederherstellen der Objektdaten) nur über eine einzige Kopie.

Führen Sie nicht die `sn-recovery-postinstall.sh` Skript, wenn Sie der Meinung sind, dass die auf einem ausgefallenen Speichervolume verbleibenden Daten nicht von einer anderen Stelle im Grid wiederhergestellt werden können (z. B. wenn Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie erstellt, oder wenn Volumes auf mehreren Knoten ausgefallen sind). Wenden Sie sich stattdessen an den technischen Support, um zu erfahren, wie Sie Ihre Daten wiederherstellen können.

4. Führen Sie den `sn-recovery-postinstall.sh` Skript: `sn-recovery-postinstall.sh`

Dieses Skript formatiert alle Speichervolumes neu, die nicht gemountet werden konnten oder bei denen festgestellt wurde, dass sie nicht richtig formatiert waren. Es erstellt bei Bedarf die Cassandra-Datenbank auf dem Knoten neu und startet die Dienste auf dem Speicherknoten.

Beachten Sie Folgendes:

- Die Ausführung des Skripts kann Stunden dauern.
- Im Allgemeinen sollten Sie die SSH-Sitzung in Ruhe lassen, während das Skript ausgeführt wird.
- Drücken Sie nicht **Strg+C**, während die SSH-Sitzung aktiv ist.
- Das Skript wird im Hintergrund ausgeführt, wenn eine Netzwerkstörung auftritt und die SSH-Sitzung beendet, aber Sie können den Fortschritt auf der Wiederherstellungsseite verfolgen.
- Wenn der Speicherknoten den RSM-Dienst verwendet, kann es vorkommen, dass das Skript 5 Minuten lang blockiert, während die Knotendienste neu gestartet werden. Diese 5-minütige Verzögerung ist immer dann zu erwarten, wenn der RSM-Dienst zum ersten Mal gestartet wird.

Der RSM-Dienst ist auf Speicherknoten vorhanden, die den ADC-Dienst enthalten.

Einige StorageGRID Wiederherstellungsverfahren verwenden Reaper zur Durchführung von Cassandra-Reparaturen. Reparaturen erfolgen automatisch, sobald die entsprechenden bzw. erforderlichen Leistungen begonnen haben. Möglicherweise bemerken Sie eine Skriptausgabe, in der „Reaper“ oder „Cassandra-Reparatur“ erwähnt wird. Wenn eine Fehlermeldung angezeigt wird, die darauf hinweist, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

5. Als `sn-recovery-postinstall.sh` Skript ausgeführt wird, überwachen Sie die Wiederherstellungsseite im Grid Manager.

   Der Fortschrittsbalken und die Spalte „Phase“ auf der Wiederherstellungsseite bieten einen allgemeinen Status der `sn-recovery-postinstall.sh` Skript.

6. Nach dem `sn-recovery-postinstall.sh` Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speichervolumes wiederherstellen, die vom Skript formatiert wurden.

   Das Skript fragt, ob Sie den Volume-Wiederherstellungsprozess des Grid Managers verwenden möchten.

   - In den meisten Fällen sollten Sie"Wiederherstellen von Objektdaten mit Grid Manager" . Antwort `y` um den Grid Manager zu verwenden.
   - In seltenen Fällen, beispielsweise wenn Sie vom technischen Support dazu aufgefordert werden oder wenn Sie wissen, dass der Ersatzknoten weniger Volumes für die Objektspeicherung zur Verfügung hat als der ursprüngliche Knoten, müssen Sie"Objektdaten manuell wiederherstellen" mithilfe der `repair-data` Skript. Wenn einer dieser Fälle zutrifft, antworten Sie `n` .

     Wenn Sie antworten `n` zur Verwendung des Volume-Wiederherstellungsprozesses des Grid Managers (manuelle Wiederherstellung der Objektdaten):

     - Sie können Objektdaten mit Grid Manager nicht wiederherstellen.
     - Sie können den Fortschritt manueller Wiederherstellungsaufträge mit Grid Manager überwachen.

   Nachdem Sie Ihre Auswahl getroffen haben, wird das Skript abgeschlossen und die nächsten Schritte zur Wiederherstellung der Objektdaten werden angezeigt. Nachdem Sie diese Schritte überprüft haben, drücken Sie eine beliebige Taste, um zur Befehlszeile zurückzukehren.

Objektdaten auf Speichervolume wiederherstellen (Systemlaufwerkfehler)

Nachdem Sie Speichervolumes für einen Speicherknoten wiederhergestellt haben, der kein Gerät ist, können Sie die replizierten oder erasure-coded Objektdaten wiederherstellen, die beim Ausfall des Speicherknotens verloren gegangen sind.

Welches Verfahren soll ich anwenden?

Stellen Sie Objektdaten nach Möglichkeit mithilfe der Seite **Volume-Wiederherstellung** im Grid Manager wieder her.

- Wenn die Volumes unter **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** aufgelistet sind, stellen Sie die Objektdaten mithilfe des"Seite zur Volume-Wiederherstellung im Grid Manager" .

- Wenn die Volumes nicht unter **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** aufgeführt sind, befolgen Sie die folgenden Schritte zur Verwendung des `repair-data` Skript zum Wiederherstellen von Objektdaten.

  Wenn der wiederhergestellte Storage Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie die `repair-data` Skript.

> Das Skript „repair-data“ ist veraltet und wird in einer zukünftigen Version entfernt. Verwenden Sie nach Möglichkeit die"Volume-Wiederherstellungsverfahren im Grid Manager" .

Verwenden Sie die `repair-data` Skript zum Wiederherstellen von Objektdaten

Bevor Sie beginnen

- Sie haben bestätigt, dass der wiederhergestellte Speicherknoten den Verbindungsstatus **Verbunden** hat. auf der Registerkarte **KNOTEN** > **Übersicht** im Grid Manager.

Informationen zu diesem Vorgang

Objektdaten können von anderen Speicherknoten oder einem Cloud-Speicherpool wiederhergestellt werden, vorausgesetzt, die ILM-Regeln des Grids wurden so konfiguriert, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und diese Kopie auf einem Speichervolume vorhanden war, das ausgefallen ist, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, muss StorageGRID mehrere Anfragen an den Endpunkt des Cloud-Speicherpools senden, um die Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Wiederherstellungszeitraums und der damit verbundenen Kosten zu erhalten.

Über die `repair-data` Skript

Um Objektdaten wiederherzustellen, führen Sie den `repair-data` Skript. Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans, um sicherzustellen, dass die ILM-Regeln eingehalten werden.

Wählen Sie unten **Replizierte Daten** oder **Erasure-coded (EC) Daten**, um die verschiedenen Optionen für die `repair-data` Skript, je nachdem, ob Sie replizierte Daten oder erasure-coded Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssätze ausführen.

> Weitere Informationen zum `repair-data` Skript, geben Sie `repair-data --help` von der Befehlszeile des primären Admin-Knotens.

> Das Skript „repair-data“ ist veraltet und wird in einer zukünftigen Version entfernt. Verwenden Sie nach Möglichkeit die"Volume-Wiederherstellungsverfahren im Grid Manager" .

Replizierte Daten

Zum Wiederherstellen replizierter Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Sie können Reparaturen replizierter Daten mit diesem Befehl verfolgen:

```
repair-data show-replicated-repair-status
```

Löschcodierte (EC) Daten

Zum Wiederherstellen von Erasure-Code-Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Sie können die Reparatur von Erasure-Codierten Daten mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```

> Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Wenn jedoch nicht alle löschcodierten Daten berücksichtigt werden können, kann die Reparatur nicht abgeschlossen werden. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

> Der EC-Reparaturauftrag reserviert vorübergehend viel Speicherplatz. Möglicherweise werden Speicherwarnungen ausgelöst, die jedoch nach Abschluss der Reparatur behoben werden. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturjob abgeschlossen ist, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Hostnamen für Speicherknoten suchen

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. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicherknotens für die wiederhergestellten Speichervolumes zu finden. Um eine Liste aller Knoten im Raster anzuzeigen, geben

Sie Folgendes ein: `cat /etc/hosts` .

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Speichervolumes ausgefallen sind, reparieren Sie den gesamten Knoten. Befolgen Sie die Anweisungen für **replizierte Daten**, **löschcodierte (EC) Daten** oder beides, je nachdem, ob Sie replizierte Daten, löschcodierte (EC) Daten oder beides verwenden.

Wenn nur einige Volumes ausgefallen sind, gehen Sie zuwenn nur einige Volumes ausgefallen sind .

> Du kannst nicht rennen `repair-data` Operationen für mehr als einen Knoten gleichzeitig. Um mehrere Knoten wiederherzustellen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Raster replizierte Daten enthält, verwenden Sie die `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option, wobei `--nodes` ist der Hostname (Systemname), um den gesamten Speicherknoten zu reparieren.

Dieser Befehl repariert die replizierten Daten auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Beim Wiederherstellen von Objektdaten wird die Warnung „Objekte verloren“ ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Speicherknoten im gesamten System können Warnungen ausgelöst werden. Sie sollten die Ursache des Verlusts ermitteln und feststellen, ob eine Wiederherstellung möglich ist. Sehen "Untersuchen Sie verlorene Gegenstände" .

Löschcodierte (EC) Daten

Wenn Ihr Grid Erasure-Coding-Daten enthält, verwenden Sie die `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option, wobei `--nodes` ist der Hostname (Systemname), um den gesamten Speicherknoten zu reparieren.

Dieser Befehl repariert die erasure-coded Daten auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Die Operation gibt einen eindeutigen `repair ID` das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese `repair ID` um den Fortschritt und das Ergebnis der `repair_data` Betrieb. Nach Abschluss des Wiederherstellungsprozesses wird keine weitere Rückmeldung zurückgegeben.

Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige der Volumes ausgefallen sind, reparieren Sie die betroffenen Volumes. Befolgen Sie die Anweisungen für **replizierte Daten**, **löschcodierte (EC) Daten** oder beides, je nachdem, ob Sie replizierte Daten, löschcodierte (EC) Daten oder beides verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zuwenn alle Volumes ausgefallen sind .

Geben Sie die Volume-IDs im Hexadezimalformat ein. Zum Beispiel, `0000` ist der erste Band und `000F` ist der sechzehnte Band. Sie können ein Volume, einen Volumebereich oder mehrere Volumes angeben, die nicht in einer Sequenz stehen.

Alle Volumes müssen sich auf demselben Speicherknoten befinden. Wenn Sie Volumes für mehr als einen Speicherknoten wiederherstellen müssen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Grid replizierte Daten enthält, verwenden Sie die `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wo `--nodes` ist der Hostname des Knotens). Fügen Sie dann entweder die `--volumes` oder `--volume-range` Option, wie in den folgenden Beispielen gezeigt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf dem Volume wieder her `0002` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf allen Volumes im Bereich wieder her `0003` Zu `0009` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Mehrere Volumes, nicht in einer Sequenz: Dieser Befehl stellt replizierte Daten auf Volumes wieder her `0001` , `0005` , Und `0008` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Beim Wiederherstellen von Objektdaten wird die Warnung „Objekte verloren“ ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Speicherknoten im gesamten System können Warnungen ausgelöst werden. Beachten Sie die Alarmbeschreibung und die empfohlenen Maßnahmen, um die Ursache des Verlusts zu ermitteln und festzustellen, ob eine Wiederherstellung möglich ist.

Löschcodierte (EC) Daten

Wenn Ihr Grid Erasure-Coding-Daten enthält, verwenden Sie die `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wo `--nodes` ist der Hostname des Knotens). Fügen Sie dann entweder die `--volumes` oder `--volume-range` Option, wie in den folgenden Beispielen gezeigt.

Einzelnes Volume: Dieser Befehl stellt löschcodierte Daten auf dem Volume wieder her `0007` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt die löschcodierten Daten auf allen Volumes im Bereich wieder her `0004` Zu `0006` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Mehrere Volumes, nicht in einer Sequenz: Dieser Befehl stellt erased-coded Daten auf Volumes wieder her `000A` , `000C` , Und `000E` auf einem Speicherknoten namens SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Operation gibt einen eindeutigen `repair ID` das identifiziert dies `repair_data`

Betrieb. Verwenden Sie diese `repair ID` um den Fortschritt und das Ergebnis der `repair_data` Betrieb. Nach Abschluss des Wiederherstellungsprozesses wird keine weitere Rückmeldung zurückgegeben.

> Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

Monitorreparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **löschcodierte (EC) Daten** oder beides verwenden.

Sie können auch den Status der laufenden Volume-Wiederherstellungsaufträge überwachen und einen Verlauf der abgeschlossenen Wiederherstellungsaufträge anzeigen."Grid-Manager" .

Replizierte Daten

- Um einen geschätzten Prozentsatz der Fertigstellung der replizierten Reparatur zu erhalten, addieren Sie die `show-replicated-repair-status` Option zum Befehl „repair-data“.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob die Reparaturen abgeschlossen sind:
  a. Wählen Sie **NODES** > ***Speicherknoten wird repariert*** > **ILM**.
  b. Überprüfen Sie die Attribute im Abschnitt „Bewertung“. Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut **Warten – Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
  a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
  b. Wählen Sie ***grid*** > ***Reparierter Speicherknoten*** > **LDR** > **Datenspeicher**.
  c. Verwenden Sie eine Kombination der folgenden Attribute, um so gut wie möglich zu bestimmen, ob replizierte Reparaturen abgeschlossen sind.

> ⓘ Möglicherweise liegen Cassandra-Inkonsistenzen vor und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

    - **Reparaturversuche (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt replizierter Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Speicherknoten versucht, ein Hochrisikoobjekt zu reparieren. Wenn dieses Attribut über einen Zeitraum, der länger ist als der aktuelle Scanzeitraum (bereitgestellt durch das Attribut **Scanzeitraum – Geschätzt**), nicht ansteigt, bedeutet dies, dass beim ILM-Scan auf keinem Knoten ein Hochrisikoobjekt gefunden wurde, das repariert werden muss.

> ⓘ Hochrisikoobjekte sind Objekte, bei denen die Gefahr eines vollständigen Verlusts besteht. Dies schließt keine Objekte ein, die ihrer ILM-Konfiguration nicht entsprechen.

    - **Scan-Zeitraum – Geschätzt (XSCM)**: Verwenden Sie dieses Attribut, um abzuschätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn das Attribut **Reparaturversuche** über einen Zeitraum, der länger als der aktuelle Scanzeitraum ist, nicht ansteigt, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt wurden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period – Estimated (XSCM)** gilt für das gesamte Raster und ist das Maximum aller Knoten-Scan-Perioden. Sie können den Attributverlauf **Scan-Zeitraum – Geschätzt** für das Raster abfragen, um einen geeigneten Zeitrahmen zu bestimmen.

Löschcodierte (EC) Daten

So überwachen Sie die Reparatur von Erasure-Code-Daten und wiederholen alle möglicherweise fehlgeschlagenen Anfragen:

1. Bestimmen Sie den Status der Datenreparaturen mit Erasure Code:
   - Wählen Sie **SUPPORT** > **Tools** > **Metriken**, um die geschätzte Zeit bis zur Fertigstellung und den Fertigstellungsgrad für den aktuellen Auftrag anzuzeigen. Wählen Sie dann im Abschnitt „Grafana“ die Option „EC-Übersicht“ aus. Sehen Sie sich die Dashboards **Geschätzte Zeit bis zur Fertigstellung des Grid EC-Jobs** und **Prozentsatz der Fertigstellung des Grid EC-Jobs**

an.

- Verwenden Sie diesen Befehl, um den Status eines bestimmten `repair-data` Betrieb:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

  ```
  repair-data show-ec-repair-status
  ```

Die Ausgabe listet Informationen auf, einschließlich `repair ID` , für alle bisherigen und laufenden Reparaturen.

2. Wenn die Ausgabe zeigt, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie die `--repair-id` Option zum erneuten Versuch der Reparatur.

   Mit diesem Befehl wird eine fehlgeschlagene Knotenreparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Mit diesem Befehl wird eine fehlgeschlagene Volumereparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung des Storage Node-Systemlaufwerks

Nachdem Sie das Systemlaufwerk für einen Storage Node wiederhergestellt haben, müssen Sie überprüfen, ob der gewünschte Status des Storage Node auf „Online“ eingestellt ist, und sicherstellen, dass der Status standardmäßig „Online“ ist, wenn der Storage Node-Server neu gestartet wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Überprüfen Sie die Werte von **Wiederhergestellter Speicherknoten** > **LDR** > **Speicher** > **Speicherstatus – Gewünscht** und **Speicherstatus – Aktuell**.

   Der Wert beider Attribute sollte „Online“ sein.

3. Wenn „Speicherstatus – Gewünscht“ auf „Schreibgeschützt“ eingestellt ist, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf die Registerkarte **Konfiguration**.
   b. Wählen Sie aus der Dropdown-Liste **Speicherstatus – Gewünscht** die Option **Online** aus.
   c. Klicken Sie auf **Änderungen übernehmen**.

d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherstatus – Gewünscht** und **Speicherstatus – Aktuell** auf „Online“ aktualisiert wurden.

Wiederherstellen von Objektdaten mit Grid Manager

Sie können Objektdaten für ein ausgefallenes Speichervolume oder einen ausgefallenen Speicherknoten mithilfe von Grid Manager wiederherstellen. Sie können Grid Manager auch verwenden, um laufende Wiederherstellungsprozesse zu überwachen und einen Wiederherstellungsverlauf anzuzeigen.

Bevor Sie beginnen

- Sie haben eines der folgenden Verfahren zum Formatieren fehlerhafter Volumes abgeschlossen:
  - "Appliance-Speichervolumes erneut mounten und neu formatieren (manuelle Schritte)"
  - "Speichervolumes erneut mounten und neu formatieren (manuelle Schritte)"
- Sie haben bestätigt, dass der Speicherknoten, auf dem Sie Objekte wiederherstellen, den Verbindungsstatus **Verbunden** hat. auf der Registerkarte **KNOTEN** > **Übersicht** im Grid Manager.
- Sie haben Folgendes bestätigt:
  - Eine Netzerweiterung zum Hinzufügen eines Speicherknotens ist nicht in Bearbeitung.
  - Die Außerbetriebnahme eines Speicherknotens ist nicht im Gange oder fehlgeschlagen.
  - Eine Wiederherstellung eines ausgefallenen Speichervolumes ist nicht in Bearbeitung.
  - Eine Wiederherstellung eines Speicherknotens mit einem ausgefallenen Systemlaufwerk ist nicht im Gange.
  - Ein EC-Neuausgleichsauftrag ist nicht in Bearbeitung.
  - Das Klonen des Appliance-Knotens ist nicht im Gange.

