



StorageGRID 11.7-Dokumentation

StorageGRID

NetApp
June 12, 2025

Inhalt

StorageGRID 11.7-Dokumentation	1
Versionshinweise	2
Los geht's	3
Weitere Informationen zu StorageGRID	3
Was ist StorageGRID?	3
Hybrid Clouds mit StorageGRID	6
StorageGRID Architektur und Netzwerktopologie	7
Managen von Daten mit StorageGRID	16
Entdecken Sie StorageGRID	29
Netzwerkrichtlinien	41
Netzwerkrichtlinien: Überblick	41
StorageGRID-Netzwerktypen	42
Beispiele für Netzwerktopologie	46
Netzwerkanforderungen	53
Netzwerkspezifische Anforderungen	54
Implementierungs-spezifische Netzwerküberlegungen	56
Netzwerkinstallation und -Bereitstellung	59
Richtlinien nach der Installation	60
Referenz für Netzwerk-Ports	60
Schnellstart für StorageGRID	70
Installation und Upgrade	73
Appliance-Hardware installieren	73
Schnellstart für die Hardwareinstallation	73
Hardware-Übersichten	74
Installation vorbereiten	102
Automatisierung der Appliance-Installation und -Konfiguration	148
Automatisieren Sie die StorageGRID-Konfiguration	154
Überblick über die Installations-REST-APIs	155
Hardware installieren	157
Richten Sie die Hardware ein	198
Implementieren des Appliance-Node	248
Installieren Sie Red hat Enterprise Linux oder CentOS	285
Red hat Enterprise Linux oder CentOS: Übersicht installieren	285
Planung und Vorbereitung der Installation von Red hat oder CentOS	286
Implementierung von virtuellen Grid-Nodes (Red hat oder CentOS)	310
Grid Konfiguration und vollständige Installation (Red hat oder CentOS)	331
Automatisierung der Installation (Red hat Enterprise Linux oder CentOS)	345
Überblick über DIE REST API zur Installation	348
Weitere Schritte	349
Fehlerbehebung bei Installationsproblemen	350
Beispiel /etc/sysconfig/Network-scripts	350
Installieren Sie Ubuntu oder Debian	353
Installieren Sie Ubuntu oder Debian: Übersicht	353

Planen und bereiten Sie sich auf die Installation von Ubuntu oder Debian vor	354
Virtuelle Grid-Nodes implementieren (Ubuntu oder Debian)	378
Grid und vollständige Installation konfigurieren (Ubuntu oder Debian)	399
Automatisieren der Installation (Ubuntu oder Debian)	413
Überblick über DIE REST API zur Installation	416
Weitere Schritte	417
Fehlerbehebung bei Installationsproblemen	418
Beispiel /etc/Netzwerk/Schnittstellen	418
VMware installieren	420
Installieren von VMware: Übersicht	420
Planung und Vorbereitung der VMware Installation	421
Virtual Machine Grid-Nodes (VMware) implementieren	429
Grid-Konfiguration und vollständige Installation (VMware)	438
Automatisieren der Installation (VMware)	452
Überblick über DIE REST API zur Installation	466
Weitere Schritte	467
Fehlerbehebung bei Installationsproblemen	468
Upgrade der StorageGRID Software	469
Upgrade der StorageGRID Software: Übersicht	469
Neuerungen bei StorageGRID 11.7	469
Funktionen entfernt oder veraltet	474
Änderungen an der Grid-Management-API	476
Änderungen an der Mandantenmanagement-API	476
Planung und Vorbereitung für Upgrades	477
Software-Upgrade	485
Behebung von Upgrade-Problemen	493
Konfiguration und Management	496
StorageGRID verwalten	496
Administration StorageGRID: Überblick	496
Erste Schritte mit Grid Manager	496
Kontrolle des Zugriffs auf StorageGRID	526
Grid-Verbund verwenden	574
Sicherheitsmanagement	612
Verwalten von Mandanten	689
Client-Verbindungen konfigurieren	708
Netzwerke und Verbindungen verwalten	751
Verwenden Sie AutoSupport	768
Managen Sie Storage-Nodes	783
Managen Sie Admin-Nodes	805
Archiv-Nodes Managen	816
Datenmigration zu StorageGRID	839
Objektmanagement mit ILM	841
Objekte mit ILM managen: Übersicht	841
ILM und Objekt-Lebenszyklus	842
Speicherklassen erstellen und zuweisen	864

Nutzung von Speicherpools	866
Verwendung Von Cloud Storage Pools	875
Profile für das Erasure Coding managen	896
Regionen konfigurieren (nur optional und S3)	900
ILM-Regel erstellen	902
ILM-Richtlinie erstellen	919
Arbeiten mit ILM-Richtlinien und ILM-Regeln	936
Verwenden Sie die S3-Objektsperre	940
Beispiele für ILM-Regeln und -Richtlinien	949
Systemhärtung	968
Systemhärtung: Übersicht	969
Hardening-Richtlinien für Software Upgrades	969
Hardening Guidelines for StorageGRID Networks	970
Hardening-Richtlinien für StorageGRID-Knoten	971
Härtungsrichtlinien für TLS und SSH	974
Andere Hinweise zur Verhärtung	975
Konfigurieren Sie StorageGRID für FabricPool	976
Configure StorageGRID for FabricPool: Übersicht	977
Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier	978
Verwenden Sie den FabricPool-Einrichtungsassistenten	980
Konfigurieren Sie StorageGRID manuell	995
Konfigurieren Sie ONTAP System Manager	1006
Konfigurieren Sie den DNS-Server	1008
StorageGRID Best Practices für FabricPool	1008
FabricPool-Daten aus StorageGRID entfernen	1013
Verwenden Sie StorageGRID	1014
Verwenden Sie ein Mandantenkonto	1014
Verwenden Sie ein Mandantenkonto: Überblick	1014
So melden Sie sich an und melden sich ab	1015
Mandantenmanager-Dashboard verstehen	1020
Mandantenmanagement-API	1023
Netzverbundverbindungen verwenden	1028
Verwalten von Gruppen und Benutzern	1041
Managen von S3-Zugriffsschlüsseln	1061
Management von S3-Buckets	1066
Management von S3-Plattform-Services	1087
S3-REST-API VERWENDEN	1130
Von S3 REST API unterstützte Versionen und Updates	1130
Schnelle Referenz: Unterstützte S3-API-Anforderungen	1132
Mandantenkonten und -Verbindungen konfigurieren	1151
Unterstützung von StorageGRID Plattform-Services	1154
So implementiert StorageGRID die S3-REST-API	1155
Unterstützung für Amazon S3-REST-API	1173
StorageGRID S3-Anforderungen	1224
Bucket- und Gruppenzugriffsrichtlinien	1245

Konfigurieren Sie die Sicherheit für DIE REST API	1271
Monitoring und Prüfung von Vorgängen	1273
Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen	1277
Swift REST API verwenden (veraltet)	1279
Übersicht über die Swift REST API	1279
Mandantenkonten und -Verbindungen konfigurieren	1282
Von Swift UNTERSTÜTZTE REST-API-Operationen	1286
StorageGRID Swift REST-API-Operationen	1299
Konfigurieren Sie die Sicherheit für DIE REST API	1302
Monitoring und Prüfung von Vorgängen	1304
Monitoring und Fehlerbehebung	1309
Überwachen Sie das StorageGRID-System	1309
Überwachen eines StorageGRID-Systems: Übersicht	1309
Das Dashboard anzeigen und verwalten	1309
Zeigen Sie die Seite Knoten an	1312
Informationen, die Sie regelmäßig überwachen sollten	1348
Alarmer und Alarme	1378
Referenz für Protokolldateien	1474
Konfigurieren von Überwachungsmeldungen und Protokollzielen	1493
Verwenden Sie einen externen Syslog-Server	1497
Verwenden Sie SNMP-Überwachung	1509
Erfassung zusätzlicher StorageGRID-Daten	1526
Fehlerbehebung für das StorageGRID-System	1559
Fehlerbehebung bei einem StorageGRID-System: Übersicht	1559
Behebung von Objekt- und Storage-Problemen	1568
Behebung von Metadatenproblemen	1605
Fehlerbehebung bei Zertifikatfehlern	1612
Fehlerbehebung bei Problemen mit Admin-Node und Benutzeroberfläche	1613
Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen	1617
Fehlerbehebung für einen externen Syslog-Server	1626
Prüfung von Audit-Protokollen	1630
Audit-Protokolle: Übersicht	1630
Meldungsfluss und -Aufbewahrung von Audits	1630
Zugriff auf die Audit-Log-Datei	1633
Drehung der Audit-Log-Dateien	1634
Format der Auditprotokolldatei	1635
Überwachungsmeldungsformat	1648
Überwachungsmeldungen und der Lebenszyklus von Objekten	1652
Audit-Meldungen	1660
Wartung	1715
Erweitern Sie Ihr Raster	1715
Raster erweitern: Übersicht	1715
Planen Sie eine Erweiterung von StorageGRID	1716
Sammeln Sie die erforderlichen Materialien	1727
Hinzufügen von Storage-Volumes	1734

Grid-Nodes oder Standort hinzufügen	1742
Erweitertes System konfigurieren	1757
Wenden Sie sich an den technischen Support	1767
Stellen Sie Nodes wieder her und warten Sie das Grid	1768
Recovery and Maintain: Übersicht	1768
Recovery Package Herunterladen	1769
StorageGRID Hotfix Verfahren	1769
Verfahren zur Recovery von Grid-Nodes	1777
Durchführen der Standortwiederherstellung durch den technischen Support	1897
Verfahren zur Deaktivierung	1899
Benennen Sie Raster, Standorte und Nodes um	1951
Netzwerkwartungsverfahren	1961
Verfahren auf Host-Ebene und Middleware	1988
Verfahren für den Grid-Node	1996
Halten Sie die Appliance-Konfiguration aufrecht	2021
Allgemeine Verfahren für die Knotenwartung: Übersicht	2021
Stellen Sie das Gerät in den Wartungsmodus	2022
MTU-Einstellung ändern	2024
Überprüfen Sie die DNS-Server-Konfiguration	2026
Aktualisieren Sie die MAC-Adressenverweise	2028
Überwachung der Node-Verschlüsselung im Wartungsmodus	2029
Klonen von Appliance-Nodes	2034
Instandhaltung der SGF6112 Hardware	2041
SGF6112-Appliance warten	2041
Konfigurationswartungsverfahren	2042
Hardware-Wartungsverfahren	2048
Wartung der SG6000 Hardware	2082
Warten Sie die SG6000-Appliance	2082
Verfahren zur Wartungskonfiguration	2083
Hardware-Verfahren	2108
Instandhaltung der SG5700 Hardware	2140
SG5700 Appliance warten	2140
Verfahren zur Wartungskonfiguration	2140
Hardware-Verfahren	2159
SG5600-Appliance warten	2174
Instandhaltung der SG100 und SG1000 Hardware	2174
Wartung von SG100 und SG1000 Appliances	2174
Verfahren zur Wartungskonfiguration	2175
Hardware-Verfahren	2179
StorageGRID in Ihrer Umgebung aktivieren	2189
Rechtliche Hinweise	2190
Urheberrecht	2190
Marken	2190
Patente	2190
Datenschutzrichtlinie	2190

StorageGRID 11.7-Dokumentation

Versionshinweise

Release-spezifische Informationen zu neuen Funktionen, entfernten oder veralteten Funktionen, festen Problemen und bekannten Problemen erhalten

Loggen Sie sich auf der NetApp Support Site unter ein ["PDF-Datei anzeigen oder herunterladen"](#) Enthält die Versionshinweise zu StorageGRID 11.7.