Informationen zu diesem Vorgang

Nachdem Sie die Laufwerke ausgetauscht und die manuellen Schritte zum Formatieren der Volumes ausgeführt haben, zeigt Grid Manager die Volumes auf der Registerkarte **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** als Kandidaten für die Wiederherstellung an.

Stellen Sie Objektdaten nach Möglichkeit mithilfe der Seite „Volume-Wiederherstellung“ im Grid Manager wieder her. Sie können entwederAktivieren Sie den automatischen Wiederherstellungsmodus um die Volume-Wiederherstellung automatisch zu starten, wenn die Volumes zur Wiederherstellung bereit sind oderFühren Sie die Volume-Wiederherstellung manuell durch . Befolgen Sie diese Richtlinien:

- Wenn die Volumes unter **WARTUNG** > **Volume-Wiederherstellung** > **Wiederherzustellende Knoten** aufgeführt sind, stellen Sie die Objektdaten wie in den folgenden Schritten beschrieben wieder her. Die Bände werden aufgelistet, wenn:
  - Einige, aber nicht alle Speichervolumes in einem Knoten sind ausgefallen
  - Alle Speichervolumes in einem Knoten sind ausgefallen und werden durch die gleiche Anzahl an Volumes oder mehr Volumes ersetzt

  Auf der Seite „Volume-Wiederherstellung“ im Grid Manager können Sie außerdemÜberwachen Sie den Volume-Wiederherstellungsprozess UndRestaurierungsverlauf anzeigen .
- Wenn die Volumes im Grid Manager nicht als Kandidaten für die Wiederherstellung aufgeführt sind, befolgen Sie die entsprechenden Schritte zur Verwendung des `repair-data` Skript zum Wiederherstellen

von Objektdaten:

- "Wiederherstellen von Objektdaten auf dem Speichervolume (Fehler des Systemlaufwerks)"
- "Stellen Sie die Objektdaten auf einem Speichervolume wieder her, auf dem das Systemlaufwerk intakt ist."
- "Stellen Sie Objektdaten auf dem Speichervolume für die Appliance wieder her"

> Das Skript „repair-data“ ist veraltet und wird in einer zukünftigen Version entfernt.

Wenn der wiederhergestellte Storage Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie die `repair-data` Skript.

Sie können zwei Arten von Objektdaten wiederherstellen:

- Replizierte Datenobjekte werden von anderen Standorten wiederhergestellt, vorausgesetzt, die ILM-Regeln des Grids wurden so konfiguriert, dass Objektkopien verfügbar sind.
  - Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und diese Kopie auf einem Speichervolume vorhanden war, das ausgefallen ist, können Sie das Objekt nicht wiederherstellen.
  - Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, muss StorageGRID mehrere Anfragen an den Endpunkt des Cloud-Speicherpools senden, um die Objektdaten wiederherzustellen.
- Erasure-Coded (EC)-Datenobjekte werden durch die Neuzusammensetzung der gespeicherten Fragmente wiederhergestellt. Beschädigte oder verlorene Fragmente werden durch den Erasure-Coding-Algorithmus aus den verbleibenden Daten- und Paritätsfragmenten wiederhergestellt.

  Die Reparatur von Daten mit Löschcode kann beginnen, während einige Speicherknoten offline sind. Wenn jedoch nicht alle mit dem Löschcode versehenen Daten ermittelt werden können, kann die Reparatur nicht abgeschlossen werden. Die Reparatur wird abgeschlossen, nachdem alle Knoten verfügbar sind.

> Die Volumewiederherstellung hängt von der Verfügbarkeit der Ressourcen ab, auf denen Objektkopien gespeichert sind. Der Fortschritt der Volumenwiederherstellung ist nicht linear und kann Tage oder Wochen dauern.

Aktivieren Sie den automatischen Wiederherstellungsmodus

Wenn Sie den automatischen Wiederherstellungsmodus aktivieren, beginnt die Volumewiederherstellung automatisch, wenn die Volumes zur Wiederherstellung bereit sind.

Schritte

1. Gehen Sie im Grid Manager zu **WARTUNG** > **Volume-Wiederherstellung**.
2. Wählen Sie die Registerkarte **Wiederherzustellende Knoten** und schieben Sie dann den Schalter für den **Automatischen Wiederherstellungsmodus** in die aktivierte Position.
3. Wenn das Bestätigungsdialogfeld angezeigt wird, überprüfen Sie die Details.

- Sie können Volume-Wiederherstellungsaufträge auf keinem Knoten manuell starten.
- Die Volumewiederherstellung beginnt nur dann automatisch, wenn keine anderen Wartungsvorgänge ausgeführt werden.
- Sie können den Status des Auftrags auf der Fortschrittsüberwachungsseite überwachen.
- StorageGRID versucht automatisch, Volume-Wiederherstellungen, die nicht gestartet werden können, erneut durchzuführen.

4. Wenn Sie die Auswirkungen der Aktivierung des automatischen Wiederherstellungsmodus verstehen, wählen Sie im Bestätigungsdialogfeld **Ja** aus.

   Sie können den automatischen Wiederherstellungsmodus jederzeit deaktivieren.

Fehlerhaftes Volume oder Knoten manuell wiederherstellen

Befolgen Sie diese Schritte, um ein ausgefallenes Volume oder einen ausgefallenen Knoten wiederherzustellen.

Schritte

1. Gehen Sie im Grid Manager zu **WARTUNG** > **Volume-Wiederherstellung**.
2. Wählen Sie die Registerkarte **Wiederherzustellende Knoten** und schieben Sie dann den Schalter für den **Automatischen Wiederherstellungsmodus** in die deaktivierte Position.

   Die Zahl auf der Registerkarte gibt die Anzahl der Knoten mit Volumes an, die wiederhergestellt werden müssen.

3. Erweitern Sie jeden Knoten, um die darin enthaltenen Volumes, die wiederhergestellt werden müssen, und deren Status anzuzeigen.
4. Beheben Sie alle Probleme, die die Wiederherstellung jedes Volumes verhindern. Probleme werden angezeigt, wenn Sie „Warten auf manuelle Schritte“ auswählen, sofern dies als Volumestatus angezeigt wird.
5. Wählen Sie einen Knoten zur Wiederherstellung aus, bei dem alle Volumes den Status „Bereit zur Wiederherstellung“ aufweisen.

   Sie können die Volumes jeweils nur für einen Knoten wiederherstellen.

   Jedes Volume im Knoten muss anzeigen, dass es zur Wiederherstellung bereit ist.

6. Wählen Sie **Wiederherstellung starten**.
7. Beheben Sie alle möglicherweise angezeigten Warnungen oder wählen Sie „Trotzdem starten“ aus, um die Warnungen zu ignorieren und die Wiederherstellung zu starten.

Knoten werden von der Registerkarte **Wiederherzustellende Knoten** auf die Registerkarte **Wiederherstellungsfortschritt** verschoben, wenn die Wiederherstellung beginnt.

Wenn eine Volumewiederherstellung nicht gestartet werden kann, kehrt der Knoten zur Registerkarte **Wiederherzustellende Knoten** zurück.

Wiederherstellungsfortschritt anzeigen

Die Registerkarte **Wiederherstellungsfortschritt** zeigt den Status des Volume-Wiederherstellungsprozesses

und Informationen zu den Volumes für einen wiederherzustellenden Knoten an.

Die Datenreparaturraten für replizierte und erasure-coded Objekte in allen Volumes sind Durchschnittswerte, die alle laufenden Wiederherstellungen zusammenfassen, einschließlich der Wiederherstellungen, die mit dem `repair-data` Skript. Außerdem wird der Prozentsatz der Objekte in diesen Bänden angegeben, die intakt sind und keiner Restaurierung bedürfen.

> Die Wiederherstellung replizierter Daten hängt von der Verfügbarkeit der Ressourcen ab, auf denen die replizierten Kopien gespeichert sind. Der Fortschritt der Wiederherstellung replizierter Daten ist nicht linear und kann Tage oder Wochen dauern.

Im Abschnitt „Wiederherstellungsaufträge“ werden Informationen zu Volumewiederherstellungen angezeigt, die vom Grid Manager gestartet wurden.

- Die Zahl in der Abschnittsüberschrift „Wiederherstellungsaufträge“ gibt die Anzahl der Datenträger an, die entweder wiederhergestellt werden oder zur Wiederherstellung in die Warteschlange gestellt werden.
- Die Tabelle zeigt Informationen zu jedem Volume in einem Knoten an, das wiederhergestellt wird, sowie den Fortschritt.
  - Der Fortschritt für jeden Knoten zeigt den Prozentsatz für jeden Job an.
  - Erweitern Sie die Spalte „Details“, um die Startzeit der Wiederherstellung und die Auftrags-ID anzuzeigen.
- Wenn eine Volumewiederherstellung fehlschlägt:
  - Die Spalte „Status“ zeigt `failed (attempting retry)` und wird automatisch wiederholt.
  - Wenn mehrere Wiederherstellungsaufträge fehlgeschlagen sind, wird automatisch zuerst der letzte Auftrag wiederholt.
  - Die Warnung **EC-Reparaturfehler** wird ausgelöst, wenn die Wiederholungsversuche weiterhin fehlschlagen. Befolgen Sie die Schritte in der Warnung, um das Problem zu beheben.

Wiederherstellungsverlauf anzeigen

Die Registerkarte **Wiederherstellungsverlauf** zeigt Informationen zu allen erfolgreich abgeschlossenen Volumewiederherstellungen.

> Größen gelten nicht für replizierte Objekte und werden nur für Wiederherstellungen angezeigt, die Erasure-Coded-Datenobjekte (EC) enthalten.

Überwachen von Reparaturdatenaufträgen

Sie können den Status von Reparaturaufträgen überwachen, indem Sie das `repair-data` Skript von der Befehlszeile aus.

Hierzu zählen Jobs, die Sie manuell initiiert haben, oder Jobs, die StorageGRID im Rahmen eines Außerbetriebnahmeverfahrens automatisch initiiert hat.

> Wenn Sie Volume-Wiederherstellungsjobs ausführen,"Überwachen Sie den Fortschritt und sehen Sie sich den Verlauf dieser Jobs im Grid Manager an" stattdessen.

Überwachen Sie den Status von `repair-data` Jobs basierend darauf, ob Sie **replizierte Daten**, **löschcodierte (EC) Daten** oder beides verwenden.

Replizierte Daten

- Um einen geschätzten Prozentsatz der Fertigstellung der replizierten Reparatur zu erhalten, addieren Sie die `show-replicated-repair-status` Option zum Befehl „repair-data“.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob die Reparaturen abgeschlossen sind:
  a. Wählen Sie **NODES** > ***Speicherknoten wird repariert*** > **ILM**.
  b. Überprüfen Sie die Attribute im Abschnitt „Bewertung“. Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut **Warten – Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
  a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
  b. Wählen Sie ***grid*** > ***Reparierter Speicherknoten*** > **LDR** > **Datenspeicher**.
  c. Verwenden Sie eine Kombination der folgenden Attribute, um so gut wie möglich zu bestimmen, ob replizierte Reparaturen abgeschlossen sind.

> ⓘ Möglicherweise liegen Cassandra-Inkonsistenzen vor und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

    - **Reparaturversuche (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt replizierter Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Speicherknoten versucht, ein Hochrisikoobjekt zu reparieren. Wenn dieses Attribut über einen Zeitraum, der länger ist als der aktuelle Scanzeitraum (bereitgestellt durch das Attribut **Scanzeitraum – Geschätzt**), nicht ansteigt, bedeutet dies, dass beim ILM-Scan auf keinem Knoten ein Hochrisikoobjekt gefunden wurde, das repariert werden muss.

> ⓘ Hochrisikoobjekte sind Objekte, bei denen die Gefahr eines vollständigen Verlusts besteht. Dies schließt keine Objekte ein, die ihrer ILM-Konfiguration nicht entsprechen.

    - **Scan-Zeitraum – Geschätzt (XSCM)**: Verwenden Sie dieses Attribut, um abzuschätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn das Attribut **Reparaturversuche** über einen Zeitraum, der länger als der aktuelle Scanzeitraum ist, nicht ansteigt, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt wurden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period – Estimated (XSCM)** gilt für das gesamte Raster und ist das Maximum aller Knoten-Scan-Perioden. Sie können den Attributverlauf **Scan-Zeitraum – Geschätzt** für das Raster abfragen, um einen geeigneten Zeitrahmen zu bestimmen.

Löschcodierte (EC) Daten

So überwachen Sie die Reparatur von Erasure-Code-Daten und wiederholen alle möglicherweise fehlgeschlagenen Anfragen:

1. Bestimmen Sie den Status der Datenreparaturen mit Erasure Code:
   - Wählen Sie **SUPPORT** > **Tools** > **Metriken**, um die geschätzte Zeit bis zur Fertigstellung und den Fertigstellungsgrad für den aktuellen Auftrag anzuzeigen. Wählen Sie dann im Abschnitt „Grafana“ die Option „EC-Übersicht“ aus. Sehen Sie sich die Dashboards **Geschätzte Zeit bis zur Fertigstellung des Grid EC-Jobs** und **Prozentsatz der Fertigstellung des Grid EC-Jobs**

an.

- Verwenden Sie diesen Befehl, um den Status eines bestimmten `repair-data` Betrieb:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

  ```
  repair-data show-ec-repair-status
  ```

Die Ausgabe listet Informationen auf, einschließlich `repair ID` , für alle bisherigen und laufenden Reparaturen.

2. Wenn die Ausgabe zeigt, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie die `--repair-id` Option zum erneuten Versuch der Reparatur.

   Mit diesem Befehl wird eine fehlgeschlagene Knotenreparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Mit diesem Befehl wird eine fehlgeschlagene Volumereparatur unter Verwendung der Reparatur-ID 6949309319275667690 erneut versucht:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Wiederherstellung nach Admin-Knoten-Fehlern

Wiederherstellung des primären oder nicht primären Admin-Knotens

Der Wiederherstellungsprozess für einen Admin-Knoten hängt davon ab, ob es sich um den primären Admin-Knoten oder einen nicht-primären Admin-Knoten handelt.

Die allgemeinen Schritte zum Wiederherstellen eines primären oder nicht primären Admin-Knotens sind dieselben, auch wenn sich die Details der Schritte unterscheiden.

Befolgen Sie immer das richtige Wiederherstellungsverfahren für den Admin-Knoten, den Sie wiederherstellen. Die Verfahren sehen auf hoher Ebene gleich aus, unterscheiden sich jedoch im Detail.

Auswahlmöglichkeiten

- "Wiederherstellung nach Fehlern des primären Admin-Knotens"
- "Wiederherstellung nach Fehlern nicht-primärer Admin-Knoten"

Wiederherstellung nach Fehlern des primären Admin-Knotens

Wiederherstellung nach Fehlern des primären Admin-Knotens

Sie müssen eine Reihe bestimmter Aufgaben ausführen, um einen Ausfall des primären Admin-Knotens zu beheben. Der primäre Admin-Knoten hostet den Configuration Management Node (CMN)-Dienst für das Grid.

Sie müssen einen ausgefallenen primären Admin-Knoten umgehend reparieren oder ersetzen, da das Grid sonst möglicherweise nicht mehr in der Lage ist, neue Objekte aufzunehmen. Der genaue Zeitraum hängt von Ihrer Objektaufnahmerate ab: Wenn Sie eine genauere Einschätzung des Zeitrahmens für Ihr Raster benötigen, wenden Sie sich an den technischen Support.

Der Configuration Management Node (CMN)-Dienst auf dem primären Admin-Knoten ist für die Ausgabe von Blöcken mit Objektkennungen für das Grid verantwortlich. Diese Kennungen werden den Objekten bei der Aufnahme zugewiesen. Neue Objekte können nur aufgenommen werden, wenn Kennungen verfügbar sind. Die Objektaufnahme kann fortgesetzt werden, während das CMN nicht verfügbar ist, da im Raster ein Vorrat an Kennungen für etwa einen Monat zwischengespeichert ist. Wenn die zwischengespeicherten Kennungen jedoch aufgebraucht sind, können keine neuen Objekte mehr hinzugefügt werden.

Befolgen Sie diese allgemeinen Schritte, um einen primären Admin-Knoten wiederherzustellen:

1. "Kopieren Sie die Prüfprotokolle vom ausgefallenen primären Admin-Knoten"
2. "Ersetzen Sie den primären Admin-Knoten"
3. "Konfigurieren Sie den Ersatz-Primäradministratorknoten"
4. "Ermitteln Sie, ob für den wiederhergestellten primären Admin-Knoten ein Hotfix erforderlich ist."
5. "Stellen Sie das Überwachungsprotokoll auf dem wiederhergestellten primären Admin-Knoten wieder her"
6. "Wiederherstellen der Admin-Knoten-Datenbank beim Wiederherstellen eines primären Admin-Knotens"
7. "Stellen Sie Prometheus-Metriken wieder her, wenn Sie einen primären Admin-Knoten wiederherstellen"

Kopieren Sie die Prüfprotokolle vom ausgefallenen primären Admin-Knoten

Wenn Sie Prüfprotokolle vom ausgefallenen primären Admin-Knoten kopieren können, sollten Sie diese aufbewahren, um die Aufzeichnungen der Systemaktivität und -nutzung des Grids aufrechtzuerhalten. Sie können die gespeicherten Prüfprotokolle auf dem wiederhergestellten primären Admin-Knoten wiederherstellen, nachdem dieser betriebsbereit ist.

Informationen zu diesem Vorgang

Bei diesem Verfahren werden die Audit-Protokolldateien vom ausgefallenen Admin-Knoten an einen temporären Speicherort auf einem separaten Grid-Knoten kopiert. Diese aufbewahrten Prüfprotokolle können dann auf den Ersatz-Admin-Knoten kopiert werden. Prüfprotokolle werden nicht automatisch auf den neuen Admin-Knoten kopiert.

Je nach Art des Fehlers können Sie möglicherweise keine Prüfprotokolle von einem ausgefallenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Knoten verfügt, beginnt der wiederhergestellte Admin-Knoten mit der Aufzeichnung von Ereignissen im Prüfprotokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Knoten umfasst, können Sie die Prüfprotokolle von einem anderen Admin-Knoten wiederherstellen.

Wenn auf die Überwachungsprotokolle auf dem ausgefallenen Admin-Knoten jetzt nicht zugegriffen werden kann, können Sie möglicherweise später darauf zugreifen, beispielsweise nach der Hostwiederherstellung.

Schritte

1. Melden Sie sich nach Möglichkeit beim ausgefallenen Admin-Knoten an. Andernfalls melden Sie sich beim

primären Admin-Knoten oder einem anderen Admin-Knoten an, falls verfügbar.

a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Stoppen Sie den AMS-Dienst, um zu verhindern, dass er eine neue Protokolldatei erstellt:`service ams stop`
3. Navigieren Sie zum Audit-Exportverzeichnis:

   ```
   cd /var/local/log
   ```

4. Benennen Sie die Quelle um `audit.log` Datei in einen eindeutigen nummerierten Dateinamen. Benennen Sie beispielsweise die Datei audit.log um in `2023-10-25.txt.1` .

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```

5. Starten Sie den AMS-Dienst neu: `service ams start`
6. Erstellen Sie das Verzeichnis, um alle Audit-Protokolldateien an einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Geben Sie bei der entsprechenden Aufforderung das Kennwort für den Administrator ein.

7. Kopieren Sie alle Audit-Protokolldateien an den temporären Speicherort: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Geben Sie bei der entsprechenden Aufforderung das Kennwort für den Administrator ein.

8. Als Root abmelden: `exit`

Primären Admin-Knoten ersetzen

Um einen primären Admin-Knoten wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen ausgefallenen primären Admin-Knoten durch einen primären Admin-Knoten ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen primären Admin-Knoten, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen primären Admin-Knoten ersetzen, der auf einer Service-Appliance gehostet wird.

Verwenden Sie das Verfahren, das der von Ihnen für den Knoten ausgewählten Ersatzplattform entspricht. Nachdem Sie das Verfahren zum Ersetzen des Knotens abgeschlossen haben (das für alle Knotentypen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die Wiederherstellung des primären Admin-Knotens weitergeleitet.

Ersatzplattform	Verfahren
VMware	"Ersetzen eines VMware-Knotens"
Linux	"Ersetzen eines Linux-Knotens"
Servicegeräte	"Ersetzen einer Service-Appliance"
OpenStack	Von NetApp bereitgestellte Festplattendateien und Skripts für virtuelle Maschinen für OpenStack werden für Wiederherstellungsvorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Bereitstellung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann die Anweisungen für"Ersetzen eines Linux-Knotens" .

Konfigurieren Sie den Ersatz-Primäradministratorknoten

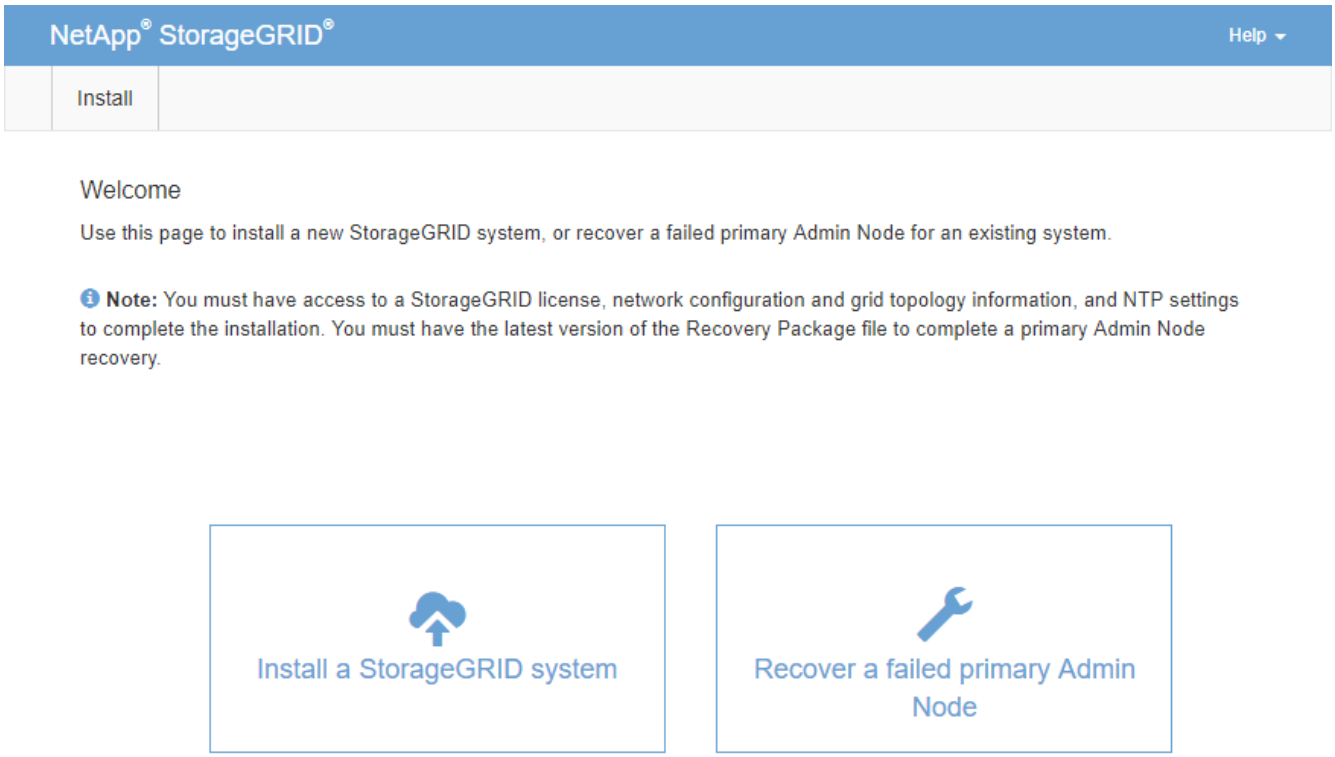
Der Ersatzknoten muss als primärer Admin-Knoten für Ihr StorageGRID System konfiguriert werden.

Bevor Sie beginnen

- Für primäre Admin-Knoten, die auf virtuellen Maschinen gehostet werden, wurde die virtuelle Maschine bereitgestellt, eingeschaltet und initialisiert.
- Für primäre Admin-Knoten, die auf einer Service-Appliance gehostet werden, haben Sie die Appliance ersetzt und Software installiert. Siehe die "Installationsanleitung für Ihr Gerät" .
- Sie verfügen über die neueste Sicherung der Wiederherstellungspaketdatei(`sgws-recovery-package-id-revision.zip`).
- Sie haben die Bereitstellungspassphrase.

Schritte

1. Öffnen Sie Ihren Webbrowser und navigieren Sie zu `https://primary_admin_node_ip` .
2. Verwalten Sie bei Bedarf ein temporäres Installateurkennwort:
   - Wenn mit einer dieser Methoden bereits ein Kennwort festgelegt wurde, geben Sie das Kennwort ein, um fortzufahren.
     - Ein Benutzer hat das Kennwort beim Zugriff auf das Installationsprogramm zuvor festgelegt
     - Für Bare-Metal-Systeme wurde das Passwort automatisch aus der Knotenkonfigurationsdatei importiert unter `/etc/storagegrid/nodes/<node_name>.conf`
     - Für VMs wurde das SSH-/Konsolenkennwort automatisch aus den OVF-Eigenschaften importiert
   - Wenn kein Kennwort festgelegt wurde, legen Sie optional ein Kennwort fest, um das StorageGRID Installationsprogramm zu sichern.
3. Klicken Sie auf **Einen ausgefallenen primären Admin-Knoten wiederherstellen**.



4. Laden Sie die aktuellste Sicherung des Wiederherstellungspakets hoch:
   a. Klicken Sie auf **Durchsuchen**.
   b. Suchen Sie die aktuellste Wiederherstellungspaketdatei für Ihr StorageGRID -System und klicken Sie auf **Öffnen**.
5. Geben Sie die Bereitstellungspassphrase ein.
6. Klicken Sie auf **Wiederherstellung starten**.

   Der Wiederherstellungsprozess beginnt. Der Grid Manager ist möglicherweise für einige Minuten nicht verfügbar, während die erforderlichen Dienste gestartet werden. Wenn die Wiederherstellung abgeschlossen ist, wird die Anmeldeseite angezeigt.

7. Wenn Single Sign-On (SSO) für Ihr StorageGRID -System aktiviert ist und die Vertrauensstellung der vertrauenden Seite für den wiederhergestellten Admin-Knoten für die Verwendung des Standardzertifikats der Verwaltungsschnittstelle konfiguriert wurde, aktualisieren (oder löschen und erstellen) Sie die Vertrauensstellung der vertrauenden Seite des Knotens in Active Directory Federation Services (AD FS). Verwenden Sie das neue Standardserverzertifikat, das während des Wiederherstellungsprozesses des Admin-Knotens generiert wurde.

   Informationen zum Konfigurieren einer Vertrauensstellung der vertrauenden Seite finden Sie unter"Konfigurieren der einmaligen Anmeldung" . Um auf das Standardserverzertifikat zuzugreifen, melden Sie sich bei der Befehlsshell des Admin-Knotens an. Gehen Sie zum `/var/local/mgmt-api` Verzeichnis und wählen Sie das `server.crt` Datei.

Nach der Wiederherstellung eines primären Admin-Knotens,"Bestimmen Sie, ob Sie einen Hotfix anwenden müssen" .

Hotfix-Anforderung für primären Admin-Knoten ermitteln

Stellen Sie nach der Wiederherstellung eines primären Administratorknotens fest, ob Sie einen Hotfix anwenden müssen.

Bevor Sie beginnen

Die Wiederherstellung des primären Admin-Knotens ist abgeschlossen.

Schritte

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Wählen Sie **NODES**.
3. Wählen Sie aus der Liste links den primären Admin-Knoten aus.
4. Beachten Sie auf der Registerkarte „Übersicht“ die im Feld „Softwareversion“ angezeigte Version.
5. Wählen Sie einen beliebigen anderen Rasterknoten aus.
6. Beachten Sie auf der Registerkarte „Übersicht“ die im Feld „Softwareversion“ angezeigte Version.
   - Wenn die in den Feldern **Softwareversion** angezeigten Versionen identisch sind, müssen Sie keinen Hotfix anwenden.
   - Wenn die in den Feldern **Software Version** angezeigten Versionen unterschiedlich sind, müssen Sie"einen Hotfix anwenden" um den wiederhergestellten primären Admin-Knoten auf dieselbe Version zu aktualisieren.

Wiederherstellen des Überwachungsprotokolls auf dem wiederhergestellten primären Admin-Knoten

Wenn Sie das Prüfprotokoll des ausgefallenen primären Admin-Knotens aufbewahren konnten, können Sie es auf den primären Admin-Knoten kopieren, den Sie wiederherstellen.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten ist installiert und läuft.
- Sie haben die Prüfprotokolle an einen anderen Speicherort kopiert, nachdem der ursprüngliche Admin-Knoten ausgefallen war.

Informationen zu diesem Vorgang

Wenn ein Admin-Knoten ausfällt, gehen die auf diesem Admin-Knoten gespeicherten Prüfprotokolle möglicherweise verloren. Möglicherweise können Daten vor Verlust bewahrt werden, indem Prüfprotokolle vom ausgefallenen Admin-Knoten kopiert und diese Prüfprotokolle dann auf dem wiederhergestellten Admin-Knoten wiederhergestellt werden. Je nach Fehler ist es möglicherweise nicht möglich, Prüfprotokolle vom ausgefallenen Admin-Knoten zu kopieren. In diesem Fall können Sie, wenn die Bereitstellung über mehr als einen Admin-Knoten verfügt, Prüfprotokolle von einem anderen Admin-Knoten wiederherstellen, da Prüfprotokolle auf alle Admin-Knoten repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Prüfprotokoll nicht vom ausgefallenen Knoten kopiert werden kann, beginnt der wiederhergestellte Admin-Knoten mit der Aufzeichnung von Ereignissen im Prüfprotokoll, als ob die Installation neu wäre.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktionalität wiederherzustellen.

Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf den Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn einer der folgenden Punkte zutrifft:

- Sie haben einen externen Syslog-Server konfiguriert und Prüfprotokolle werden jetzt an den Syslog-Server statt an Admin-Knoten gesendet.
- Sie haben ausdrücklich angegeben, dass Prüfmeldungen nur auf den lokalen Knoten gespeichert werden sollen, die sie generiert haben.

Sehen"Konfigurieren von Überwachungsmeldungen und Protokollzielen" für Details.

Schritte

1. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@recovery_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.

   Nachdem Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

2. Überprüfen Sie, welche Audit-Dateien erhalten geblieben sind: `cd /var/local/log`
3. Kopieren Sie die gespeicherten Audit-Protokolldateien auf den wiederhergestellten Admin-Knoten: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Geben Sie bei der entsprechenden Aufforderung das Kennwort für den Administrator ein.

4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom ausgefallenen Grid-Knoten, nachdem Sie überprüft haben, dass sie erfolgreich auf den wiederhergestellten Admin-Knoten kopiert wurden.
5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Protokolldateien auf dem wiederhergestellten Admin-Knoten: `chown ams-user: bycast *`
6. Als Root abmelden: `exit`

Wiederherstellen der Admin-Knoten-Datenbank beim Wiederherstellen des primären Admin-Knotens

Wenn Sie die historischen Informationen zu Attributen und Warnungen auf einem ausgefallenen primären Admin-Knoten behalten möchten, können Sie die Admin-Knoten-Datenbank wiederherstellen. Sie können diese Datenbank nur wiederherstellen, wenn Ihr StorageGRID -System einen weiteren Admin-Knoten enthält.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten ist installiert und läuft.
- Das StorageGRID -System umfasst mindestens zwei Admin-Knoten.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen

Informationen verloren. Diese Datenbank enthält die folgenden Informationen:

- Alarmverlauf
- Historische Attributdaten, die in Diagrammen im Legacy-Stil auf der Knotenseite verwendet werden

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Softwareinstallationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen zu Servern und Diensten, die derzeit Teil des Systems sind oder später hinzugefügt werden.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID System über einen weiteren Admin-Knoten verfügt, können Sie die historischen Informationen wiederherstellen, indem Sie die Admin-Knoten-Datenbank von einem nicht primären Admin-Knoten (dem *Quell-Admin-Knoten*) auf den wiederhergestellten primären Admin-Knoten kopieren. Wenn Ihr System nur über einen primären Admin-Knoten verfügt, können Sie die Admin-Knoten-Datenbank nicht wiederherstellen.

> Das Kopieren der Admin-Knoten-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während die Dienste auf dem Quell-Admin-Knoten gestoppt sind.

Schritte

1. Melden Sie sich beim Quelladministratorknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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.
2. Stoppen Sie den MI-Dienst vom Quell-Admin-Knoten aus: `service mi stop`
3. Stoppen Sie vom Quelladministratorknoten aus den Dienst „Management Application Program Interface“ (mgmt-api): `service mgmt-api stop`
4. Führen Sie auf dem wiederhergestellten Admin-Knoten die folgenden Schritte aus:
   a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   b. Beenden Sie den MI-Dienst: `service mi stop`
   c. Stoppen Sie den mgmt-api-Dienst: `service mgmt-api stop`
   d. Fügen Sie dem SSH-Agenten den privaten SSH-Schlüssel hinzu. Eingeben:`ssh-add`
   e. Geben Sie das SSH-Zugriffskennwort ein, das im `Passwords.txt` Datei.
   f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Bestätigen Sie bei der entsprechenden Aufforderung, dass Sie die MI-Datenbank auf dem wiederhergestellten Admin-Knoten überschreiben möchten.

Die Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten.

h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel aus dem SSH-Agenten. Eingeben:`ssh-add -D`

5. Starten Sie die Dienste auf dem Quelladministratorknoten neu: `service servermanager start`

Stellen Sie Prometheus-Metriken wieder her, wenn Sie den primären Admin-Knoten wiederherstellen

Optional können Sie die von Prometheus verwalteten historischen Metriken auf einem ausgefallenen primären Admin-Knoten beibehalten. Die Prometheus-Metriken können nur wiederhergestellt werden, wenn Ihr StorageGRID -System einen weiteren Admin-Knoten enthält.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten ist installiert und läuft.
- Das StorageGRID -System umfasst mindestens zwei Admin-Knoten.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten verwalteten Metriken verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Softwareinstallationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Knoten gestartet wurde, zeichnet er Metriken auf, als hätten Sie eine Neuinstallation des StorageGRID -Systems durchgeführt.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID System über einen weiteren Admin-Knoten verfügt, können Sie die historischen Metriken wiederherstellen, indem Sie die Prometheus-Datenbank von einem nicht primären Admin-Knoten (dem *Quell-Admin-Knoten*) auf den wiederhergestellten primären Admin-Knoten kopieren. Wenn Ihr System nur über einen primären Admin-Knoten verfügt, können Sie die Prometheus-Datenbank nicht wiederherstellen.

> ⓘ Das Kopieren der Prometheus-Datenbank kann eine Stunde oder länger dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während die Dienste auf dem Quell-Admin-Knoten gestoppt sind.