Los geht's

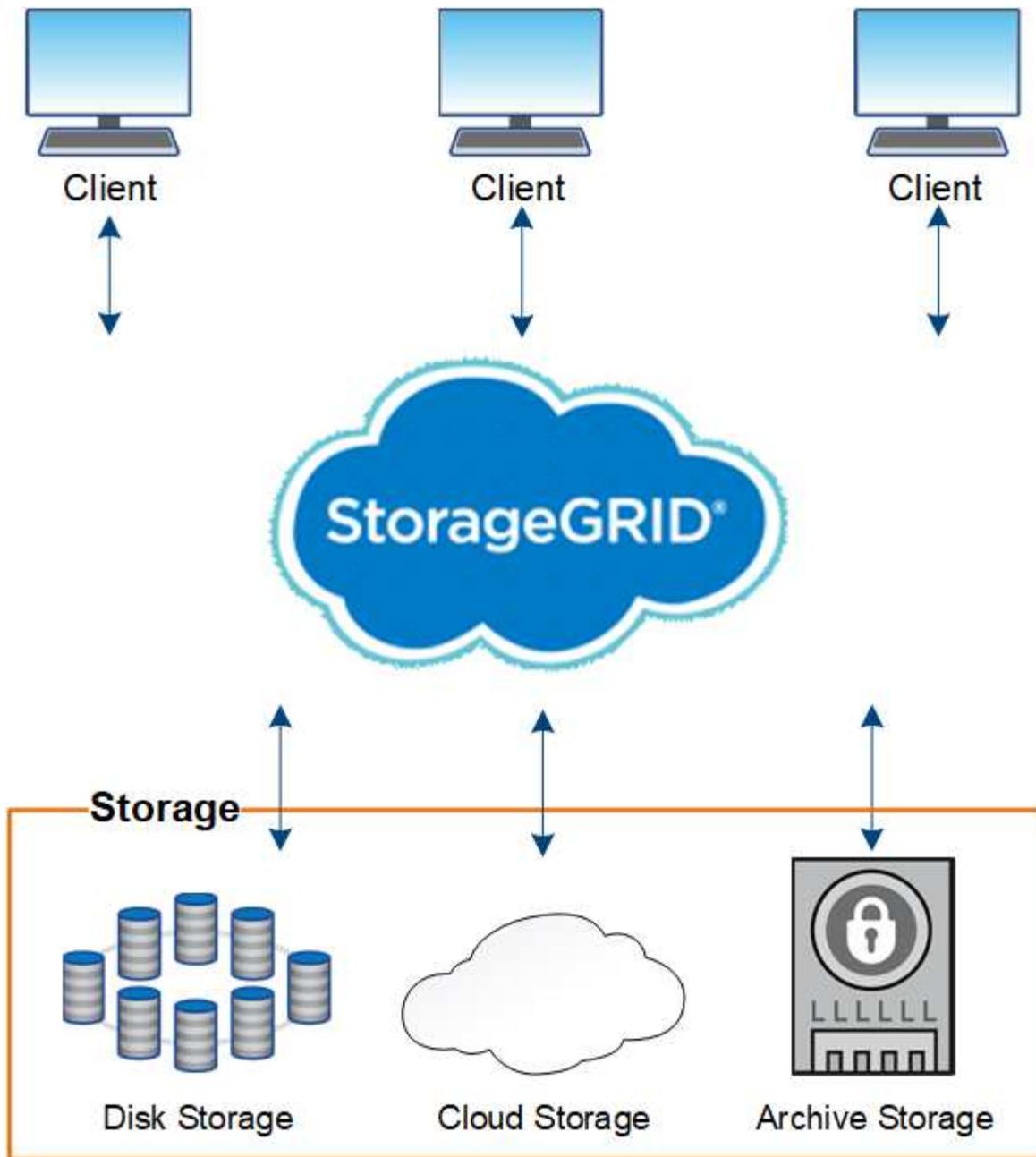
Weitere Informationen zu StorageGRID

Was ist StorageGRID?

NetApp StorageGRID ist eine Suite für softwaredefinierten Objekt-Storage, die eine Vielzahl von Anwendungsfällen in Public-, Private- und Hybrid-Multi-Cloud-Umgebungen unterstützt. StorageGRID bietet nicht nur nativen Support für die Amazon S3-API, sondern auch branchenführende Innovationen wie automatisiertes Lifecycle Management. Damit können Sie unstrukturierte Daten kostengünstig über längere Zeiträume hinweg speichern, sichern, schützen und aufbewahren.

StorageGRID bietet sicheren, langlebigen Storage für unstrukturierte Daten jeder Größenordnung. Die integrierten, metadatengestützten Lifecycle Management-Richtlinien optimieren den Speicherort Ihrer Daten während ihrer gesamten Lebensdauer. Inhalte werden zur richtigen Zeit am richtigen Ort und auf der richtigen Storage-Tier platziert, um Kosten zu senken.

StorageGRID besteht aus geografisch verteilten, redundanten und heterogenen Nodes, die sich in vorhandene Client-Applikationen und Next-Generation-Applikationen integrieren lassen.



Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Vorteile von StorageGRID

Das StorageGRID System bietet unter anderem folgende Vorteile:

- Extrem skalierbar und leicht zu verwendende Daten-Repositories mit geografisch verteilten Standorten für unstrukturierte Daten
- Standard-Objekt-Storage-Protokolle:
 - Amazon Web Services Simple Storage Service (S3)

- OpenStack Swift



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

- Hybrid Cloud-fähig: Richtlinienbasiertes Information Lifecycle Management (ILM) speichert Objekte in Public Clouds, einschließlich Amazon Web Services (AWS) und Microsoft Azure. StorageGRID Plattform-Services ermöglichen die Content-Replizierung, Ereignisbenachrichtigung und Metadatenuche von Objekten, die in Public Clouds gespeichert sind.
- Flexible Datensicherung für Langlebigkeit und Verfügbarkeit Die Daten lassen sich durch Replizierung und ein mehrstufiges Erasure Coding zur Fehlerkorrektur sichern. Überprüfung von Daten im Ruhezustand und auf der Übertragungsstrecke sorgt für Integrität für langfristige Aufbewahrung.
- Dynamisches Lifecycle Management für Daten zum Management der Storage-Kosten Sie können ILM-Regeln erstellen, die den Daten-Lebenszyklus auf Objektebene managen und Datenlokalität, Aufbewahrungszeitraum, Performance, Kosten und Aufbewahrungszeit anpassen.
- Hochverfügbarkeit des Daten-Storage und einiger Managementfunktionen, mit integriertem Lastausgleich zur Optimierung der Datenlast über StorageGRID-Ressourcen hinweg.
- Unterstützung mehrerer Storage-Mandantenkonten, um die auf dem System gespeicherten Objekte durch unterschiedliche Einheiten zu trennen
- Zahlreiche Tools für das Monitoring des Systemzustands des StorageGRID Systems, einschließlich eines umfassenden Alarmsystems, einer grafischen Konsole und detaillierten Status für alle Knoten und Standorte
- Support für Software- oder hardwarebasierte Implementierung Sie können StorageGRID auf einer der folgenden Methoden implementieren:
 - Virtual Machines in VMware ausgeführt.
 - Container-Engines auf Linux Hosts
 - Speziell entwickelte StorageGRID Appliances
 - Storage Appliances bieten Objekt-Storage.
 - Services Appliances stellen Services für die Grid-Administration und den Lastausgleich bereit.
- Erfüllen der relevanten Speicheranforderungen dieser Vorschriften:
 - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), die Börsenmitglieder, Broker oder Händler regelt.
 - Financial Industry Regulatory Authority (FINRA) Rule 4511(c), die die Format- und Medienanforderungen der SEC Rule 17a-4(f) vorgibt.
 - Commodity Futures Trading Commission (CFTC) in der Verordnung 17 CFR § 1.31(c)-(d), die den Handel mit Commodity Futures regelt.
- Unterbrechungsfreie Upgrades und Wartungsvorgänge Zugriff auf Inhalte bleibt während Upgrades, Erweiterungen, Stilllegen und Wartungsarbeiten erhalten.
- Verbundenes Identitätsmanagement. Integration in Active Directory, OpenLDAP oder Oracle Directory Service zur Benutzerauthentifizierung. Unterstützt Single Sign-On (SSO) unter Verwendung 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 richtlinienbasiertes Datenmanagement implementieren, um Objekte in Cloud-Storage-Pools zu speichern. Dabei werden StorageGRID Plattformservices genutzt und Daten per Tiering von ONTAP zu StorageGRID mit NetApp FabricPool verschoben.

Cloud-Storage-Pools

Mit Cloud-Storage-Pools können Sie Objekte außerhalb des StorageGRID Systems speichern. Beispielsweise können Sie selten genutzte Objekte auf kostengünstigeren Cloud-Storage verschieben, wie z. B. Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archiv-Zugriffs-Tier in Microsoft Azure Blob Storage. Oder Sie möchten vielleicht ein Cloud-Backup von StorageGRID Objekten pflegen. Mit dieser können Daten, die aufgrund eines Ausfalls des Storage Volumes oder des Storage-Nodes verloren gingen, wiederhergestellt werden.