Schritte

1. Melden Sie sich beim Quelladministratorknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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.
2. Stoppen Sie den Prometheus-Dienst vom Quell-Admin-Knoten aus: `service prometheus stop`
3. Führen Sie auf dem wiederhergestellten Admin-Knoten die folgenden Schritte aus:
   a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

b. Stoppen Sie den Prometheus-Dienst: `service prometheus stop`

c. Fügen Sie dem SSH-Agenten den privaten SSH-Schlüssel hinzu. Eingeben:`ssh-add`

d. Geben Sie das SSH-Zugriffskennwort ein, das im `Passwords.txt` Datei.

e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Drücken Sie bei der entsprechenden Aufforderung die Eingabetaste, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem wiederhergestellten Admin-Knoten zerstören möchten.

Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten. Es erscheint folgender Status:

Datenbank geklont, Dienste werden gestartet

a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel aus dem SSH-Agenten. Eingeben:`ssh-add -D`

4. Starten Sie den Prometheus-Dienst auf dem Quell-Admin-Knoten neu.`service prometheus start`

Wiederherstellung nach Fehlern nicht-primärer Admin-Knoten

Wiederherstellung nach Fehlern nicht-primärer Admin-Knoten

Sie müssen die folgenden Aufgaben ausführen, um den Ausfall eines nicht primären Admin-Knotens zu beheben. Ein Admin-Knoten hostet den Configuration Management Node (CMN)-Dienst und wird als primärer Admin-Knoten bezeichnet. Obwohl Sie mehrere Admin-Knoten haben können, enthält jedes StorageGRID System nur einen primären Admin-Knoten. Alle anderen Admin-Knoten sind nicht primäre Admin-Knoten.

Befolgen Sie diese allgemeinen Schritte, um einen nicht primären Admin-Knoten wiederherzustellen:

1. "Kopieren Sie die Prüfprotokolle vom ausgefallenen nicht-primären Admin-Knoten"
2. "Ersetzen Sie den nicht primären Admin-Knoten"
3. "Wählen Sie „Wiederherstellung starten“, um den nicht-primären Admin-Knoten zu konfigurieren."
4. "Wiederherstellen des Überwachungsprotokolls auf einem wiederhergestellten nicht primären Admin-Knoten"
5. "Wiederherstellen der Admin-Knoten-Datenbank beim Wiederherstellen eines nicht primären Admin-Knotens"
6. "Stellen Sie Prometheus-Metriken wieder her, wenn Sie einen nicht primären Admin-Knoten wiederherstellen"

Kopieren Sie Audit-Protokolle von einem ausgefallenen nicht-primären Admin-Knoten

Wenn Sie Prüfprotokolle vom ausgefallenen Admin-Knoten kopieren können, sollten Sie diese aufbewahren, um die Aufzeichnungen der Systemaktivität und -nutzung des Grids aufrechtzuerhalten. Sie können die gespeicherten Prüfprotokolle auf dem wiederhergestellten nicht primären Admin-Knoten wiederherstellen, nachdem dieser betriebsbereit ist.

Bei diesem Verfahren werden die Audit-Protokolldateien vom ausgefallenen Admin-Knoten an einen temporären Speicherort auf einem separaten Grid-Knoten kopiert. Diese aufbewahrten Prüfprotokolle können dann auf den Ersatz-Admin-Knoten kopiert werden. Prüfprotokolle werden nicht automatisch auf den neuen Admin-Knoten kopiert.

Je nach Art des Fehlers können Sie möglicherweise keine Prüfprotokolle von einem ausgefallenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Knoten verfügt, beginnt der wiederhergestellte Admin-Knoten mit der Aufzeichnung von Ereignissen im Prüfprotokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Knoten umfasst, können Sie die Prüfprotokolle von einem anderen Admin-Knoten wiederherstellen.

> Wenn auf die Überwachungsprotokolle auf dem ausgefallenen Admin-Knoten jetzt nicht zugegriffen werden kann, können Sie möglicherweise später darauf zugreifen, beispielsweise nach der Hostwiederherstellung.

1. Melden Sie sich nach Möglichkeit beim ausgefallenen Admin-Knoten an. Andernfalls melden Sie sich beim primären Admin-Knoten oder einem anderen Admin-Knoten an, falls verfügbar.
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Stoppen Sie den AMS-Dienst, um zu verhindern, dass er eine neue Protokolldatei erstellt:`service ams stop`
3. Navigieren Sie zum Audit-Exportverzeichnis:

   ```
   cd /var/local/log
   ```
4. Benennen Sie die Quelldatei audit.log in einen eindeutigen nummerierten Dateinamen um. Benennen Sie beispielsweise die Datei audit.log um in `2023-10-25.txt.1` .

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```
5. Starten Sie den AMS-Dienst neu: `service ams start`
6. Erstellen Sie das Verzeichnis, um alle Audit-Protokolldateien an einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren: `ssh admin@grid_node_IP mkdir -p`

`/var/local/tmp/saved-audit-logs`

Geben Sie bei der entsprechenden Aufforderung das Kennwort für den Administrator ein.

7. Kopieren Sie alle Audit-Protokolldateien an den temporären Speicherort: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Geben Sie bei der entsprechenden Aufforderung das Kennwort für den Administrator ein.

8. Als Root abmelden: `exit`

Nicht-primären Admin-Knoten ersetzen

Um einen nicht primären Admin-Knoten wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen ausgefallenen nicht primären Admin-Knoten durch einen nicht primären Admin-Knoten ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen nicht primären Admin-Knoten, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen nicht primären Admin-Knoten ersetzen, der auf einer Service-Appliance gehostet wird.

Verwenden Sie das Verfahren, das der von Ihnen für den Knoten ausgewählten Ersatzplattform entspricht. Nachdem Sie das Verfahren zum Ersetzen des Knotens abgeschlossen haben (das für alle Knotentypen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die Wiederherstellung nicht primärer Admin-Knoten weitergeleitet.

Ersatzplattform	Verfahren
VMware	"Ersetzen eines VMware-Knotens"
Linux	"Ersetzen eines Linux-Knotens"
Servicegeräte	"Ersetzen einer Service-Appliance"
OpenStack	Von NetApp bereitgestellte Festplattendateien und Skripts für virtuelle Maschinen für OpenStack werden für Wiederherstellungsvorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Bereitstellung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann die Anweisungen für"Ersetzen eines Linux-Knotens" .

Wählen Sie „Wiederherstellung starten“, um den nicht primären Admin-Knoten zu konfigurieren

Nachdem Sie einen nicht primären Admin-Knoten ersetzt haben, müssen Sie im Grid Manager „Wiederherstellung starten“ auswählen, um den neuen Knoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Bevor Sie beginnen

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

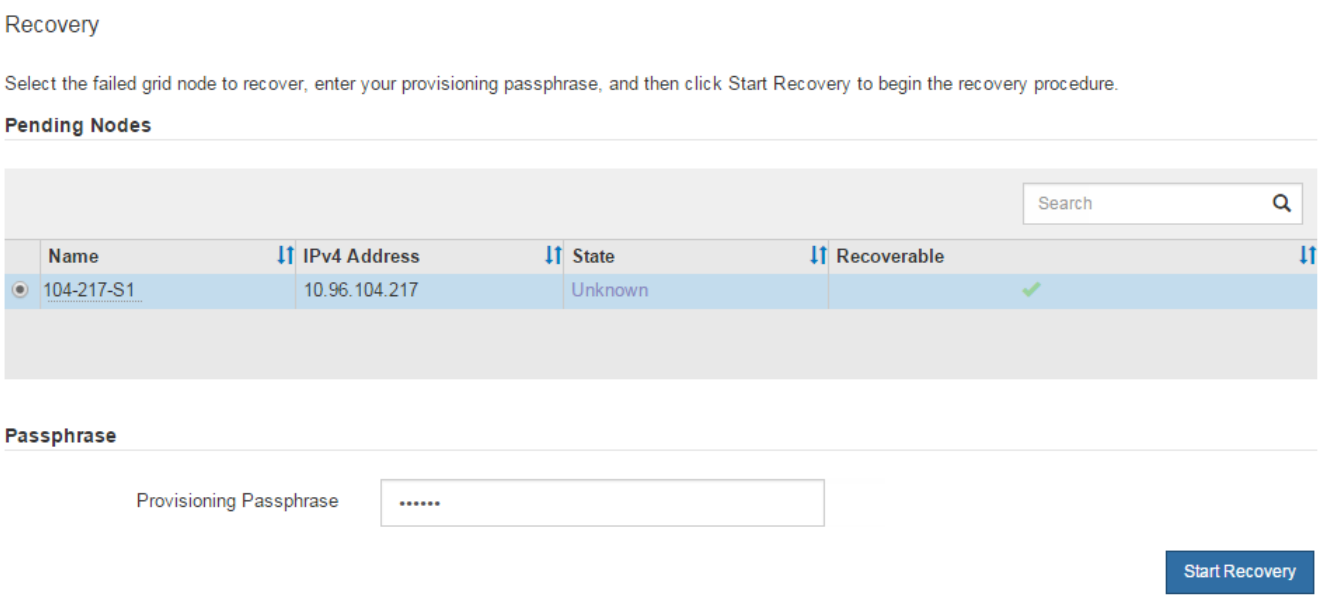
- Sie haben die Bereitstellungspassphrase.
- Sie haben den Ersatzknoten bereitgestellt und konfiguriert.

Schritte

1. Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Wiederherstellung**.
2. Wählen Sie in der Liste „Ausstehende Knoten“ den Grid-Knoten aus, den Sie wiederherstellen möchten.

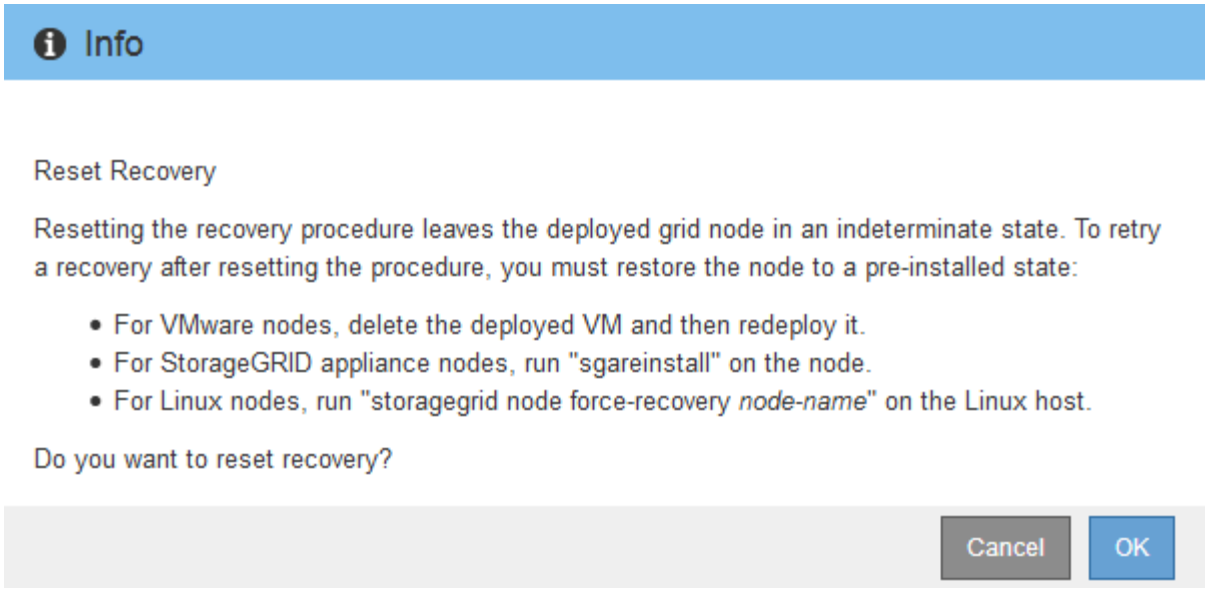
   Knoten werden in der Liste angezeigt, nachdem sie ausgefallen sind. Sie können einen Knoten jedoch erst auswählen, wenn er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Bereitstellungspassphrase** ein.
4. Klicken Sie auf **Wiederherstellung starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Grid-Knoten wird wiederhergestellt“.

> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das darauf hinweist, dass der Knoten in einem unbestimmten Zustand verbleibt, wenn Sie die Prozedur zurücksetzen.



Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Verfahrens wiederholen möchten, müssen Sie den Knoten wie folgt in einen vorinstallierten Zustand zurückversetzen:

- **VMware**: Löschen Sie den bereitgestellten virtuellen Grid-Knoten. Wenn Sie dann bereit sind, die Wiederherstellung neu zu starten, stellen Sie den Knoten erneut bereit.
- **Linux**: Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen: `storagegrid node force-recovery node-name`
- **Appliance**: Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Verfahrens wiederholen möchten, müssen Sie den Appliance-Knoten in einen vorinstallierten Zustand zurücksetzen, indem Sie `sgareinstall` auf dem Knoten. Sehen "Gerät für Neuinstallation vorbereiten (nur Plattformaustausch)" .

6. Wenn Single Sign-On (SSO) für Ihr StorageGRID -System aktiviert ist und die Vertrauensstellung der vertrauenden Seite für den wiederhergestellten Admin-Knoten für die Verwendung des Standardzertifikats der Verwaltungsschnittstelle konfiguriert wurde, aktualisieren (oder löschen und erstellen) Sie die Vertrauensstellung der vertrauenden Seite des Knotens in Active Directory Federation Services (AD FS). Verwenden Sie das neue Standardserverzertifikat, das während des Wiederherstellungsprozesses des Admin-Knotens generiert wurde.

> Informationen zum Konfigurieren einer Vertrauensstellung der vertrauenden Seite finden Sie unter"Konfigurieren der einmaligen Anmeldung" . Um auf das Standardserverzertifikat zuzugreifen, melden Sie sich bei der Befehlsshell des Admin-Knotens an. Gehen Sie zum `/var/local/mgmt-api` Verzeichnis und wählen Sie das `server.crt` Datei.

Wiederherstellen des Überwachungsprotokolls auf dem wiederhergestellten nicht primären Admin-Knoten

Wenn Sie das Prüfprotokoll des ausgefallenen nicht primären Admin-Knotens aufbewahren konnten, sodass die historischen Prüfprotokollinformationen erhalten bleiben, können Sie es auf den nicht primären Admin-Knoten kopieren, den Sie wiederherstellen.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten ist installiert und läuft.

- Sie haben die Prüfprotokolle an einen anderen Speicherort kopiert, nachdem der ursprüngliche Admin-Knoten ausgefallen war.

Informationen zu diesem Vorgang

Wenn ein Admin-Knoten ausfällt, gehen die auf diesem Admin-Knoten gespeicherten Prüfprotokolle möglicherweise verloren. Möglicherweise können Daten vor Verlust bewahrt werden, indem Prüfprotokolle vom ausgefallenen Admin-Knoten kopiert und diese Prüfprotokolle dann auf dem wiederhergestellten Admin-Knoten wiederhergestellt werden. Je nach Fehler ist es möglicherweise nicht möglich, Prüfprotokolle vom ausgefallenen Admin-Knoten zu kopieren. In diesem Fall können Sie, wenn die Bereitstellung über mehr als einen Admin-Knoten verfügt, Prüfprotokolle von einem anderen Admin-Knoten wiederherstellen, da Prüfprotokolle auf alle Admin-Knoten repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Prüfprotokoll nicht vom ausgefallenen Knoten kopiert werden kann, beginnt der wiederhergestellte Admin-Knoten mit der Aufzeichnung von Ereignissen im Prüfprotokoll, als ob die Installation neu wäre.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktionalität wiederherzustellen.

> Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf den Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn einer der folgenden Punkte zutrifft:
>
> - Sie haben einen externen Syslog-Server konfiguriert und Prüfprotokolle werden jetzt an den Syslog-Server statt an Admin-Knoten gesendet.
> - Sie haben ausdrücklich angegeben, dass Prüfmeldungen nur auf den lokalen Knoten gespeichert werden sollen, die sie generiert haben.
>
> Sehen"Konfigurieren von Überwachungsmeldungen und Protokollzielen" für Details.

Schritte

1. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

   a. Geben Sie den folgenden Befehl ein:
   `ssh admin@recovery_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.

   Nachdem Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

2. Überprüfen Sie, welche Audit-Dateien erhalten geblieben sind:

   ```
   cd /var/local/log
   ```

3. Kopieren Sie die gespeicherten Audit-Protokolldateien auf den wiederhergestellten Admin-Knoten:

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   Geben Sie bei der entsprechenden Aufforderung das Kennwort für den Administrator ein.

4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom ausgefallenen Grid-Knoten, nachdem Sie überprüft haben, dass sie erfolgreich auf den wiederhergestellten Admin-Knoten kopiert wurden.

5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Protokolldateien auf dem wiederhergestellten Admin-Knoten:

   ```
   chown ams-user:bycast *
   ```

6. Als Root abmelden: `exit`

Wiederherstellen der Admin-Knoten-Datenbank beim Wiederherstellen eines nicht primären Admin-Knotens

Wenn Sie die historischen Informationen zu Attributen und Warnungen auf einem nicht primären Admin-Knoten, der ausgefallen ist, behalten möchten, können Sie die Admin-Knoten-Datenbank vom primären Admin-Knoten wiederherstellen.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten ist installiert und läuft.
- Das StorageGRID -System umfasst mindestens zwei Admin-Knoten.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen Informationen verloren. Diese Datenbank enthält die folgenden Informationen:

- Alarmverlauf
- Historische Attributdaten, die in Diagrammen im Legacy-Stil auf der Seite „Knoten“ verwendet werden

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Softwareinstallationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen zu Servern und Diensten, die derzeit Teil des Systems sind oder später hinzugefügt werden.

Wenn Sie einen nicht primären Admin-Knoten wiederhergestellt haben, können Sie die historischen Informationen wiederherstellen, indem Sie die Admin-Knoten-Datenbank vom primären Admin-Knoten (dem *Quell-Admin-Knoten*) auf den wiederhergestellten Knoten kopieren.

> ⓘ Das Kopieren der Admin-Knoten-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während die Dienste auf dem Quellknoten angehalten sind.