Zusätzlich wird Storage von Drittanbietern unterstützt, einschließlich Festplatten- und Tape Storage.



Die Verwendung von Cloud Storage Pools mit FabricPool wird nicht unterstützt, weil die zusätzliche Latenz zum Abrufen eines Objekts aus dem Cloud-Storage-Pool-Ziel hinzugefügt wird.

S3-Plattform-Services

Mit S3-Plattform-Services können Unternehmen Remote-Services als Endpunkte zur Objektreplizierung, für Ereignisbenachrichtigungen oder zur Integration von Suchvorgängen nutzen. Plattform-Services werden unabhängig von den ILM-Regeln des Grid und für einzelne S3-Buckets aktiviert. Folgende Services werden unterstützt:

- Der CloudMirror Replizierungsservice spiegelt angegebene Objekte automatisch auf einen S3-Ziel-Bucket, der sich auf Amazon S3 oder auf einem zweiten StorageGRID System befinden kann.
- Der Ereignisbenachrichtigungsservice sendet Meldungen über bestimmte Aktionen an einen externen Endpunkt, der das Empfangen von Amazon SNS-Ereignissen (Simple Notification Service) unterstützt.
- Der Such-Integrationsservice sendet Objektmetadaten an einen externen Elasticsearch-Service, sodass Metadaten mit Tools von Drittanbietern durchsucht, visualisiert und analysiert werden können.

So können Sie beispielsweise CloudMirror Replizierung verwenden, um spezifische Kundendaten in Amazon S3 zu spiegeln und anschließend AWS Services für Analysen Ihrer Daten nutzen.

ONTAP Daten-Tiering mit FabricPool

Sie können die Kosten von ONTAP Storage reduzieren, indem Sie Daten mithilfe von FabricPool auf StorageGRID verschieben. FabricPool ermöglicht automatisiertes Tiering von Daten auf kostengünstige Objekt-Storage-Tiers, entweder vor Ort oder an anderen Standorten.

Im Gegensatz zu manuellen Tiering-Lösungen senkt FabricPool durch das Automatisieren von Daten-Tiering die Gesamtbetriebskosten, um die Storage-Kosten zu senken. Durch Tiering in Public und Private Clouds einschließlich StorageGRID profitieren Sie von den Vorteilen der Wirtschaftlichkeit der Cloud.

Verwandte Informationen

- ["Was ist Cloud-Storage-Pool?"](#)

- "Was sind Plattform-Services?"
- "Konfigurieren Sie StorageGRID für FabricPool"

StorageGRID Architektur und Netzwerktopologie

Ein StorageGRID System besteht aus mehreren Typen von Grid-Nodes an einem oder mehreren Datacenter-Standorten.

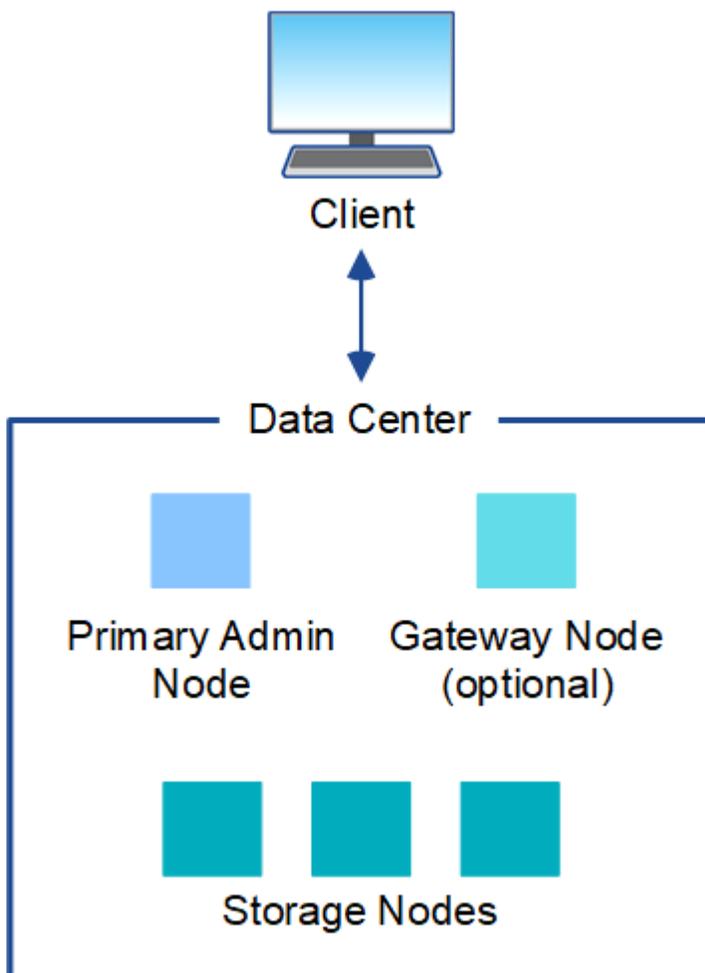
Weitere Informationen zur StorageGRID Netzwerktopologie, -Anforderungen und -Grid-Kommunikation finden Sie im "[Netzwerkrichtlinien](#)".

Implementierungstopologien

Das StorageGRID System kann an einem einzelnen Datacenter-Standort oder an mehreren Datacenter-Standorten implementiert werden.

Ein Standort

Bei einer Implementierung über einen einzigen Standort werden die Infrastruktur und der Betrieb des StorageGRID Systems zentralisiert.

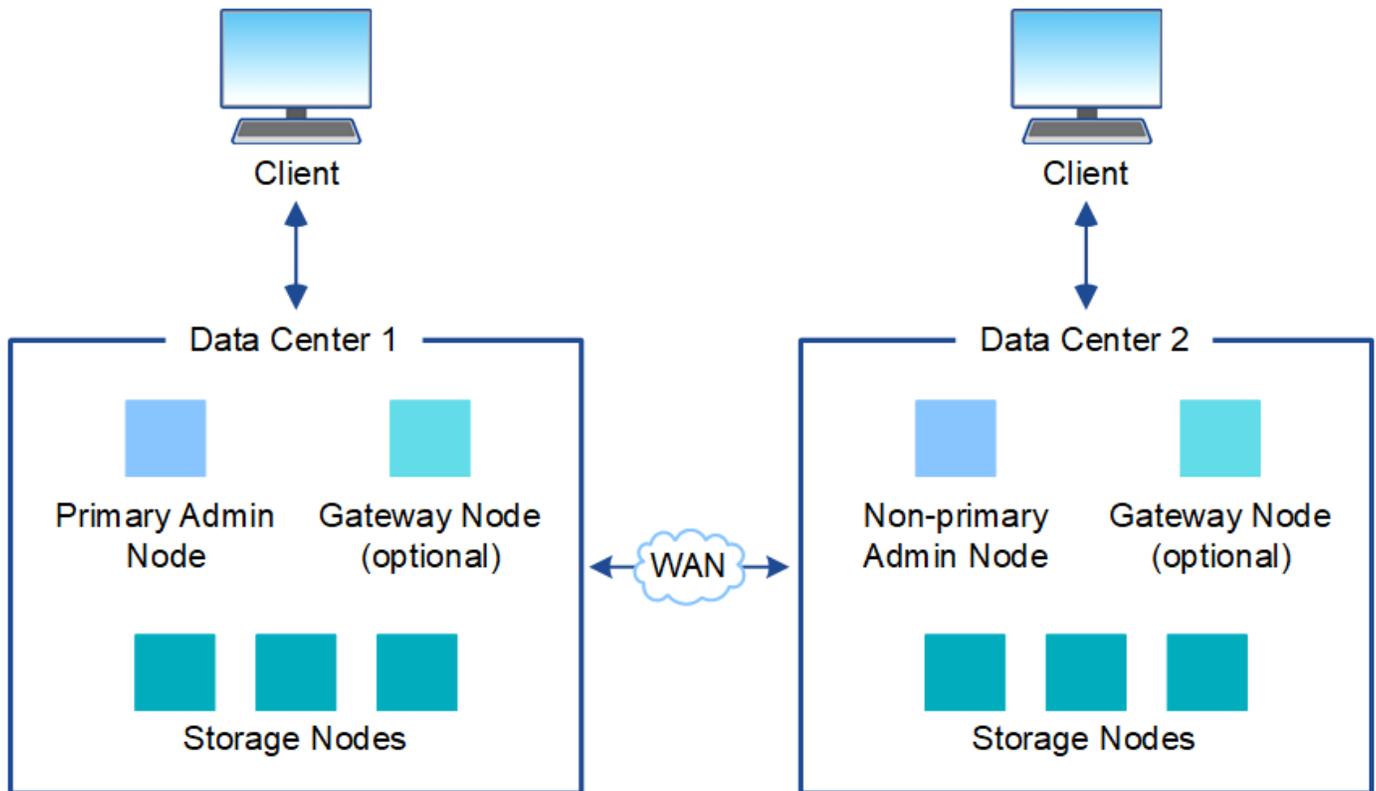


Mehrere Standorte

In einer Implementierung mit mehreren Standorten können an jedem Standort unterschiedliche Typen und eine

unterschiedliche Anzahl von StorageGRID Ressourcen installiert werden. So könnte beispielsweise mehr Storage für ein Datacenter als für ein anderes erforderlich sein.

Unterschiedliche Standorte befinden sich häufig an geografischen Standorten über unterschiedliche Ausfall-Domains, wie z. B. Erdbebenfehlerleitungen oder Überschwemmungsgebiete. Die Daten-Sharing und Disaster Recovery werden durch die automatische Verteilung der Daten an andere Standorte realisiert.



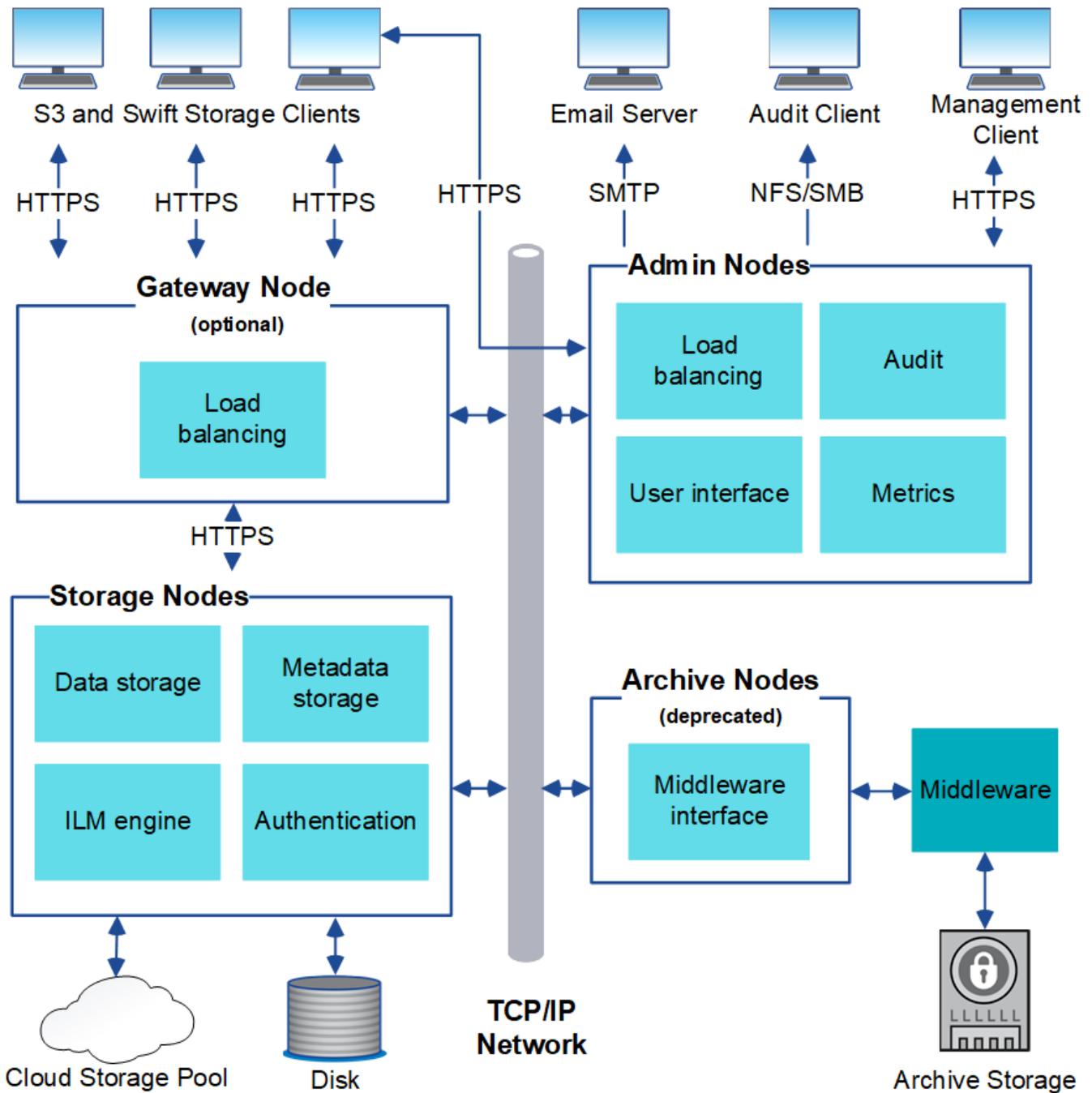
Darüber hinaus können mehrere logische Standorte innerhalb eines einzigen Datacenters eingesetzt werden, um die Verfügbarkeit und Ausfallsicherheit durch verteilte Replizierung und Erasure Coding zu verbessern.

Redundanz des Grid-Nodes

Bei einer Implementierung an einem Standort oder an mehreren Standorten können Sie optional mehrere Admin-Nodes oder Gateway-Nodes enthalten, um Redundanz zu gewährleisten. Sie können beispielsweise mehr als einen Admin-Node an einem einzelnen Standort oder an mehreren Standorten installieren. Allerdings kann jedes StorageGRID System nur einen primären Admin-Node haben.

Systemarchitektur

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



S3- und Swift-Clients speichern und abrufen von Objekten in StorageGRID. Andere Clients werden verwendet, um E-Mail-Benachrichtigungen zu senden, auf die StorageGRID-Managementoberfläche zuzugreifen und optional auf die Audit-Freigabe zuzugreifen.

S3- und Swift-Clients können eine Verbindung zu einem Gateway-Node oder einem Admin-Node herstellen, um die Load-Balancing-Schnittstelle zu Storage-Nodes zu verwenden. Alternativ können S3 und Swift Clients über HTTPS eine direkte Verbindung zu Storage-Nodes herstellen.

Objekte können in StorageGRID auf Software- oder hardwarebasierten Storage-Nodes oder in Cloud-Storage-Pools, die aus externen S3-Buckets oder Azure Blob Storage-Containern bestehen, gespeichert werden.

Grid Nodes und Services

Der grundlegende Baustein eines StorageGRID Systems ist der Grid-Node. Nodes enthalten Services. Dies sind Softwaremodule, die einen Grid-Node mit einem Satz von Funktionen ausstatten.

Das StorageGRID System nutzt vier Typen von Grid-Nodes:

- **Admin Nodes** bieten Managementdienste wie Systemkonfiguration, Überwachung und Protokollierung an. Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Jedes Grid muss über einen primären Admin-Node verfügen und möglicherweise über zusätzliche nicht-primäre Admin-Nodes für Redundanz verfügen. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID-Systems an. Wartungsverfahren müssen jedoch mit dem primären Admin-Node durchgeführt werden.

Admin-Nodes können auch verwendet werden, um den S3- und Swift-Client-Datenverkehr auszugleichen.

- **Storage Nodes** managen und speichern Objektdaten und Metadaten. Jedes StorageGRID System muss mindestens drei Storage-Nodes aufweisen. Wenn Sie über mehrere Standorte verfügen, muss jeder Standort im StorageGRID System auch drei Storage-Nodes aufweisen.
- **Gateway-Knoten (optional)** bieten eine Load-Balancing-Schnittstelle, über die Client-Anwendungen eine Verbindung zu StorageGRID herstellen können. Ein Load Balancer leitet die Clients nahtlos an einen optimalen Storage Node weiter, sodass der Ausfall von Nodes oder sogar einem gesamten Standort transparent ist. Sie können eine Kombination aus Gateway-Knoten und Admin-Knoten zum Lastausgleich verwenden oder einen HTTP-Load-Balancer eines Drittanbieters implementieren.
- **Archive Nodes (veraltet)** bieten eine optionale Schnittstelle, über die Objektdaten auf Band archiviert werden können.

Weitere Informationen finden Sie unter "[StorageGRID verwalten](#)".

Softwarebasierte Nodes

Auf Software-basierte Grid-Nodes lassen sich wie folgt implementieren:

- Als Virtual Machines (VMs) in VMware vSphere
- Innerhalb von Container-Engines auf Linux Hosts Folgende Betriebssysteme werden unterstützt:
 - Red Hat Enterprise Linux
 - CentOS
 - Ubuntu
 - Debian

Weitere Informationen finden Sie im Folgenden:

- "[VMware installieren](#)"
- "[Installieren Sie Red hat Enterprise Linux oder CentOS](#)"
- "[Installieren Sie Ubuntu oder Debian](#)"

Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um eine Liste der unterstützten Versionen zu erhalten.

StorageGRID Appliance-Nodes

StorageGRID Hardware-Appliances wurden speziell für den Einsatz in einem StorageGRID System entwickelt. Einige Geräte können als Storage-Nodes verwendet werden. Andere Appliances können als Admin-Nodes oder Gateway-Nodes verwendet werden. Die Appliance-Nodes können mit softwarebasierten Nodes kombiniert oder vollständig entwickelten Appliance-Grids ohne Abhängigkeiten von externen Hypervisoren, Storage- oder Computing-Hardware implementiert werden.

Folgende StorageGRID Appliances sind verfügbar:

- Die **SGF6112 Storage Appliance** ist ein All-Flash-Server mit 1 Höheneinheit (1 HE) und 12 NVMe-SSD-Laufwerken (Nonvolatile Memory Express) mit integrierten Computing- und Storage-Controllern.
- Die Services-Appliances *SG100 und SG1000 sind 1U-Server (1-Rack-Unit), die jeweils als primärer Admin-Node, nicht primärer Admin-Node oder Gateway-Node betrieben werden können. Beide Appliances können gleichzeitig als Gateway-Nodes und Admin-Nodes (primär und nicht primär) betrieben werden.
- Die **SG6000 Storage Appliance** wird als Storage Node ausgeführt und kombiniert den 1U SG6000-CN Computing Controller mit einem 2U oder 4U Storage Controller Shelf. Die SG6000 ist in zwei Modellen erhältlich:
 - **SGF6024**: Kombiniert den SG6000-CN Computing Controller mit einem 2-HE-Storage Controller Shelf, das 24 Solid State-Laufwerke (SSDs) und redundante Storage Controller umfasst.
 - **SG6060**: Kombiniert den SG6000-CN Computing Controller mit einem 4U-Gehäuse, das 58 NL-SAS-Laufwerke, 2 SSDs und redundante Speicher-Controller umfasst. Jede SG6060 Appliance unterstützt ein oder zwei Erweiterungs-Shelfs mit 60 Laufwerken mit bis zu 178 dedizierten Objektspeichern.
- Die SG5700 Storage Appliance* ist eine integrierte Storage- und Computing-Plattform, die als Storage Node ausgeführt wird. Die SG5700 ist in zwei Modellen erhältlich:
 - **SG5712**: Ein 2U-Gehäuse mit 12 NL-SAS-Laufwerken und integrierten Storage- und Computing-Controllern.
 - **SG5760**: Ein 4-HE-Gehäuse, das 60 NL-SAS-Laufwerke sowie integrierte Storage- und Computing-Controller umfasst.

Weitere Informationen finden Sie im Folgenden:

- ["NetApp Hardware Universe"](#)
- ["SGF6112 Storage Appliance"](#)
- ["SG100- und SG1000-Services-Appliances"](#)
- ["SG6000 Storage-Appliances"](#)
- ["SG5700 Storage-Appliances"](#)

Primäre Dienste für Admin-Nodes

Die folgende Tabelle zeigt die primären Dienste für Admin-Nodes. Diese Tabelle enthält jedoch nicht alle Node-Services.