Schritte

1. Melden Sie sich beim Quelladministratorknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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.
2. Führen Sie den folgenden Befehl vom Quelladministratorknoten aus. Geben Sie dann die Bereitstellungspassphrase ein, wenn Sie dazu aufgefordert werden. `recover-access-points`

3. Stoppen Sie den MI-Dienst vom Quell-Admin-Knoten aus: `service mi stop`
4. Stoppen Sie vom Quelladministratorknoten aus den Dienst „Management Application Program Interface“ (mgmt-api): `service mgmt-api stop`
5. Führen Sie auf dem wiederhergestellten Admin-Knoten die folgenden Schritte aus:
   a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   b. Beenden Sie den MI-Dienst: `service mi stop`
   c. Stoppen Sie den mgmt-api-Dienst: `service mgmt-api stop`
   d. Fügen Sie dem SSH-Agenten den privaten SSH-Schlüssel hinzu. Eingeben:`ssh-add`
   e. Geben Sie das SSH-Zugriffskennwort ein, das im `Passwords.txt` Datei.
   f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Bestätigen Sie bei der entsprechenden Aufforderung, dass Sie die MI-Datenbank auf dem wiederhergestellten Admin-Knoten überschreiben möchten.

      Die Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten.

   h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel aus dem SSH-Agenten. Eingeben:`ssh-add -D`
6. Starten Sie die Dienste auf dem Quelladministratorknoten neu: `service servermanager start`

Stellen Sie Prometheus-Metriken wieder her, wenn Sie einen nicht primären Admin-Knoten wiederherstellen

Optional können Sie die von Prometheus verwalteten historischen Metriken auf einem nicht primären Admin-Knoten beibehalten, der ausgefallen ist.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten ist installiert und läuft.
- Das StorageGRID -System umfasst mindestens zwei Admin-Knoten.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten verwalteten Metriken verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Softwareinstallationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Knoten gestartet wurde, zeichnet er Metriken auf, als hätten Sie eine Neuinstallation des StorageGRID -Systems durchgeführt.

Wenn Sie einen nicht primären Admin-Knoten wiederhergestellt haben, können Sie die historischen Metriken

wiederherstellen, indem Sie die Prometheus-Datenbank vom primären Admin-Knoten (dem *Quell-Admin-Knoten*) auf den wiederhergestellten Admin-Knoten kopieren.

> Das Kopieren der Prometheus-Datenbank kann eine Stunde oder länger dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während die Dienste auf dem Quell-Admin-Knoten gestoppt sind.

Schritte

1. Melden Sie sich beim Quelladministratorknoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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.
2. Stoppen Sie den Prometheus-Dienst vom Quell-Admin-Knoten aus: `service prometheus stop`
3. Führen Sie auf dem wiederhergestellten Admin-Knoten die folgenden Schritte aus:
   a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   b. Stoppen Sie den Prometheus-Dienst: `service prometheus stop`
   c. Fügen Sie dem SSH-Agenten den privaten SSH-Schlüssel hinzu. Eingeben:`ssh-add`
   d. Geben Sie das SSH-Zugriffskennwort ein, das im `Passwords.txt` Datei.
   e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Drücken Sie bei der entsprechenden Aufforderung die Eingabetaste, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem wiederhergestellten Admin-Knoten zerstören möchten.

      Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten. Es erscheint folgender Status:

   Datenbank geklont, Dienste werden gestartet

   a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel aus dem SSH-Agenten. Eingeben:`ssh-add -D`
4. Starten Sie den Prometheus-Dienst auf dem Quell-Admin-Knoten neu.`service prometheus start`

Wiederherstellung nach Gateway-Knotenfehlern

Gateway-Knoten ersetzen

Sie können einen ausgefallenen Gateway-Knoten durch einen Gateway-Knoten ersetzen, der auf derselben physischen oder virtuellen Hardware ausgeführt wird, oder Sie können einen Gateway-Knoten, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen Gateway-Knoten ersetzen, der auf einer Service-Appliance gehostet wird.

Das Verfahren zum Ersetzen des Knotens, das Sie befolgen müssen, hängt davon ab, welche Plattform vom Ersatzknoten verwendet wird. Nachdem Sie das Verfahren zum Ersetzen des Knotens abgeschlossen haben (das für alle Knotentypen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die Wiederherstellung des Gateway-Knotens weitergeleitet.

Ersatzplattform	Verfahren
VMware	"Ersetzen eines VMware-Knotens"
Linux	"Ersetzen eines Linux-Knotens"
Servicegeräte	"Ersetzen einer Service-Appliance"
OpenStack	Von NetApp bereitgestellte Festplattendateien und Skripts für virtuelle Maschinen für OpenStack werden für Wiederherstellungsvorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Bereitstellung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann die Anweisungen für"Ersetzen eines Linux-Knotens" .

Wählen Sie „Wiederherstellung starten“, um den Gateway-Knoten zu konfigurieren.

Nachdem Sie einen Gateway-Knoten ersetzt haben, müssen Sie im Grid Manager „Wiederherstellung starten“ auswählen, um den neuen Knoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Bevor Sie beginnen

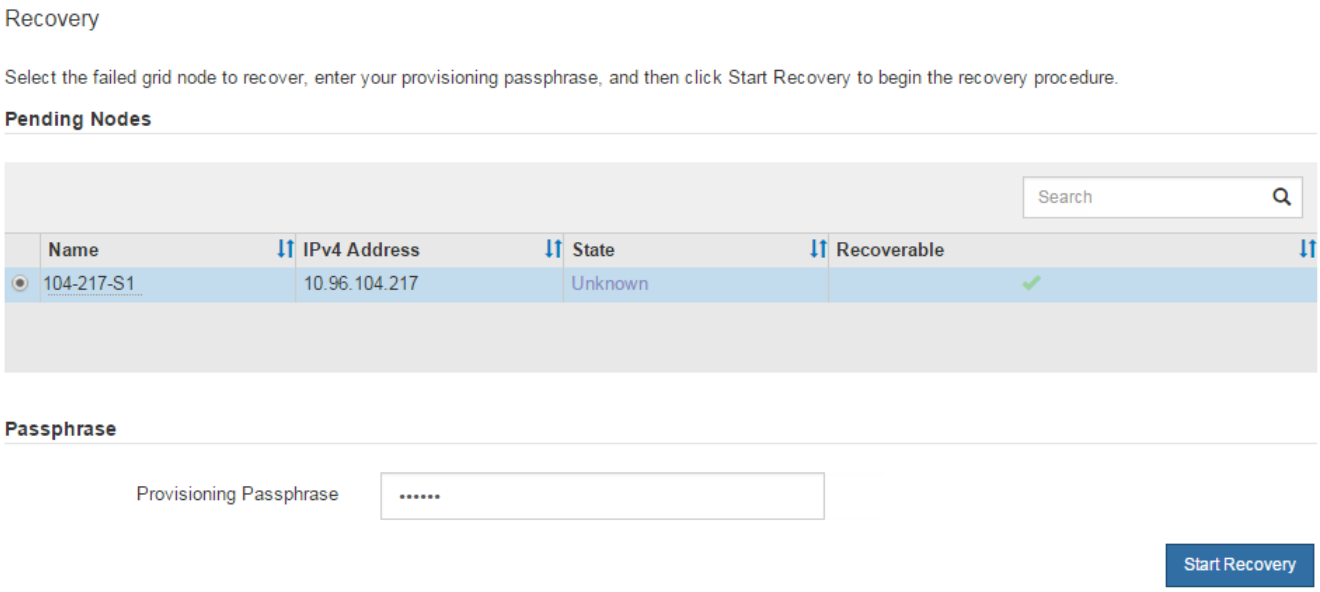
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie haben die Bereitstellungspassphrase.
- Sie haben den Ersatzknoten bereitgestellt und konfiguriert.

Schritte

1. Wählen Sie im Grid Manager **WARTUNG** > **Aufgaben** > **Wiederherstellung**.
2. Wählen Sie in der Liste „Ausstehende Knoten“ den Grid-Knoten aus, den Sie wiederherstellen möchten.

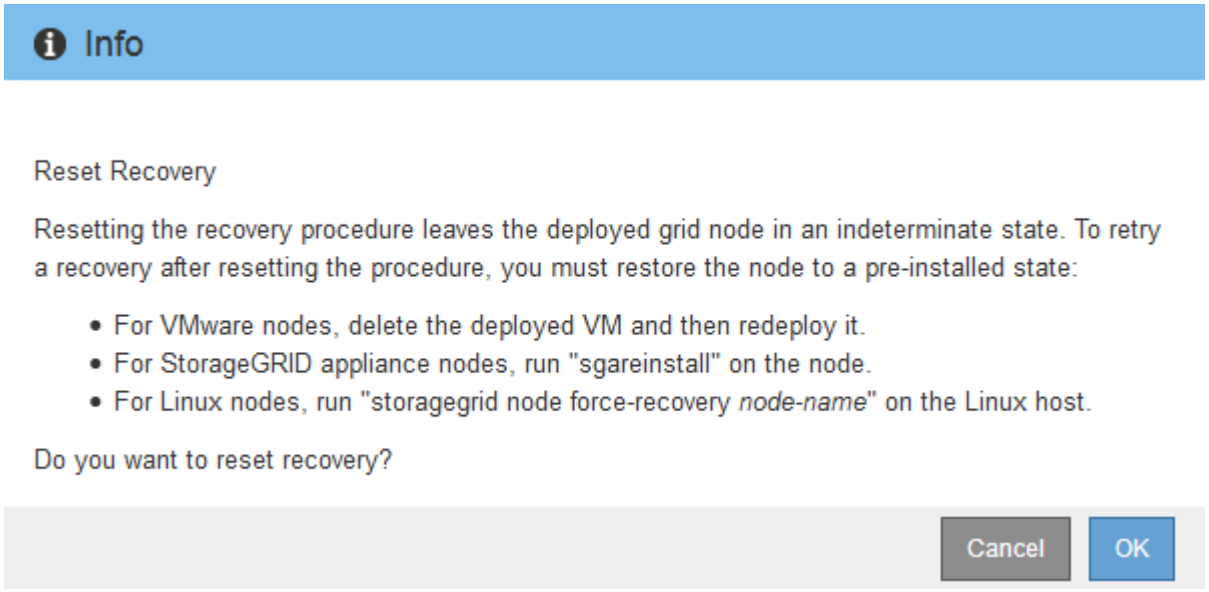
   Knoten werden in der Liste angezeigt, nachdem sie ausgefallen sind. Sie können einen Knoten jedoch erst auswählen, wenn er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Bereitstellungspassphrase** ein.
4. Klicken Sie auf **Wiederherstellung starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Grid-Knoten wird wiederhergestellt“.

> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das darauf hinweist, dass der Knoten in einem unbestimmten Zustand verbleibt, wenn Sie die Prozedur zurücksetzen.



Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Verfahrens wiederholen möchten, müssen Sie den Knoten wie folgt in einen vorinstallierten Zustand zurückversetzen:

- **VMware**: Löschen Sie den bereitgestellten virtuellen Grid-Knoten. Wenn Sie dann bereit sind, die Wiederherstellung neu zu starten, stellen Sie den Knoten erneut bereit.
- **Linux**: Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen: `storagegrid node force-recovery node-name`
- **Appliance**: Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Verfahrens wiederholen möchten, müssen Sie den Appliance-Knoten in einen vorinstallierten Zustand zurücksetzen, indem Sie

`sgareinstall` auf dem Knoten. Sehen "Gerät für Neuinstallation vorbereiten (nur Plattformaustausch)" .

Wiederherstellung nach Archivknotenfehlern

Wiederherstellung nach Archivknotenfehlern

Die Unterstützung für Archivknoten wurde entfernt.

Informationen zum Wiederherstellen von Archivknoten finden Sie unter "Wiederherstellung nach Archivknotenfehlern (StorageGRID 11.8-Dokumentationssite)" .

Linux-Knoten ersetzen

Linux-Knoten ersetzen

Wenn ein Fehler die Bereitstellung eines oder mehrerer neuer physischer oder virtueller Hosts oder die Neuinstallation von Linux auf einem vorhandenen Host erfordert, müssen Sie den Ersatzhost bereitstellen und konfigurieren, bevor Sie den Grid-Knoten wiederherstellen können. Dieses Verfahren ist ein Schritt des Grid-Knoten-Wiederherstellungsprozesses für alle Grid-Knotentypen.

„Linux“ bezieht sich auf eine Bereitstellung von Red Hat® Enterprise Linux®, Ubuntu® oder Debian®. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

Dieses Verfahren wird nur als ein Schritt im Prozess der Wiederherstellung softwarebasierter Speicherknoten, primärer oder nicht primärer Admin-Knoten oder Gateway-Knoten durchgeführt. Die Schritte sind unabhängig vom Typ des Grid-Knotens, den Sie wiederherstellen, identisch.

Wenn mehr als ein Grid-Knoten auf einem physischen oder virtuellen Linux-Host gehostet wird, können Sie die Grid-Knoten in beliebiger Reihenfolge wiederherstellen. Wenn Sie jedoch zuerst einen primären Admin-Knoten wiederherstellen (sofern vorhanden), verhindern Sie, dass die Wiederherstellung anderer Grid-Knoten ins Stocken gerät, wenn diese versuchen, den primären Admin-Knoten zu kontaktieren, um sich für die Wiederherstellung zu registrieren.

Bereitstellen neuer Linux-Hosts

Mit wenigen Ausnahmen bereiten Sie die neuen Hosts genauso vor wie während des Erstinstallationsprozesses.

Um neue oder neu installierte physische oder virtuelle Linux-Hosts bereitzustellen, befolgen Sie die Schritte zum Vorbereiten der Hosts in den StorageGRID -Installationsanweisungen für Ihr Linux-Betriebssystem:

- "Installieren Sie Linux (Red Hat Enterprise Linux)"
- "Installieren Sie Linux (Ubuntu oder Debian)"

Dieses Verfahren umfasst Schritte zum Ausführen der folgenden Aufgaben:

1. Installieren Sie Linux.
2. Konfigurieren Sie das Hostnetzwerk.

3. Konfigurieren Sie den Hostspeicher.
4. Installieren Sie die Container-Engine.
5. Installieren Sie den StorageGRID Hostdienst.

> Beenden Sie den Vorgang, nachdem Sie die Aufgabe „ StorageGRID Hostdienst installieren“ in den Installationsanweisungen abgeschlossen haben. Starten Sie die Aufgabe „Grid-Knoten bereitstellen“ nicht.

Beachten Sie beim Ausführen dieser Schritte die folgenden wichtigen Richtlinien:

- Achten Sie darauf, dieselben Hostschnittstellennamen zu verwenden, die Sie auf dem ursprünglichen Host verwendet haben.
- Wenn Sie gemeinsam genutzten Speicher zur Unterstützung Ihrer StorageGRID -Knoten verwenden oder einige oder alle Laufwerke oder SSDs von den ausgefallenen auf die Ersatzknoten verschoben haben, müssen Sie dieselben Speicherzuordnungen wiederherstellen, die auf dem ursprünglichen Host vorhanden waren. Wenn Sie beispielsweise WWIDs und Aliase in `/etc/multipath.conf` wie in den Installationsanweisungen empfohlen, achten Sie darauf, die gleichen Alias/WWID-Paare in `/etc/multipath.conf` auf dem Ersatzhost.
- Wenn der StorageGRID Knoten Speicher verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass für das Volume keine FabricPool -Tiering-Richtlinie aktiviert ist. Das Deaktivieren der FabricPool Tiering-Funktion für Volumes, die mit StorageGRID -Knoten verwendet werden, vereinfacht die Fehlerbehebung und Speichervorgänge.

> Verwenden Sie FabricPool niemals, um Daten im Zusammenhang mit StorageGRID zurück auf StorageGRID selbst zu verschieben. Das Zurückführen von StorageGRID -Daten in StorageGRID erhöht die Fehlerbehebung und die Betriebskomplexität.

Wiederherstellen von Grid-Knoten auf dem Host

Um einen ausgefallenen Grid-Knoten auf einem neuen Linux-Host wiederherzustellen, führen Sie diese Schritte aus, um die Knotenkonfigurationsdatei wiederherzustellen.

1. Wiederherstellen und Validieren des Knotensdurch Wiederherstellen der Knotenkonfigurationsdatei. Bei einer Neuinstallation erstellen Sie für jeden Grid-Knoten, der auf einem Host installiert werden soll, eine Knotenkonfigurationsdatei. Wenn Sie einen Grid-Knoten auf einem Ersatzhost wiederherstellen, stellen Sie die Knotenkonfigurationsdatei für alle ausgefallenen Grid-Knoten wieder her oder ersetzen sie.
2. Starten Sie den StorageGRID -Hostdienst .
3. Nach BedarfStellen Sie alle Knoten wieder her, die nicht gestartet werden können .

Wenn Blockspeichervolumes vom vorherigen Host beibehalten wurden, müssen Sie möglicherweise zusätzliche Wiederherstellungsverfahren durchführen. Mithilfe der Befehle in diesem Abschnitt können Sie feststellen, welche zusätzlichen Verfahren erforderlich sind.

Wiederherstellen und Validieren von Grid-Knoten

Sie müssen die Grid-Konfigurationsdateien für alle ausgefallenen Grid-Knoten wiederherstellen und dann die Grid-Konfigurationsdateien validieren und alle Fehler beheben.

Informationen zu diesem Vorgang

Sie können jeden Grid-Knoten importieren, der auf dem Host vorhanden sein soll, solange sein `/var/local` Das Volume ging nicht durch den Ausfall des vorherigen Hosts verloren. Zum Beispiel die `/var/local` Das Volume ist möglicherweise noch vorhanden, wenn Sie gemeinsam genutzten Speicher für StorageGRID -Systemdatenvolumes verwendet haben, wie in den StorageGRID Installationsanweisungen für Ihr Linux-Betriebssystem beschrieben. Durch das Importieren des Knotens wird seine Knotenkonfigurationsdatei auf dem Host wiederhergestellt.

Wenn es nicht möglich ist, fehlende Knoten zu importieren, müssen Sie deren Grid-Konfigurationsdateien neu erstellen.