Service	Tastenfunktion
Audit Management System (AMS)	Verfolgt Systemaktivitäten und -Ereignisse.
Configuration Management Node (CMN)	Verwaltet die systemweite Konfiguration. Nur primärer Admin-Node.

Service	Tastenfunktion
Management-Applikations-Programmierschnittstelle (Management-API)	Verarbeitet Anforderungen aus der Grid-Management-API und der Mandantenmanagement-API.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. Hinweis: dieser Service befindet sich auch auf Gateway Nodes.
Lastausgleich	Sorgt für einen Lastenausgleich des S3- und Swift-Datenverkehrs von Clients zu Storage Nodes. Hinweis: dieser Service befindet sich auch auf Gateway Nodes.
Netzwerk-Management-System (NMS)	Bietet Funktionen für den Grid Manager.
Prometheus	Sammelt und speichert Zeitreihenmetriken von den Services auf allen Knoten.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Primäre Services für Storage-Nodes

Die folgende Tabelle enthält die primären Services für Storage-Nodes. In dieser Tabelle werden jedoch nicht alle Node-Services aufgeführt.



Einige Services, wie z. B. der ADC-Service und der RSM-Service, bestehen in der Regel nur auf drei Storage-Nodes an jedem Standort.

Service	Tastenfunktion
Konto (Konto)	Management von Mandantenkonten.
Administrativer Domänen-Controller (ADC)	Aufrechterhaltung der Topologie und Grid-Konfiguration
Cassandra	Speichert und sichert Objekt-Metadaten.
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch.
Chunk	Verwaltet Erasure-codierte Daten und Paritätsfragmente.
Data Mover (dmv)	Verschiebt Daten in Cloud-Storage-Pools

Service	Tastenfunktion
Verteilter Datenspeicher (DDS)	Überwacht Objekt-Metadaten-Storage
Identität (idnt)	Föderiert Benutzeridentitäten von LDAP und Active Directory
LDR (Local Distribution Router)	Verarbeitet Protokollanfragen von Objekt-Storage und managt Objektdaten auf der Festplatte.
Replicated State Machine (RSM)	Stellt sicher, dass Serviceanfragen der S3-Plattform an ihre jeweiligen Endpunkte gesendet werden.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Primäre Dienste für Gateway-Nodes

In der folgenden Tabelle werden die primären Services für Gateway-Nodes aufgeführt. In dieser Tabelle werden jedoch nicht alle Node-Services aufgeführt.

Service	Tastenfunktion
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. Hinweis: dieser Service befindet sich auch auf Admin Nodes.
Lastausgleich	Bietet Layer-7-Lastausgleich für den S3- und Swift-Datenverkehr von Clients zu Storage-Nodes. Dies ist der empfohlene Lastausgleichmechanismus. Hinweis: dieser Service befindet sich auch auf Admin Nodes.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Primäre Services für Archiv-Nodes

Die folgende Tabelle zeigt die primären Dienste für Archive Nodes (jetzt veraltet). In dieser Tabelle sind jedoch nicht alle Knotendienste aufgeführt.



Die Unterstützung für Archivknoten ist veraltet und wird in einer zukünftigen Version entfernt.

Service	Tastenfunktion
Archiv (ARC)	Kommunikation mit einem externen Tape-Storage-System Tivoli Storage Manager (TSM)

Service	Tastenfunktion
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

StorageGRID Services

Nachfolgend finden Sie eine vollständige Liste der StorageGRID Services.

- **Kontodienst-Spediteur**

Stellt eine Schnittstelle für den Load Balancer-Service bereit, über die der Kontodienst auf Remote-Hosts abgefragt werden kann, und informiert über Änderungen bei der Konfiguration des Load Balancer-Endpunkts am Load Balancer-Service. Der Load Balancer-Service ist auf Admin-Nodes und Gateway-Nodes vorhanden.

- **ADC-Dienst (Administrative Domain Controller)**

Verwaltet Topologiedaten, bietet Authentifizierungsservices und reagiert auf Anfragen aus den LDR- und CMN-Diensten. Der ADC-Service ist auf jedem der ersten drei Speicherknoten vorhanden, die an einem Standort installiert sind.

- **AMS Service (Audit Management System)**

Überwacht und protokolliert alle geprüften Systemereignisse und Transaktionen in einer Textdatei. Der AMS-Dienst ist auf Admin-Knoten vorhanden.

- **ARC-Service (Archiv)**

Das Tool bietet die Managementoberfläche, mit der Sie Verbindungen zu externem Archiv-Storage konfigurieren, z. B. zur Cloud über eine S3-Schnittstelle oder per Tape über TSM Middleware. Der ARC-Dienst ist auf Archiv-Knoten vorhanden.

- **Cassandra Reaper Service**

Führt automatische Reparaturen von Objektmetadaten durch. Der Cassandra Reaper Service ist auf allen Speicherknoten vorhanden.

- **Chunk Service**

Verwaltet Erasure-codierte Daten und Paritätsfragmente. Der Chunk Service ist auf Storage Nodes vorhanden.

- **CMN-Service (Configuration Management Node)**

Management systemweiter Konfigurationen und Grid-Aufgaben Jedes Grid hat einen CMN-Service, der auf dem primären Admin-Node vorhanden ist.

- **DDS Service (Distributed Data Store)**

Schnittstellen zur Cassandra-Datenbank zum Management von Objektmetadaten Der DDS-Service ist auf Speicherknoten vorhanden.

- **DMV-Service (Data Mover)**

Verschiebt Daten in Cloud-Endpunkte Der DMV-Dienst ist auf Speicherknoten vorhanden.

- **Dynamic IP Service**

Überwacht das Raster auf dynamische IP-Änderungen und aktualisiert lokale Konfigurationen. Der dynamische IP-Dienst (dynip) ist auf allen Knoten vorhanden.

- **Grafana Service**

Wird für die Darstellung von Kennzahlen im Grid Manager verwendet. Der Grafana-Service ist auf Admin-Nodes vorhanden.

- **Hochverfügbarkeits-Service**

Verwaltet hochverfügbare virtuelle IPs auf Knoten, die auf der Seite „Hochverfügbarkeitsgruppen“ konfiguriert sind. Der Dienst Hochverfügbarkeit ist auf Admin-Nodes und Gateway-Knoten vorhanden. Dieser Service wird auch als „Keepalived Service“ bezeichnet.

- * Identitätsdienst (nicht verfügbar)*

Föderiert Benutzeridentitäten von LDAP und Active Directory Der Identitäts-Service (idnt) ist auf drei Storage-Nodes an jedem Standort vorhanden.

- **Lambda Schiedsrichter Service**

Verwalten von S3 Select SelectObjectContent Requests.

- **Load Balancer Service**

Sorgt für einen Lastenausgleich des S3- und Swift-Datenverkehrs von Clients zu Storage Nodes. Der Lastverteilungsservice kann über die Konfigurationsseite Load Balancer Endpoints konfiguriert werden. Der Load Balancer-Service ist auf Admin-Nodes und Gateway-Nodes vorhanden. Dieser Service wird auch als nginx-gw-Service bezeichnet.

- **LDR-Service (Local Distribution Router)**

Verwaltet die Speicherung und Übertragung von Inhalten innerhalb des Grids. Der LDR-Service ist auf den Speicherknoten vorhanden.

- **MISCd Information Service Control Daemon Service**

Stellt eine Schnittstelle zum Abfragen und Managen von Services auf anderen Nodes sowie zum Managen von Umgebungskonfigurationen auf dem Node bereit, beispielsweise zum Abfragen des Status von Services, die auf anderen Nodes ausgeführt werden. Der MISCd-Dienst ist auf allen Knoten vorhanden.

- **Nginx Service**

Fungiert als Authentifizierungs- und sicherer Kommunikationsmechanismus für verschiedene Grid Services (wie Prometheus und Dynamic IP), der die Möglichkeit zur Kommunikation mit Services auf anderen Knoten über HTTPS-APIs ermöglicht. Der nginx-Service ist auf allen Knoten vorhanden.

- **Nginx-gw Service**

Schaltet den Lastverteilungsservice ein. Der nginx-gw-Dienst ist auf Admin-Knoten und Gateway-Knoten vorhanden.

- **NMS Service (Network Management System)**

Gibt die Überwachungs-, Berichterstellungs- und Konfigurationsoptionen an, die über den Grid Manager angezeigt werden. Der NMS-Service ist auf Admin Nodes vorhanden.

- **Persistenzdienst**

Verwaltet Dateien auf dem Root-Laufwerk, die über einen Neustart bestehen müssen. Der Persistenzdienst ist auf allen Nodes vorhanden.

- **Prometheus Service**

Erfasst Zeitreihungskennzahlen von Services auf allen Knoten. Der Prometheus-Service ist auf Admin-Knoten vorhanden.

- **RSM-Dienst (Replicated State Machine Service)**

Stellt sicher, dass Plattformserviceanforderungen an die jeweiligen Endpunkte gesendet werden. Der RSM-Dienst ist auf Speicherknoten vorhanden, die den ADC-Dienst verwenden.

- **SSM-Dienst (Server Status Monitor)**

Überwacht Hardwarebedingungen und Berichte an den NMS-Service. Auf jedem Grid-Knoten ist eine Instanz des SSM-Dienstes vorhanden.

- **Trace Collector Service**

Führt eine Trace-Erfassung durch, um Informationen für den technischen Support zu sammeln. Der Trace Collector Dienst verwendet die Open Source Jaeger Software und ist auf Admin Nodes vorhanden.

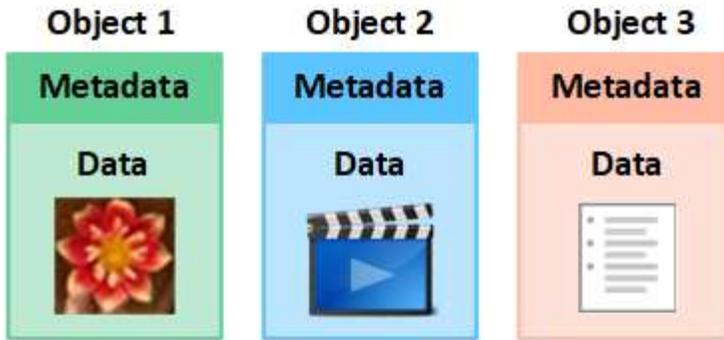
Managen von Daten mit StorageGRID

Was ist ein Objekt

Bei Objekt-Storage ist die Storage-Einheit ein Objekt und nicht eine Datei oder ein Block. Im Gegensatz zur Baumstruktur eines File-Systems oder Block-Storage werden die Daten im Objekt-Storage in einem flachen, unstrukturierten Layout organisiert.

Objekt-Storage entkoppelt den physischen Standort der Daten von der Methode zum Speichern und Abrufen dieser Daten.

Jedes Objekt in einem objektbasierten Storage-System besteht aus zwei Teilen: Objekt-Daten und Objekt-Metadaten.



Was sind Objektdaten?

Objektdaten können alles sein, z. B. ein Foto, ein Film oder eine medizinische Aufzeichnung.

Was sind Objekt-Metadaten?

Objektmetadaten sind alle Informationen, die ein Objekt beschreiben. StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im Grid zu verfolgen und den Lebenszyklus eines jeden Objekts mit der Zeit zu managen.

Objektmetadaten enthalten Informationen wie die folgenden:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), dem Objektnamen, dem Namen des S3-Buckets oder Swift-Containers, dem Mandanten-Kontonamen oder -ID, der logischen Größe des Objekts, dem Datum und der Uhrzeit der ersten Erstellung des Objekts und Datum und Uhrzeit der letzten Änderung des Objekts.
- Der aktuelle Speicherort der einzelnen Objektkopien oder Fragmente, deren Löschen codiert wurde
- Alle dem Objekt zugeordneten Benutzer-Metadaten.

Objektmetadaten sind individuell anpassbar und erweiterbar und bieten dadurch Flexibilität für die Nutzung von Applikationen.

Detaillierte Informationen zum StorageGRID Speichern von Objektmetadaten und -Speicherort finden Sie unter ["Management von Objekt-Metadaten-Storage"](#).

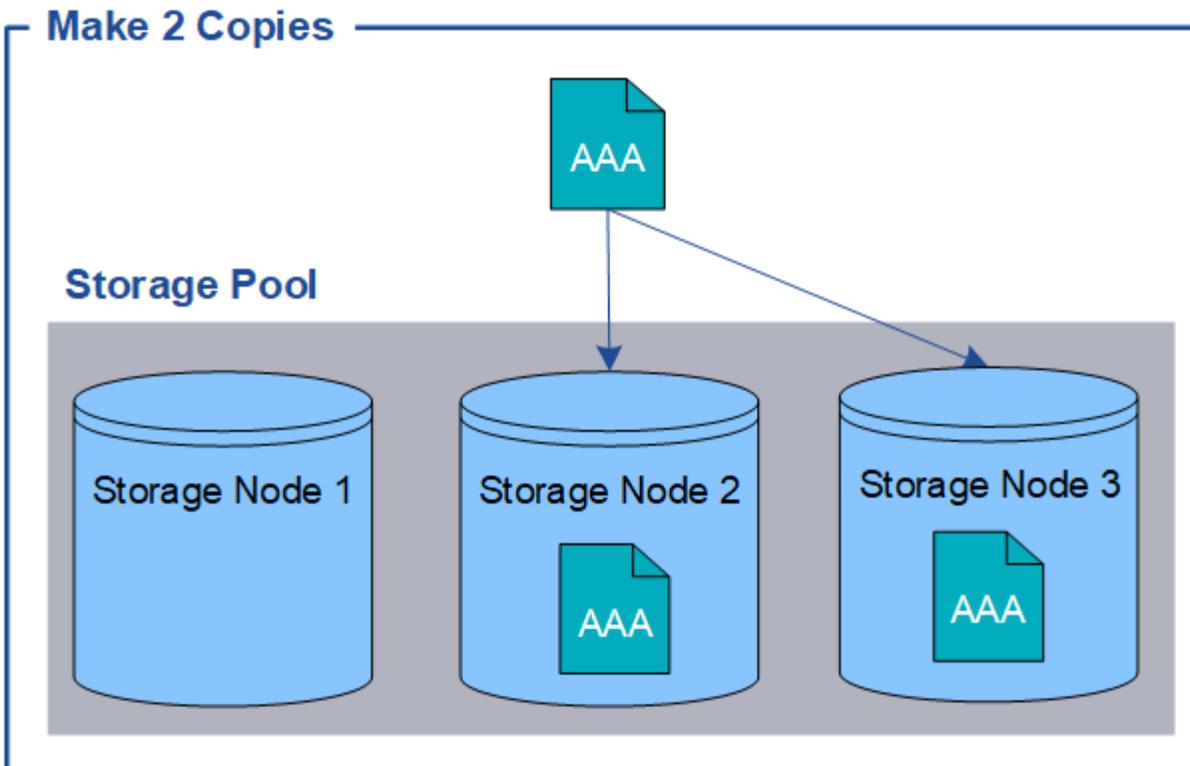
Wie werden Objektdaten gesichert?

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

Replizierung

Wenn StorageGRID Objekte mit einer ILM-Regel (Information Lifecycle Management) übereinstimmt, die für die Erstellung replizierter Kopien konfiguriert ist, erstellt das System exakte Kopien von Objektdaten und speichert sie in Storage-Nodes, Archivierungs-Nodes oder Cloud-Storage-Pools. ILM-Regeln bestimmen die Anzahl der Kopien, die erstellt werden, wo diese Kopien gespeichert werden und wie lange sie vom System aufbewahrt werden. Falls eine Kopie verloren geht, beispielsweise aufgrund des Verlusts eines Storage-Nodes, ist das Objekt nach wie vor verfügbar, wenn eine Kopie davon an einer anderen Stelle im StorageGRID System vorhanden ist.

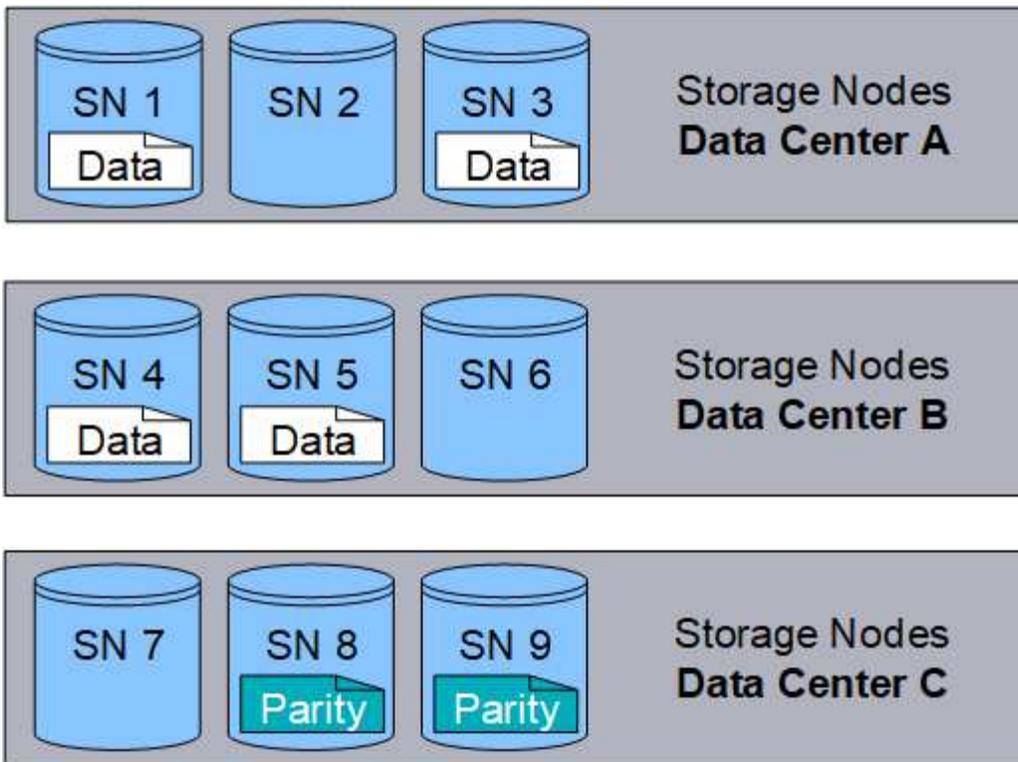
Im folgenden Beispiel gibt die Regel „2 Kopien erstellen“ an, dass zwei replizierte Kopien jedes Objekts in einem Speicherpool platziert werden, der drei Storage-Nodes enthält.



Erasure Coding

Wenn StorageGRID Objekte mit einer ILM-Regel übereinstimmt, die zur Erstellung von mit Datenkonsistenz versehenen Kopien konfiguriert ist, werden Objektdaten in Datenfragmente zerlegt, zusätzliche Paritätsfragmente berechnet und jedes Fragment auf einem anderen Storage Node gespeichert. Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Daten oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zum Erasure Coding diese Fragmente mit einer Teilmenge der verbleibenden Daten und Paritätsfragmente neu erstellen. ILM-Regeln und Erasure Coding-Profil bestimmen das verwendete Verfahren zum Erasure Coding-Verfahren.

Das folgende Beispiel zeigt den Einsatz von Erasure Coding für Objektdaten. In diesem Beispiel verwendet die ILM-Regel ein Codierungsschema für das Löschen von 4+2. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente ist in drei Datacentern auf einem anderen Storage Node gespeichert, um bei Node-Ausfällen oder Standortausfällen ihre Daten zu sichern.