Anschließend müssen Sie die Grid-Konfigurationsdatei validieren und alle möglicherweise auftretenden Netzwerk- oder Speicherprobleme beheben, bevor Sie StorageGRID neu starten. Wenn Sie die Konfigurationsdatei für einen Knoten neu erstellen, müssen Sie für den Ersatzknoten denselben Namen verwenden, der für den Knoten verwendet wurde, den Sie wiederherstellen.

Weitere Informationen zum Standort des `/var/local` Volume für einen Knoten.

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"

Schritte

1. Listen Sie in der Befehlszeile des wiederhergestellten Hosts alle aktuell konfigurierten StorageGRID Knoten auf:`sudo storagegrid node list`

   Wenn keine Rasterknoten konfiguriert sind, erfolgt keine Ausgabe. Wenn einige Grid-Knoten konfiguriert sind, erwarten Sie eine Ausgabe im folgenden Format:

   ```
   Name               Metadata-Volume
   ============================================================
   dc1-adm1           /dev/mapper/sgws-adm1-var-local
   dc1-gw1            /dev/mapper/sgws-gw1-var-local
   dc1-sn1            /dev/mapper/sgws-sn1-var-local
   dc1-arc1           /dev/mapper/sgws-arc1-var-local
   ```

   Wenn einige oder alle Grid-Knoten, die auf dem Host konfiguriert werden sollen, nicht aufgeführt sind, müssen Sie die fehlenden Grid-Knoten wiederherstellen.

2. Um Rasterknoten zu importieren, die eine `/var/local` Volumen:

   a. Führen Sie für jeden Knoten, den Sie importieren möchten, den folgenden Befehl aus:`sudo storagegrid node import node-var-local-volume-path`

      Der `storagegrid node import` Der Befehl ist nur erfolgreich, wenn der Zielknoten auf dem Host, auf dem er zuletzt ausgeführt wurde, ordnungsgemäß heruntergefahren wurde. Wenn dies nicht der Fall ist, wird ein Fehler ähnlich dem folgenden angezeigt:

      ```
      This node (node-name) appears to be owned by another host (UUID host-uuid).

   Use the --force flag if you are sure import is safe.
      ```

   a. Wenn der Fehler angezeigt wird, dass der Knoten einem anderen Host gehört, führen Sie den Befehl

erneut mit dem `--force` Flag zum Abschließen des Imports:`sudo storagegrid --force node import node-var-local-volume-path`

> Alle Knoten, die mit dem `--force` Flagge erfordert zusätzliche Wiederherstellungsschritte, bevor sie wieder in das Netz eintreten können, wie in beschrieben"Was kommt als Nächstes: Führen Sie bei Bedarf weitere Wiederherstellungsschritte durch" .

3. Für Grid-Knoten, die kein `/var/local` Volume: Erstellen Sie die Konfigurationsdatei des Knotens neu, um sie auf dem Host wiederherzustellen. Anweisungen finden Sie unter:
   - "Erstellen Sie Knotenkonfigurationsdateien für Red Hat Enterprise Linux"
   - "Erstellen Sie Knotenkonfigurationsdateien für Ubuntu oder Debian"

   > Wenn Sie die Konfigurationsdatei für einen Knoten neu erstellen, müssen Sie für den Ersatzknoten denselben Namen verwenden, der für den Knoten verwendet wurde, den Sie wiederherstellen. Stellen Sie bei Linux-Bereitstellungen sicher, dass der Name der Konfigurationsdatei den Knotennamen enthält. Sie sollten nach Möglichkeit dieselben Netzwerkschnittstellen, Blockgerätezuordnungen und IP-Adressen verwenden. Durch diese Vorgehensweise wird die Datenmenge minimiert, die während der Wiederherstellung auf den Knoten kopiert werden muss, wodurch die Wiederherstellung erheblich beschleunigt werden kann (in einigen Fällen um Minuten statt um Wochen).

> Wenn Sie neue Blockgeräte (Geräte, die der StorageGRID Knoten zuvor nicht verwendet hat) als Werte für eine der Konfigurationsvariablen verwenden, die mit `BLOCK_DEVICE_` Wenn Sie die Konfigurationsdatei für einen Knoten neu erstellen, folgen Sie den Richtlinien inBeheben Sie Fehler beim Fehlen eines Blockgeräts .

4. Führen Sie den folgenden Befehl auf dem wiederhergestellten Host aus, um alle StorageGRID Knoten aufzulisten.

   ```
   sudo storagegrid node list
   ```

5. Validieren Sie die Knotenkonfigurationsdatei für jeden Grid-Knoten, dessen Name in der Ausgabe der Storagegrid-Knotenliste angezeigt wurde:

   ```
   sudo storagegrid node validate node-name
   ```

   Sie müssen alle Fehler oder Warnungen beheben, bevor Sie den StorageGRID Hostdienst starten. In den folgenden Abschnitten werden Fehler ausführlicher beschrieben, die bei der Wiederherstellung von besonderer Bedeutung sein können.

Beheben Sie Fehler bei fehlenden Netzwerkschnittstellen

Wenn das Host-Netzwerk nicht richtig konfiguriert ist oder ein Name falsch geschrieben ist, tritt ein Fehler auf, wenn StorageGRID die im `/etc/storagegrid/nodes/node-name.conf` Datei.

Möglicherweise wird ein Fehler oder eine Warnung mit diesem Muster angezeigt:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

Der Fehler kann für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk gemeldet werden. Dieser Fehler bedeutet, dass die `/etc/storagegrid/nodes/node-name.conf` Die Datei ordnet das angegebene StorageGRID Netzwerk der Hostschnittstelle mit dem Namen zu *`host-interface-name`* , aber auf dem aktuellen Host gibt es keine Schnittstelle mit diesem Namen.

Wenn Sie diesen Fehler erhalten, überprüfen Sie, ob Sie die Schritte in"Bereitstellen neuer Linux-Hosts" . Verwenden Sie für alle Hostschnittstellen dieselben Namen wie auf dem ursprünglichen Host.

Wenn Sie die Hostschnittstellen nicht so benennen können, dass sie mit der Knotenkonfigurationsdatei übereinstimmen, können Sie die Knotenkonfigurationsdatei bearbeiten und den Wert von GRID_NETWORK_TARGET, ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET so ändern, dass er mit einer vorhandenen Hostschnittstelle übereinstimmt.

Stellen Sie sicher, dass die Hostschnittstelle Zugriff auf den entsprechenden physischen Netzwerkport oder das VLAN bietet und dass die Schnittstelle nicht direkt auf ein Bond- oder Bridge-Gerät verweist. Sie müssen entweder ein VLAN (oder eine andere virtuelle Schnittstelle) über dem Bond-Gerät auf dem Host konfigurieren oder ein Bridge- und Virtual-Ethernet-Paar (veth) verwenden.

Beheben Sie Fehler beim Fehlen eines Blockgeräts

Das System prüft, ob jeder wiederhergestellte Knoten einer gültigen speziellen Blockgerätedatei oder einem gültigen Softlink zu einer speziellen Blockgerätedatei zugeordnet ist. Wenn StorageGRID eine ungültige Zuordnung in der `/etc/storagegrid/nodes/node-name.conf` Datei wird ein Fehler mit dem Namen „fehlendes Blockgerät“ angezeigt.

Wenn Sie einen Fehler feststellen, der diesem Muster entspricht:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Das bedeutet, dass `/etc/storagegrid/nodes/node-name.conf` ordnet das von *node-name* verwendete Blockgerät zu für `PURPOSE` zum angegebenen Pfadnamen im Linux-Dateisystem, aber an diesem Speicherort gibt es keine gültige spezielle Blockgerätedatei oder keinen Softlink zu einer speziellen Blockgerätedatei.

Überprüfen Sie, ob Sie die Schritte in"Bereitstellen neuer Linux-Hosts" . Verwenden Sie für alle Blockgeräte dieselben persistenten Gerätenamen, die auf dem ursprünglichen Host verwendet wurden.

Wenn Sie die fehlende Blockgerät-Spezialdatei nicht wiederherstellen oder neu erstellen können, können Sie ein neues Blockgerät der entsprechenden Größe und Speicherkategorie zuweisen und die Knotenkonfigurationsdatei bearbeiten, um den Wert von `BLOCK_DEVICE_PURPOSE` um auf die neue spezielle Blockgerätedatei zu verweisen.

Ermitteln Sie die passende Größe und Speicherkategorie anhand der Tabellen für Ihr Linux-Betriebssystem:

- "Speicher- und Leistungsanforderungen für Red Hat Enterprise Linux"
- "Speicher- und Leistungsanforderungen für Ubuntu oder Debian"

Lesen Sie die Empfehlungen zum Konfigurieren des Hostspeichers, bevor Sie mit dem Austausch des Blockgeräts fortfahren:

- "Konfigurieren des Hostspeichers für Red Hat Enterprise Linux"
- "Konfigurieren des Hostspeichers für Ubuntu oder Debian"

> Wenn Sie ein neues Blockspeichergerät für eine der Konfigurationsdateivariablen bereitstellen müssen, beginnend mit `BLOCK_DEVICE_` Da das ursprüngliche Blockgerät mit dem ausgefallenen Host verloren gegangen ist, stellen Sie sicher, dass das neue Blockgerät unformatiert ist, bevor Sie weitere Wiederherstellungsverfahren versuchen. Das neue Blockgerät wird unformatiert, wenn Sie gemeinsam genutzten Speicher verwenden und ein neues Volume erstellt haben. Wenn Sie sich nicht sicher sind, führen Sie den folgenden Befehl für alle neuen Spezialdateien des Blockspeichergeräts aus.

> Führen Sie den folgenden Befehl nur für neue Blockspeichergeräte aus. Führen Sie diesen Befehl nicht aus, wenn Sie glauben, dass der Blockspeicher noch gültige Daten für den wiederherzustellenden Knoten enthält, da alle Daten auf dem Gerät verloren gehen.
>
> ```
> sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
> ```

Starten Sie den StorageGRID -Hostdienst

Um Ihre StorageGRID -Knoten zu starten und sicherzustellen, dass sie nach einem Host-Neustart neu gestartet werden, müssen Sie den StorageGRID Hostdienst aktivieren und starten.

Schritte

1. Führen Sie auf jedem Host die folgenden Befehle aus:

   ```
   sudo systemctl enable storagegrid
   sudo systemctl start storagegrid
   ```

2. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Bereitstellung fortgesetzt wird:

   ```
   sudo storagegrid node status node-name
   ```

3. Wenn ein Knoten den Status „Nicht ausgeführt“ oder „Gestoppt“ zurückgibt, führen Sie den folgenden Befehl aus:

   ```
   sudo storagegrid node start node-name
   ```

4. Wenn Sie den StorageGRID Hostdienst zuvor aktiviert und gestartet haben (oder wenn Sie nicht sicher sind, ob der Dienst aktiviert und gestartet wurde), führen Sie außerdem den folgenden Befehl aus:

```
sudo systemctl reload-or-restart storagegrid
```

Wiederherstellen von Knoten, die nicht normal gestartet werden können

Wenn ein StorageGRID -Knoten nicht normal wieder dem Grid beitritt und nicht als wiederherstellbar angezeigt wird, ist er möglicherweise beschädigt. Sie können den Knoten in den Wiederherstellungsmodus zwingen.

Schritte

1. Bestätigen Sie, dass die Netzwerkkonfiguration des Knotens korrekt ist.

   Der Knoten konnte möglicherweise aufgrund falscher Netzwerkschnittstellenzuordnungen oder einer falschen Grid-Netzwerk-IP-Adresse bzw. eines falschen Gateways nicht wieder mit dem Grid verbunden werden.

2. Wenn die Netzwerkkonfiguration korrekt ist, führen Sie die `force-recovery` Befehl:

   ```
   sudo storagegrid node force-recovery node-name
   ```

3. Führen Sie die zusätzlichen Wiederherstellungsschritte für den Knoten aus. Sehen "Was kommt als Nächstes: Führen Sie bei Bedarf weitere Wiederherstellungsschritte durch" .

Was kommt als Nächstes: Führen Sie bei Bedarf weitere Wiederherstellungsschritte durch

Abhängig von den spezifischen Maßnahmen, die Sie ergriffen haben, um die StorageGRID -Knoten auf dem Ersatzhost zum Laufen zu bringen, müssen Sie möglicherweise zusätzliche Wiederherstellungsschritte für jeden Knoten ausführen.

Die Knotenwiederherstellung ist abgeschlossen, wenn Sie beim Ersetzen des Linux-Hosts oder beim Wiederherstellen des ausgefallenen Grid-Knotens auf dem neuen Host keine Korrekturmaßnahmen ergreifen mussten.

Korrekturmaßnahmen und nächste Schritte

Während des Knotenaustauschs mussten Sie möglicherweise eine der folgenden Korrekturmaßnahmen ergreifen:

- Sie mussten die `--force` Flag zum Importieren des Knotens.
- Für alle `<PURPOSE>` , der Wert der `BLOCK_DEVICE_<PURPOSE>` Die Konfigurationsdateivariable bezieht sich auf ein Blockgerät, das nicht mehr dieselben Daten enthält wie vor dem Hostausfall.
- Sie haben `storagegrid node force-recovery node-name` für den Knoten.
- Sie haben ein neues Blockgerät hinzugefügt.

Wenn Sie **eine** dieser Korrekturmaßnahmen ergriffen haben, müssen Sie zusätzliche Wiederherstellungsschritte durchführen.

Art der Wiederherstellung	Nächster Schritt
Primärer Admin-Knoten	"Konfigurieren Sie den Ersatz-Primäradministratorknoten"
Nicht-primärer Admin-Knoten	"Wählen Sie „Wiederherstellung starten“, um den nicht primären Admin-Knoten zu konfigurieren"
Gateway-Knoten	"Wählen Sie „Wiederherstellung starten“, um den Gateway-Knoten zu konfigurieren."
Speicherknoten (softwarebasiert): • Wenn Sie die `--force` Flag zum Importieren des Knotens, oder Sie haben `storagegrid node force-recovery` *`node-name`* • Wenn Sie eine vollständige Neuinstallation des Knotens durchführen mussten oder /var/local wiederherstellen mussten	"Wählen Sie „Wiederherstellung starten“, um den Speicherknoten zu konfigurieren."
Speicherknoten (softwarebasiert): • Wenn Sie ein neues Blockgerät hinzugefügt haben. • Wenn aus irgendeinem `<PURPOSE>` , der Wert der `BLOCK_DEVICE_<PURPOSE>` Die Konfigurationsdateivariable bezieht sich auf ein Blockgerät, das nicht mehr dieselben Daten enthält wie vor dem Hostausfall.	"Wiederherstellung nach einem Speichervolume-Fehler, wenn das Systemlaufwerk intakt ist"

VMware-Knoten ersetzen

Wenn Sie einen ausgefallenen StorageGRID Knoten wiederherstellen, der auf VMware gehostet wurde, entfernen Sie den ausgefallenen Knoten und stellen einen Wiederherstellungsknoten bereit.

Bevor Sie beginnen

Sie haben festgestellt, dass die virtuelle Maschine nicht wiederhergestellt werden kann und ersetzt werden muss.

Informationen zu diesem Vorgang

Sie verwenden den VMware vSphere Web Client, um zunächst die mit dem ausgefallenen Grid-Knoten verknüpfte virtuelle Maschine zu entfernen. Anschließend können Sie eine neue virtuelle Maschine bereitstellen.

Dieses Verfahren ist nur ein Schritt im Wiederherstellungsprozess des Netzknotens. Das Verfahren zum Entfernen und Bereitstellen von Knoten ist für alle VMware-Knoten, einschließlich Admin-Knoten, Speicherknoten und Gateway-Knoten, gleich.

Schritte

1. Melden Sie sich beim VMware vSphere Web Client an.

2. Navigieren Sie zur ausgefallenen virtuellen Grid-Knotenmaschine.
3. Notieren Sie sich alle Informationen, die zum Bereitstellen des Wiederherstellungsknotens erforderlich sind.
   a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie die Registerkarte **Einstellungen bearbeiten** und notieren Sie sich die verwendeten Einstellungen.
   b. Wählen Sie die Registerkarte **vApp-Optionen** aus, um die Netzwerkeinstellungen des Grid-Knotens anzuzeigen und aufzuzeichnen.
4. Wenn es sich bei dem ausgefallenen Grid-Knoten um einen Speicherknoten handelt, stellen Sie fest, ob die zur Datenspeicherung verwendeten virtuellen Festplatten unbeschädigt sind, und bewahren Sie sie für die erneute Verbindung mit dem wiederhergestellten Grid-Knoten auf.
5. Schalten Sie die virtuelle Maschine aus.
6. Wählen Sie **Aktionen** > **Alle vCenter-Aktionen** > **Von Festplatte löschen**, um die virtuelle Maschine zu löschen.
7. Stellen Sie eine neue virtuelle Maschine als Ersatzknoten bereit und verbinden Sie sie mit einem oder mehreren StorageGRID Netzwerken. Anweisungen finden Sie unter"Bereitstellen eines StorageGRID -Knotens als virtuelle Maschine" .

   Wenn Sie den Knoten bereitstellen, können Sie optional Knotenports neu zuordnen oder die CPU- oder Speichereinstellungen erhöhen.

   > Nach der Bereitstellung des neuen Knotens können Sie entsprechend Ihren Speicheranforderungen neue virtuelle Festplatten hinzufügen, alle vom zuvor entfernten ausgefallenen Grid-Knoten gespeicherten virtuellen Festplatten erneut anschließen oder beides.

8. Schließen Sie das Knotenwiederherstellungsverfahren je nach dem Typ des Knotens ab, den Sie wiederherstellen.

Knotentyp	Gehe zu
Primärer Admin-Knoten	"Konfigurieren Sie den Ersatz-Primäradministratorknoten"
Nicht-primärer Admin-Knoten	"Wählen Sie „Wiederherstellung starten“, um den nicht primären Admin-Knoten zu konfigurieren"
Gateway-Knoten	"Wählen Sie „Wiederherstellung starten“, um den Gateway-Knoten zu konfigurieren."
Speicherknoten	"Wählen Sie „Wiederherstellung starten“, um den Speicherknoten zu konfigurieren."