Verwandte Informationen

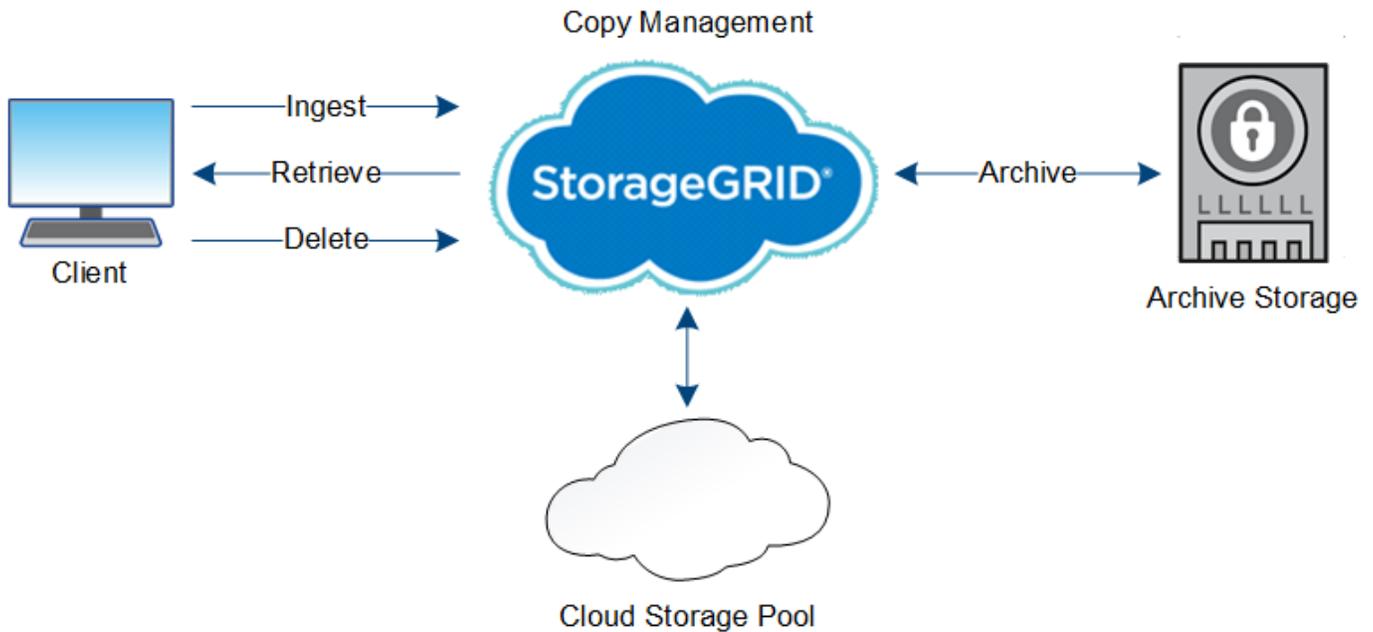
- ["Objektmanagement mit ILM"](#)
- ["Verwenden Sie das Information Lifecycle Management"](#)

Das Leben eines Objekts

Das Leben eines Objekts besteht aus verschiedenen Etappen. Jede Phase stellt die Vorgänge dar, die mit dem Objekt auftreten.

Der Lebenszyklus eines Objekts umfasst das Aufnehmen, das Kopieren-Management, das Abrufen und Löschen von Objekten.

- **Ingest:** Der Prozess einer S3- oder Swift-Client-Anwendung, bei der ein Objekt über HTTP auf das StorageGRID-System gespeichert wird. In dieser Phase beginnt das StorageGRID-System mit der Verwaltung des Objekts.
- **Kopierverwaltung:** Der Prozess des Managements replizierter und mit Erasure Coding codierter Kopien in StorageGRID, wie in den ILM-Regeln der aktiven ILM-Richtlinie beschrieben. Während der Kopiemanagementphase schützt StorageGRID Objektdaten vor Verlust. Dazu wird die angegebene Anzahl und der angegebene Typ von Objektkopien auf Storage-Nodes, in einem Cloud-Storage-Pool oder auf Archiv-Node erstellt und beibehalten.
- **Retrieve:** Der Prozess einer Client-Anwendung, die auf ein vom StorageGRID-System gespeichertes Objekt zugreift. Der Client liest das Objekt, das von einem Storage-Node, Cloud-Storage-Pool oder Archive Node abgerufen wird.
- **Löschen:** Der Vorgang, bei dem alle Objektkopien aus dem Raster entfernt werden. Objekte können entweder gelöscht werden, wenn eine Client-Applikation eine Löschanfrage an das StorageGRID System sendet, oder infolge eines automatischen Prozesses, der StorageGRID nach Ablauf der Nutzungsdauer des Objekts durchführt.



Verwandte Informationen

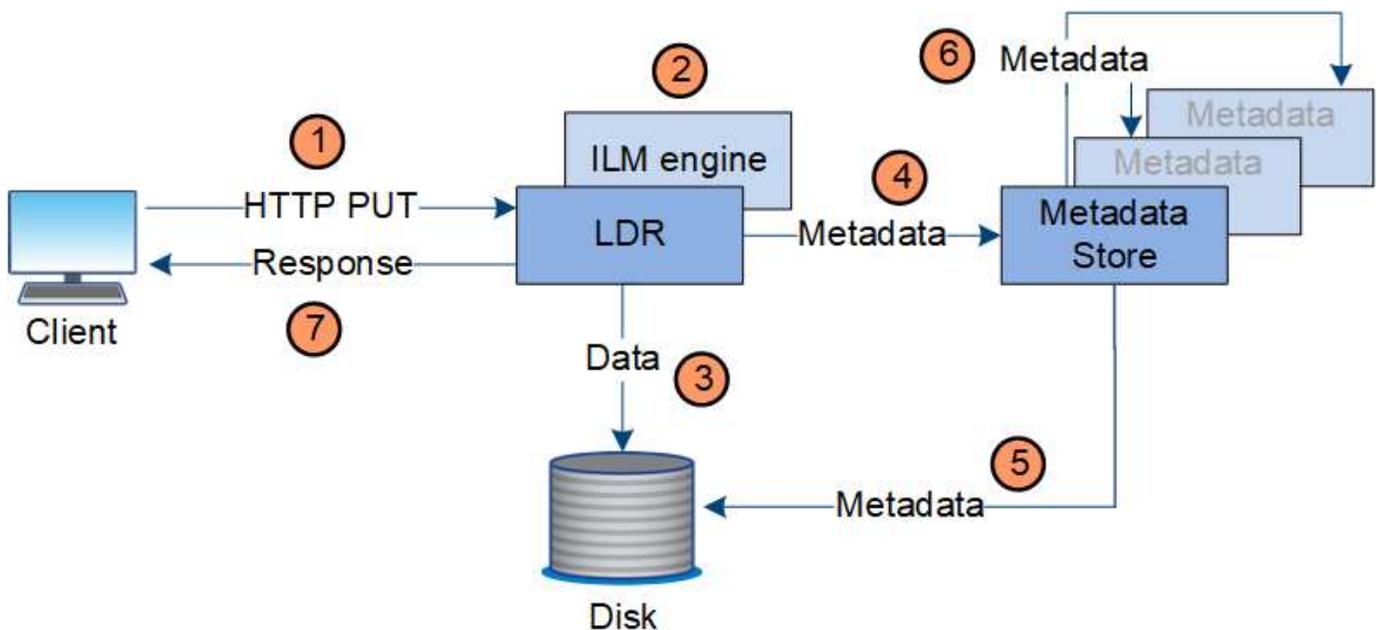
- ["Objektmanagement mit ILM"](#)
- ["Verwenden Sie das Information Lifecycle Management"](#)

Datenfluss aufnehmen

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-Service auf Storage-Nodes die Anforderung und speichert die Metadaten und Daten auf der Festplatte.



1. Die Client-Applikation erstellt das Objekt und sendet es über eine HTTP PUT-Anforderung an das StorageGRID System.
2. Das Objekt wird anhand der ILM-Richtlinie des Systems bewertet.
3. Der LDR-Service speichert die Objektdaten als replizierte Kopie oder als Kopie mit dem Erasure Coding. (Das Diagramm zeigt eine vereinfachte Version zum Speichern einer replizierten Kopie auf Festplatte.)
4. Der LDR-Service sendet die Objektmetadaten an den Metadatenpeicher.
5. Der Metadaten-Speicher speichert die Objekt-Metadaten auf der Festplatte.
6. Der Metadatenpeicher überträgt Kopien von Objektmetadaten an andere Storage-Nodes. 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.

Verwaltung von Kopien

Objektdaten werden von der aktiven ILM-Richtlinie und ihren ILM-Regeln gemanagt. ILM-Regeln erstellen replizierte oder Erasure-codierte Kopien, um Objektdaten vor Verlust zu schützen.

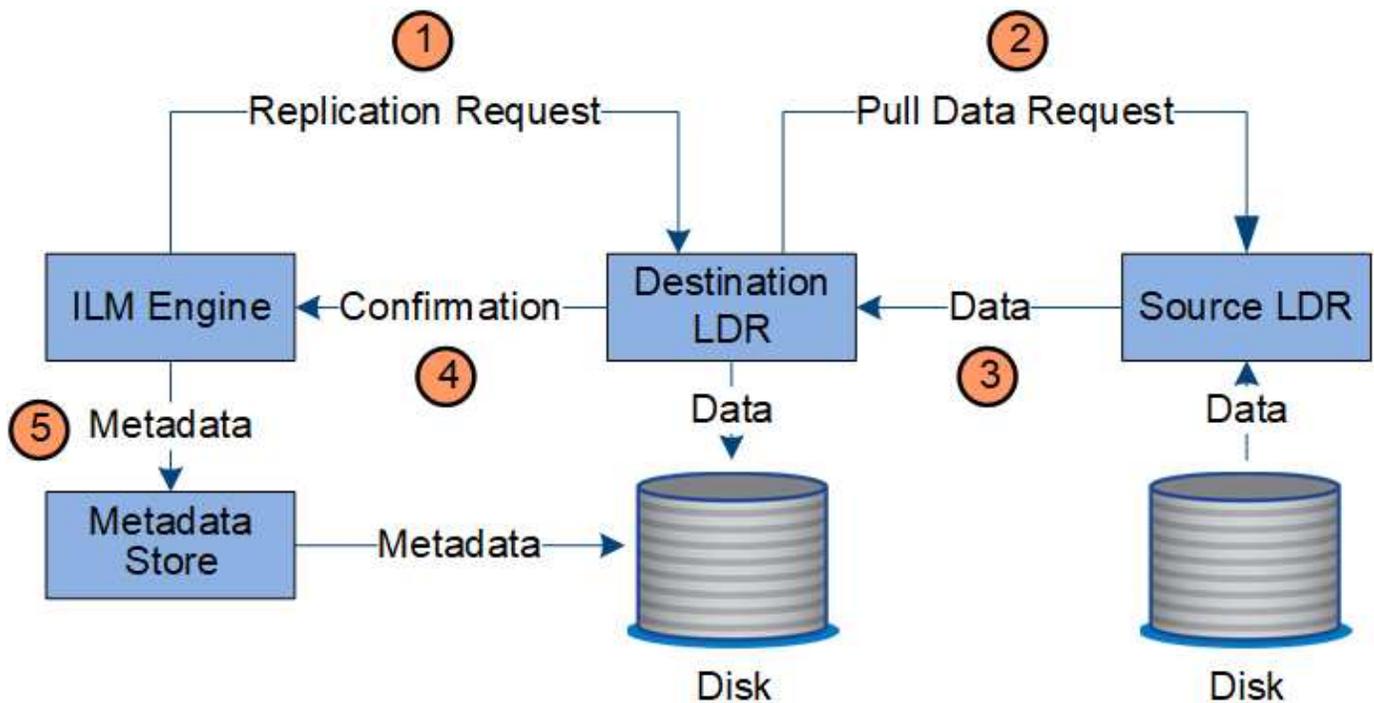
Unterschiedliche Typen und Standorte von Objektkopien können zu unterschiedlichen Zeiten der Lebensdauer des Objekts erforderlich sein. ILM-Regeln werden regelmäßig überprüft, um sicherzustellen, dass Objekte nach Bedarf platziert werden.