Ersetzen Sie den ausgefallenen Knoten durch eine Service-Appliance

Ersetzen Sie den ausgefallenen Knoten durch eine Service-Appliance

Sie können eine Service-Appliance verwenden, um einen ausgefallenen Gateway-Knoten, einen ausgefallenen nicht-primären Admin-Knoten oder einen ausgefallenen primären Admin-Knoten wiederherzustellen, der auf VMware, einem Linux-Host oder einer Service-Appliance gehostet wurde. Dieses Verfahren ist ein Schritt des Grid-Knoten-Wiederherstellungsverfahrens.

Bevor Sie beginnen

- Sie haben festgestellt, dass eine der folgenden Situationen zutrifft:
  - Die virtuelle Maschine, auf der der Knoten gehostet wird, kann nicht wiederhergestellt werden.
  - Der physische oder virtuelle Linux-Host für den Grid-Knoten ist ausgefallen und muss ersetzt werden.
  - Die Service-Appliance, die den Grid-Knoten hostet, muss ersetzt werden.
- Sie haben bestätigt, dass die Version des StorageGRID Appliance Installer auf der Service-Appliance mit der Softwareversion Ihres StorageGRID -Systems übereinstimmt. Sehen "Überprüfen und aktualisieren Sie die Version des StorageGRID Appliance Installer" .

> Stellen Sie nicht sowohl ein SG110- als auch ein SG1100-Servicegerät oder ein SG100- und ein SG1000-Servicegerät am selben Standort bereit. Dies kann zu unvorhersehbarer Leistung führen.

Informationen zu diesem Vorgang

Sie können eine Service-Appliance verwenden, um einen ausgefallenen Grid-Knoten in den folgenden Fällen wiederherzustellen:

- Der ausgefallene Knoten wurde auf VMware oder Linux gehostet ("Plattformwechsel")
- Der ausgefallene Knoten wurde auf einer Service-Appliance gehostet ("Plattformaustausch")

Services-Appliance installieren (nur Plattformwechsel)

Wenn Sie einen ausgefallenen Grid-Knoten wiederherstellen, der auf VMware oder einem Linux-Host gehostet wurde, und Sie eine Service-Appliance für den Ersatzknoten verwenden, müssen Sie zuerst die neue Appliance-Hardware mit demselben Knotennamen (Systemnamen) wie der ausgefallene Knoten installieren.

Bevor Sie beginnen

Sie verfügen über die folgenden Informationen zum ausgefallenen Knoten:

- **Knotenname**: Sie müssen die Dienst-Appliance mit demselben Knotennamen wie der ausgefallene Knoten installieren. Der Knotenname ist der Hostname (Systemname).
- **IP-Adressen**: Sie können der Service-Appliance dieselben IP-Adressen wie dem ausgefallenen Knoten zuweisen (was die bevorzugte Option ist) oder Sie können in jedem Netzwerk eine neue, nicht verwendete IP-Adresse auswählen.

Informationen zu diesem Vorgang

Führen Sie dieses Verfahren nur aus, wenn Sie einen ausgefallenen Knoten wiederherstellen, der auf VMware oder Linux gehostet wurde, und ihn durch einen Knoten ersetzen, der auf einer Service-Appliance gehostet wird.

Schritte

1. Befolgen Sie die Anweisungen zum Installieren einer neuen Service-Appliance. Sehen "Schnellstart für die Hardwareinstallation" .
2. Wenn Sie zur Eingabe eines Knotennamens aufgefordert werden, verwenden Sie den Knotennamen des ausgefallenen Knotens.

Gerät für Neuinstallation vorbereiten (nur Plattformaustausch)

Wenn Sie einen Grid-Knoten wiederherstellen, der auf einer Service-Appliance gehostet wurde, müssen Sie die Appliance zunächst für die Neuinstallation der StorageGRID -Software vorbereiten.

Führen Sie dieses Verfahren nur aus, wenn Sie einen ausgefallenen Knoten ersetzen, der auf einer Service-Appliance gehostet wurde. Führen Sie diese Schritte nicht aus, wenn der ausgefallene Knoten ursprünglich auf VMware oder einem Linux-Host gehostet wurde.

Schritte

1. Melden Sie sich beim ausgefallenen Grid-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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. Bereiten Sie das Gerät für die Installation der StorageGRID -Software vor. Eingeben: `sgareinstall`
3. Wenn Sie aufgefordert werden, fortzufahren, geben Sie Folgendes ein: `y`

   Das Gerät wird neu gestartet und Ihre SSH-Sitzung wird beendet. Normalerweise dauert es etwa 5 Minuten, bis das StorageGRID Appliance Installer verfügbar ist. In einigen Fällen kann es jedoch bis zu 30 Minuten dauern.

   Die Service-Appliance wird zurückgesetzt und auf die Daten auf dem Grid-Knoten kann nicht mehr zugegriffen werden. Während des ursprünglichen Installationsvorgangs konfigurierte IP-Adressen sollten erhalten bleiben. Es wird jedoch empfohlen, dies nach Abschluss des Vorgangs zu bestätigen.

   Nach der Ausführung des `sgareinstall` Befehl werden alle von StorageGRID bereitgestellten Konten, Kennwörter und SSH-Schlüssel entfernt und neue Hostschlüssel generiert.

Starten Sie die Softwareinstallation auf der Service-Appliance

Um einen Gateway-Knoten oder Admin-Knoten auf einer Service-Appliance zu installieren, verwenden Sie den StorageGRID Appliance Installer, der auf der Appliance enthalten ist.

Bevor Sie beginnen

- Das Gerät wird in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.

- Netzwerkverbindungen und IP-Adressen werden für das Gerät mithilfe des StorageGRID Appliance Installer konfiguriert.
- Wenn Sie einen Gateway-Knoten oder einen nicht primären Admin-Knoten installieren, kennen Sie die IP-Adresse des primären Admin-Knotens für das StorageGRID Grid.
- Alle auf der IP-Konfigurationsseite des StorageGRID Appliance Installer aufgeführten Grid-Netzwerk-Subnetze sind in der Grid-Netzwerk-Subnetzliste auf dem primären Admin-Knoten definiert.

  Sehen "Schnellstart für die Hardwareinstallation" .

- Sie verwenden eine"unterstützter Webbrowser" .
- Ihnen ist eine der dem Gerät zugewiesenen IP-Adressen zugeordnet. Sie können die IP-Adresse für das Admin-Netzwerk, das Grid-Netzwerk oder das Client-Netzwerk verwenden.
- Wenn Sie einen primären Admin-Knoten installieren, stehen Ihnen die Ubuntu- oder Debian-Installationsdateien für diese Version von StorageGRID zur Verfügung.

> ⓘ Eine aktuelle Version der StorageGRID -Software wird während der Herstellung auf das Servicegerät vorinstalliert. Wenn die vorinstallierte Softwareversion mit der in Ihrer StorageGRID Bereitstellung verwendeten Version übereinstimmt, benötigen Sie die Installationsdateien nicht.

Informationen zu diesem Vorgang

So installieren Sie die StorageGRID -Software auf einer Service-Appliance:

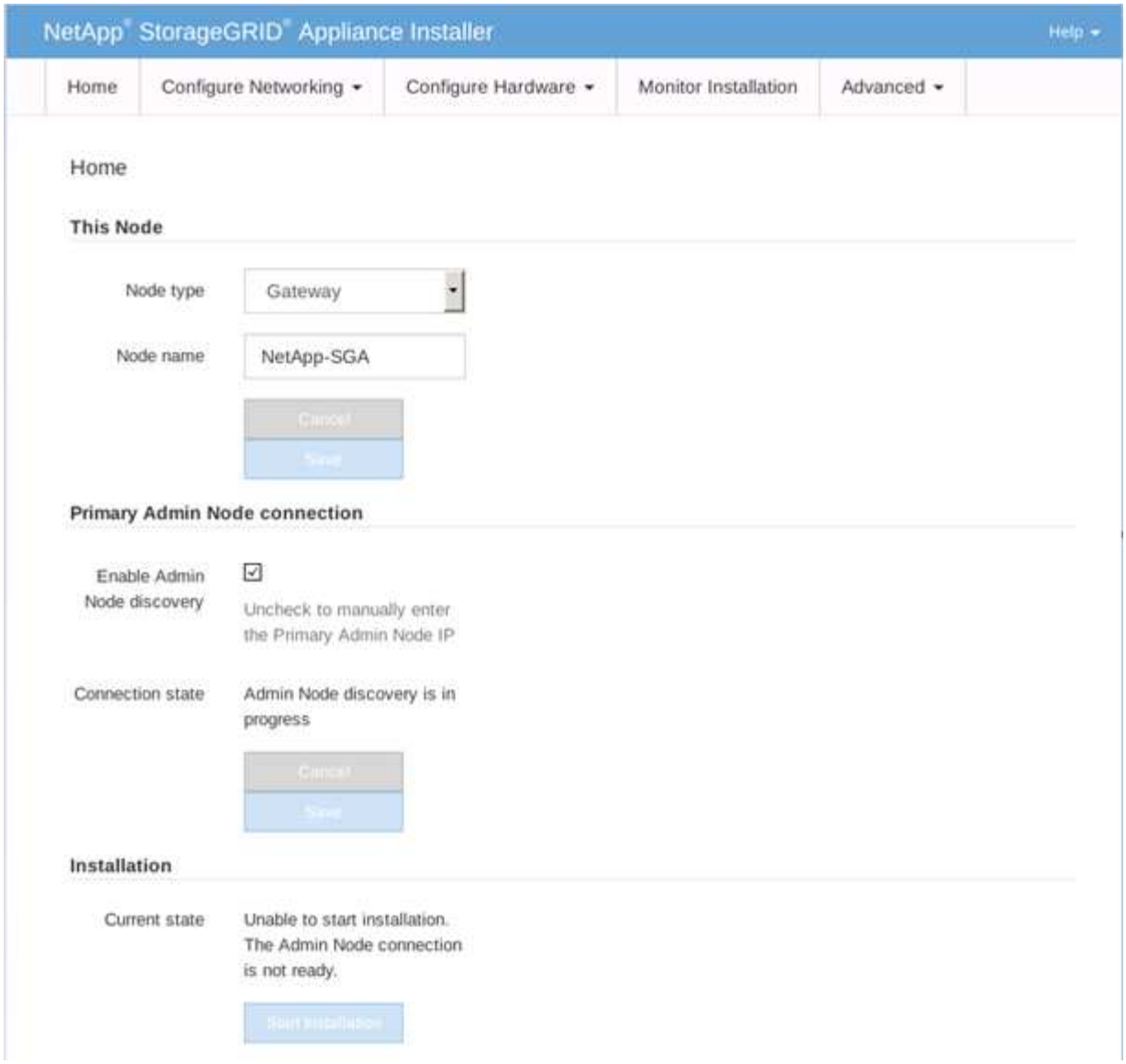
- Für einen primären Admin-Knoten geben Sie den Namen des Knotens an und laden dann die entsprechenden Softwarepakete hoch (falls erforderlich).
- Für einen nicht primären Admin-Knoten oder einen Gateway-Knoten geben Sie die IP-Adresse des primären Admin-Knotens und den Namen des Knotens an oder bestätigen diese.
- Sie starten die Installation und warten, während die Volumes konfiguriert und die Software installiert wird.
- Während des Vorgangs wird die Installation unterbrochen. Um die Installation fortzusetzen, müssen Sie sich beim Grid Manager anmelden und den ausstehenden Knoten als Ersatz für den ausgefallenen Knoten konfigurieren.
- Nachdem Sie den Knoten konfiguriert haben, wird der Installationsprozess der Appliance abgeschlossen und die Appliance neu gestartet.

Schritte

1. Öffnen Sie einen Browser und geben Sie eine der IP-Adressen für die Service-Appliance ein.

   `https://Controller_IP:8443`

   Die Startseite des StorageGRID Appliance-Installationsprogramms wird angezeigt.



2. So installieren Sie einen primären Admin-Knoten:

   a. Wählen Sie im Abschnitt „Dieser Knoten“ für **Knotentyp** die Option **Primäradministrator** aus.

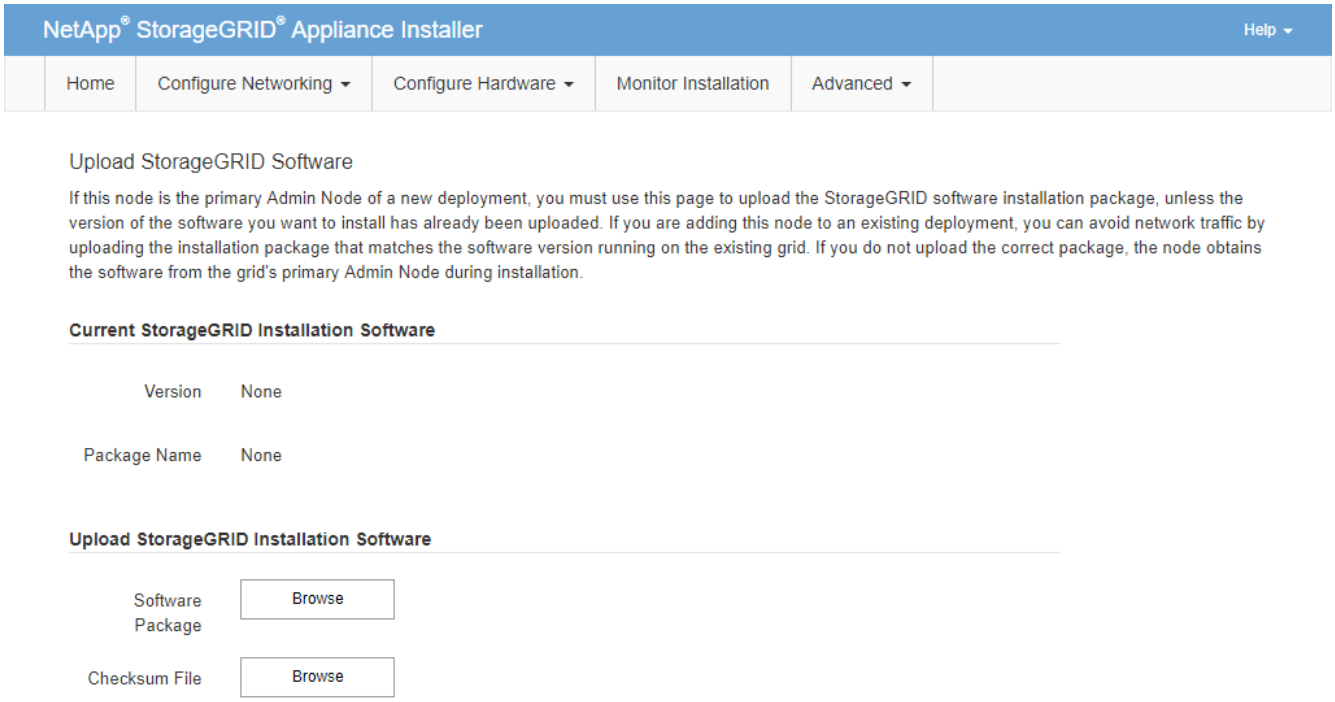
   b. Geben Sie im Feld **Knotenname** denselben Namen ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.

   c. Überprüfen Sie im Abschnitt Installation die unter Aktueller Status aufgeführte Softwareversion

      Wenn die zur Installation bereitstehende Softwareversion korrekt ist, fahren Sie mit demInstallationsschritt .

   d. Wenn Sie eine andere Softwareversion hochladen müssen, wählen Sie im Menü **Erweitert** die Option * StorageGRID -Software hochladen*.

      Die Seite „StorageGRID -Software hochladen“ wird angezeigt.



a. Klicken Sie auf **Durchsuchen**, um das **Softwarepaket** und die **Prüfsummendatei** für die StorageGRID -Software hochzuladen.

   Die Dateien werden nach der Auswahl automatisch hochgeladen.

b. Klicken Sie auf **Home**, um zur Startseite des StorageGRID Appliance Installer zurückzukehren.

3. So installieren Sie einen Gateway-Knoten oder einen nicht primären Admin-Knoten:

   a. Wählen Sie im Abschnitt „Dieser Knoten“ für **Knotentyp** je nach Knotentyp, den Sie wiederherstellen, **Gateway** oder **Nicht-primärer Administrator** aus.

   b. Geben Sie im Feld **Knotenname** denselben Namen ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.

   c. Legen Sie im Abschnitt „Verbindung zum primären Admin-Knoten“ fest, ob Sie die IP-Adresse für den primären Admin-Knoten angeben müssen.

      Das StorageGRID Appliance Installer kann diese IP-Adresse automatisch erkennen, vorausgesetzt, der primäre Admin-Knoten oder mindestens ein anderer Grid-Knoten mit konfigurierter ADMIN_IP ist im selben Subnetz vorhanden.

   d. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	a. Deaktivieren Sie das Kontrollkästchen **Admin-Knotenerkennung aktivieren**. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie auf **Speichern**. d. Warten Sie, bis der Verbindungsstatus für die neue IP-Adresse „Bereit“ lautet.

Option	Beschreibung
Automatische Erkennung aller verbundenen primären Admin-Knoten	a. Aktivieren Sie das Kontrollkästchen **Admin-Knotenerkennung aktivieren**. b. Wählen Sie aus der Liste der erkannten IP-Adressen den primären Admin-Knoten für das Grid aus, in dem diese Service-Appliance bereitgestellt wird. c. Klicken Sie auf **Speichern**. d. Warten Sie, bis der Verbindungsstatus für die neue IP-Adresse „Bereit“ lautet.

4. Bestätigen Sie im Abschnitt „Installation“, dass der aktuelle Status „Bereit zum Starten der Installation des Knotennamens“ lautet und dass die Schaltfläche „Installation starten“ aktiviert ist.

   Wenn die Schaltfläche **Installation starten** nicht aktiviert ist, müssen Sie möglicherweise die Netzwerkkonfiguration oder die Porteinstellungen ändern. Anweisungen hierzu finden Sie in der Wartungsanleitung Ihres Geräts.

5. Klicken Sie auf der Startseite des StorageGRID Appliance Installer auf **Installation starten**.

   Der aktuelle Status ändert sich in „Installation läuft“ und die Seite „Monitorinstallation“ wird angezeigt.

   Wenn Sie manuell auf die Seite „Monitorinstallation“ zugreifen müssen, klicken Sie in der Menüleiste auf „Monitorinstallation“.

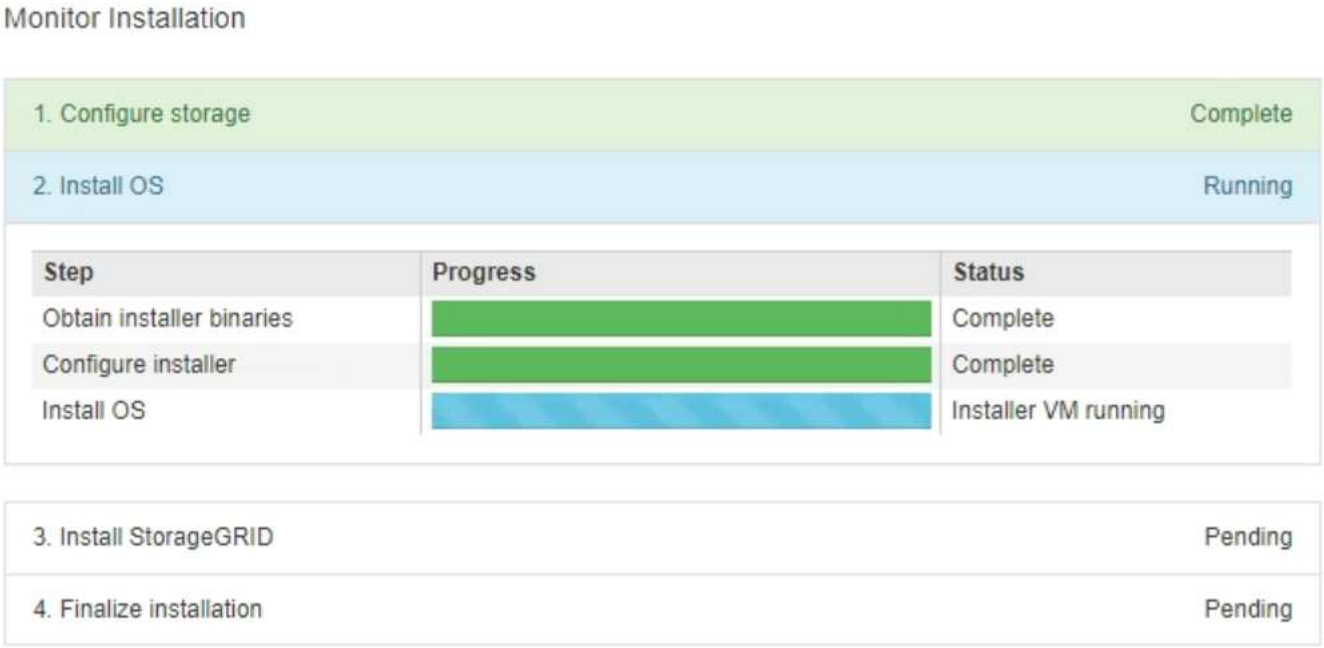
Installation der Appliance für Überwachungsdienste

Der StorageGRID Appliance Installer zeigt den Status an, bis die Installation abgeschlossen ist. Wenn die Softwareinstallation abgeschlossen ist, wird das Gerät neu gestartet.

Schritte

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

   Auf der Seite „Installation überwachen“ wird der Installationsfortschritt angezeigt.



Die blaue Statusleiste zeigt an, welche Aufgabe gerade ausgeführt wird. Grüne Statusbalken zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.

> Das Installationsprogramm stellt sicher, dass Aufgaben, die bei einer vorherigen Installation abgeschlossen wurden, nicht erneut ausgeführt werden. Wenn Sie eine Installation erneut ausführen, werden alle Aufgaben, die nicht erneut ausgeführt werden müssen, mit einer grünen Statusleiste und dem Status „Übersprungen“ angezeigt.

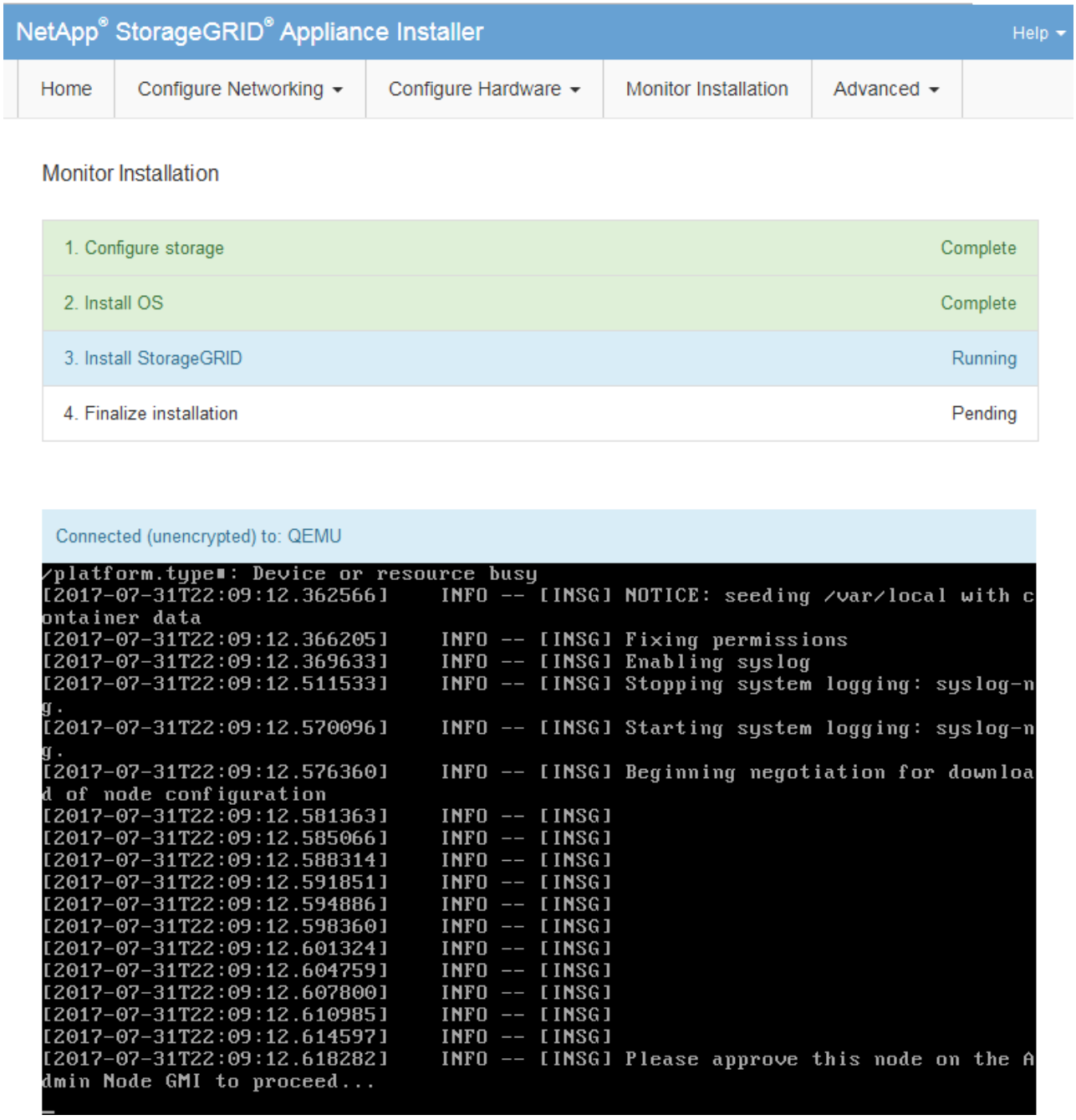
2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.
   - **1. Speicher konfigurieren**

     Während dieser Phase löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken und konfiguriert die Hosteinstellungen.

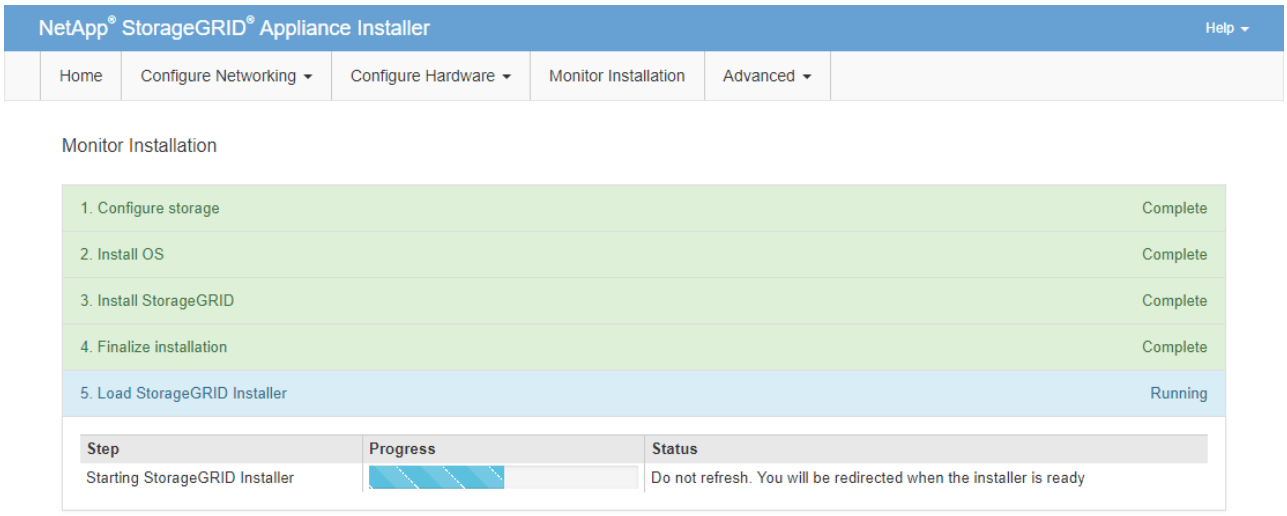
   - **2. Betriebssystem installieren**

     Während dieser Phase kopiert das Installationsprogramm das Basisbetriebssystem-Image für StorageGRID vom primären Admin-Knoten auf die Appliance oder installiert das Basisbetriebssystem aus dem Installationspaket für den primären Admin-Knoten.

3. Überwachen Sie den Installationsfortschritt weiter, bis eines der folgenden Ereignisse eintritt:
   - Bei Gateway-Knoten oder nicht primären Appliance-Admin-Knoten wird die Phase * StorageGRID installieren* angehalten und auf der eingebetteten Konsole wird eine Meldung angezeigt, in der Sie aufgefordert werden, diesen Knoten mithilfe des Grid Managers auf dem Admin-Knoten zu genehmigen.



- Für primäre Admin-Knoten der Appliance wird eine fünfte Phase (StorageGRID -Installationsprogramm laden) angezeigt. Wenn die fünfte Phase länger als 10 Minuten dauert, aktualisieren Sie die Seite manuell.



4. Fahren Sie mit dem nächsten Schritt des Wiederherstellungsprozesses für den Typ des Appliance-Grid-Knotens fort, den Sie wiederherstellen.

Art der Wiederherstellung	Referenz
Gateway-Knoten	"Wählen Sie „Wiederherstellung starten“, um den Gateway-Knoten zu konfigurieren."
Nicht-primärer Admin-Knoten	"Wählen Sie „Wiederherstellung starten“, um den nicht primären Admin-Knoten zu konfigurieren"
Primärer Admin-Knoten	"Konfigurieren Sie den Ersatz-Primäradministratorknoten"

So stellt der technische Support eine Site wieder her

Wenn eine gesamte StorageGRID -Site ausfällt oder mehrere Storage Nodes ausfallen, müssen Sie sich an den technischen Support wenden. Der technische Support beurteilt Ihre Situation, entwickelt einen Wiederherstellungsplan und stellt dann die ausgefallenen Knoten oder Sites auf eine Weise wieder her, die Ihren Geschäftszielen entspricht, die Wiederherstellungszeit optimiert und unnötigen Datenverlust verhindert.

Die Site-Wiederherstellung kann nur durch den technischen Support durchgeführt werden.

StorageGRID -Systeme sind widerstandsfähig gegenüber einer Vielzahl von Ausfällen und Sie können viele Wiederherstellungs- und Wartungsverfahren erfolgreich selbst durchführen. Es ist jedoch schwierig, ein einfaches, allgemeines Verfahren zur Site-Wiederherstellung zu erstellen, da die detaillierten Schritte von Faktoren abhängen, die für Ihre Situation spezifisch sind. Beispiel:

- **Ihre Geschäftsziele**: Nach dem vollständigen Verlust einer StorageGRID -Site sollten Sie prüfen, wie Sie Ihre Geschäftsziele am besten erreichen können. Möchten Sie beispielsweise die verlorene Site vor Ort wiederherstellen? Möchten Sie den verlorenen StorageGRID -Standort an einem neuen Standort ersetzen? Die Situation jedes Kunden ist anders und Ihr Wiederherstellungsplan muss auf Ihre Prioritäten zugeschnitten sein.

- **Genaue Art des Fehlers**: Stellen Sie vor Beginn einer Site-Wiederherstellung fest, ob alle Knoten am ausgefallenen Standort intakt sind oder ob Speicherknoten wiederherstellbare Objekte enthalten. Wenn Sie Knoten oder Speichervolumes neu erstellen, die gültige Daten enthalten, kann es zu unnötigem Datenverlust kommen.
- **Aktive ILM-Richtlinien**: Anzahl, Typ und Speicherort der Objektkopien in Ihrem Grid werden durch Ihre aktiven ILM-Richtlinien gesteuert. Die Einzelheiten Ihrer ILM-Richtlinien können sich auf die Menge der wiederherstellbaren Daten sowie auf die spezifischen Techniken auswirken, die für die Wiederherstellung erforderlich sind.

  Wenn eine Site die einzige Kopie eines Objekts enthält und die Site verloren geht, ist das Objekt verloren.

- **Bucket- (oder Container-)Konsistenz**: Die auf einen Bucket (oder Container) angewendete Konsistenz beeinflusst, ob StorageGRID Objektmetadaten vollständig auf alle Knoten und Sites repliziert, bevor einem Client mitgeteilt wird, dass die Objektaufnahme erfolgreich war. Wenn der Konsistenzwert eine eventuelle Konsistenz zulässt, sind möglicherweise einige Objektmetadaten beim Site-Fehler verloren gegangen. Dies kann sich auf die Menge der wiederherstellbaren Daten und möglicherweise auf die Details des Wiederherstellungsverfahrens auswirken.
- **Verlauf der letzten Änderungen**: Die Details Ihres Wiederherstellungsverfahrens können davon beeinflusst werden, ob zum Zeitpunkt des Fehlers Wartungsvorgänge ausgeführt wurden oder ob kürzlich Änderungen an Ihren ILM-Richtlinien vorgenommen wurden. Der technische Support muss die jüngste Historie Ihres Netzes sowie dessen aktuelle Situation beurteilen, bevor mit der Wiederherstellung der Site begonnen wird.

Die Site-Wiederherstellung kann nur durch den technischen Support durchgeführt werden.

Dies ist eine allgemeine Übersicht über den Prozess, den der technische Support zur Wiederherstellung einer ausgefallenen Site verwendet:

1. Technische Unterstützung:
   a. Nimmt eine detaillierte Bewertung des Fehlers vor.
   b. Arbeitet mit Ihnen zusammen, um Ihre Geschäftsziele zu überprüfen.
   c. Entwickelt einen auf Ihre Situation zugeschnittenen Wiederherstellungsplan.
2. Wenn der primäre Admin-Knoten ausgefallen ist, wird er vom technischen Support wiederhergestellt.
3. Der technische Support stellt alle Speicherknoten gemäß diesem Schema wieder her:
   a. Ersetzen Sie die Storage Node-Hardware oder virtuellen Maschinen nach Bedarf.
   b. Stellen Sie die Objektmetadaten auf der ausgefallenen Site wieder her.
   c. Stellen Sie Objektdaten auf den wiederhergestellten Speicherknoten wieder her.

   Wenn die Wiederherstellungsverfahren für einen einzelnen ausgefallenen Speicherknoten verwendet werden, kommt es zu Datenverlust.

   Wenn eine ganze Site ausgefallen ist, verwendet der technische Support spezielle Befehle, um Objekte und Objektmetadaten erfolgreich wiederherzustellen.

4. Der technische Support stellt andere ausgefallene Knoten wieder her.

Nachdem Objektmetadaten und Daten wiederhergestellt wurden, verwendet der technische Support Standardverfahren, um ausgefallene Gateway-Knoten oder nicht primäre Admin-Knoten wiederherzustellen.

Ähnliche Informationen

"Standortstilllegung"

So aktivieren Sie StorageGRID in Ihrer Umgebung

Gehe zu "So aktivieren Sie StorageGRID" um zu erfahren, wie Sie Anwendungen in Ihrer StorageGRID Umgebung testen und aktivieren.

So verwalten Sie StorageGRID mit der NetApp Konsole

Gehe zu "StorageGRID -Verwaltung über die NetApp Konsole" um zu erfahren, wie Sie Ihre StorageGRID -Systeme mithilfe von Grid Manager über die NetApp -Konsole verwalten und die Datendienste der NetApp Konsole für Backups, Daten-Tiering und mehr nutzen.

- BlueXP heißt jetzt NetApp Console*

Die NetApp Console basiert auf der verbesserten und neu strukturierten BlueXP -Grundlage und ermöglicht die zentrale Verwaltung von NetApp Storage und NetApp Data Services in On-Premises- und Cloud-Umgebungen auf Unternehmensniveau. Sie liefert Einblicke in Echtzeit, schnellere Workflows und eine vereinfachte Administration mit hoher Sicherheit und Konformität.

Einzelheiten zu den Änderungen finden Sie im"Versionshinweise zur NetApp Konsole" .

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

https://library.netapp.com/ecm/ecm_download_file/ECMLP3330669