Objektdaten werden vom LDR-Service gemanagt.

Content-Schutz: Replikation

Wenn für die Anweisungen zur Content-Platzierung einer ILM-Regel replizierte Kopien von Objektdaten erforderlich sind, werden von den Storage-Nodes, die den konfigurierten Storage-Pool bilden, Kopien auf Festplatte erstellt und gespeichert.

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

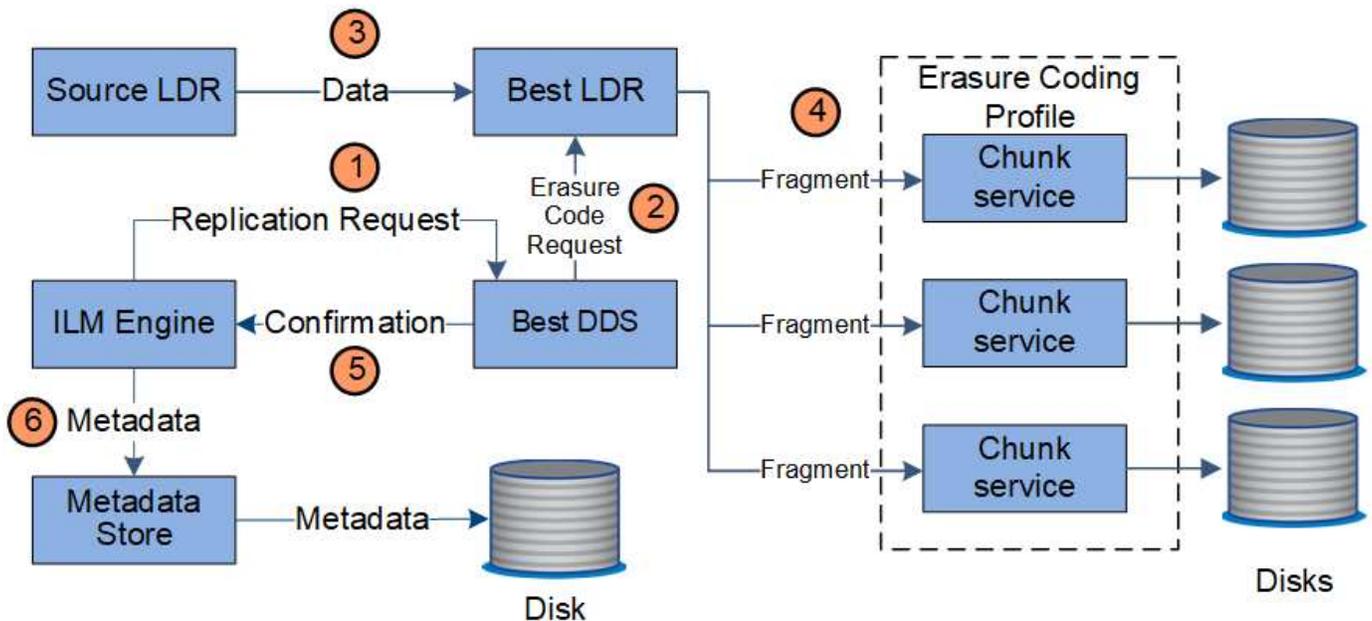


1. Die ILM-Engine fragt den ADC-Service ab, um den besten Ziel-LDR-Service innerhalb des durch die ILM-Regel festgelegten Storage-Pools zu ermitteln. Er sendet dann diesen LDR-Service einen Befehl, um die Replikation zu initiieren.
2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellspeicherort ab. Anschließend sendet er eine Replikationsanfrage an den Quell-LDR-Service.
3. Der Quell-LDR-Service sendet eine Kopie an den Ziel-LDR-Service.
4. Der Ziel-LDR-Service benachrichtigt die ILM Engine, dass die Objektdaten gespeichert wurden.
5. Die ILM-Engine aktualisiert den Metadatenpeicher mit Objektspeichermetadaten.

Content Protection: Erasure Coding

Wenn eine ILM-Regel Anweisungen zur Erstellung von Kopien von Objektdaten enthält, die nach Erasure Coding codiert wurden, werden Objektdaten in Daten- und Paritätsfragmente unterteilt und diese Fragmente über die Storage Nodes verteilt, die im Profil für Erasure Coding konfiguriert sind.

Die ILM-Engine, eine Komponente des LDR-Service, steuert das Erasure Coding und stellt sicher, dass das Erasure Coding-Profil auf Objektdaten angewendet wird.

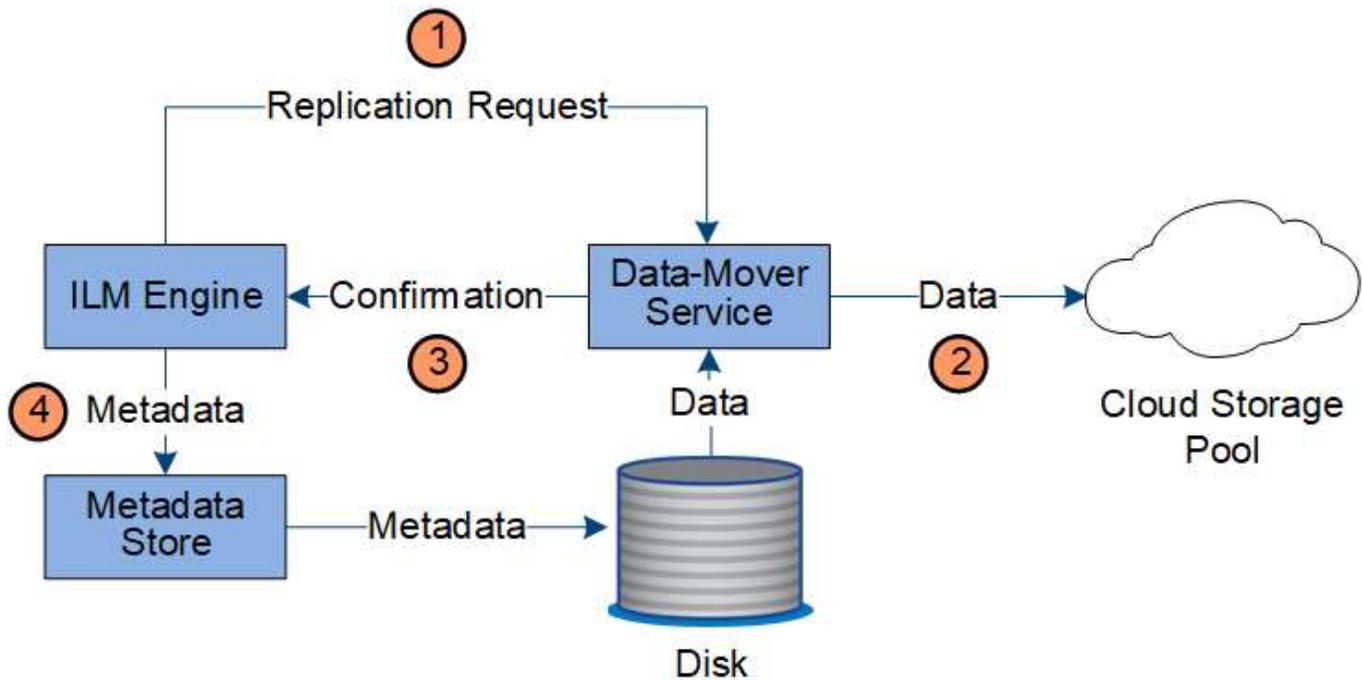


1. Die ILM-Engine fragt den ADC-Service ab, um zu bestimmen, welcher DDS-Service den Erasure Coding-Vorgang am besten ausführen kann. Sobald die ILM-Engine ermittelt wurde, sendet sie eine „Initiierung“-Anforderung an den Service.
2. Der DDS-Dienst weist ein LDR an, den Code der Objektdaten zu löschen.
3. Der Quell-LDR-Service sendet eine Kopie an den für das Erasure Coding ausgewählten LDR-Service.
4. Sobald der LDR-Service in die entsprechende Anzahl von Parität und Datenfragmenten unterteilt ist, verteilt er diese Fragmente über die Storage Nodes (Chunk-Services), aus denen der Storage-Pool des Erasure Coding-Profiles besteht.
5. Der LDR-Service benachrichtigt die ILM-Engine und bestätigt, dass Objektdaten erfolgreich verteilt werden.
6. Die ILM-Engine aktualisiert den Metadatenpeicher mit Objektspeichermetadaten.

Content-Sicherung: Cloud Storage Pool

Wenn für die Anweisungen zur Content-Platzierung einer ILM-Regel eine replizierte Kopie von Objektdaten in einem Cloud Storage-Pool gespeichert wird, werden Objektdaten in den externen S3-Bucket oder Azure Blob-Storage-Container dupliziert, der für den Cloud Storage-Pool angegeben wurde.

Die ILM-Engine, die eine Komponente des LDR-Service ist, und der Data Mover-Service steuern die Verschiebung von Objekten in den Cloud-Speicherpool.



1. Die ILM-Engine wählt einen Data Mover-Service zur Replizierung in den Cloud-Storage-Pool aus.
2. Der Data Mover-Service sendet die Objektdaten an den Cloud-Speicherpool.
3. Der Data Mover-Service benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.
4. Die ILM-Engine aktualisiert den Metadatenpeicher mit Objektspeichermetadaten.

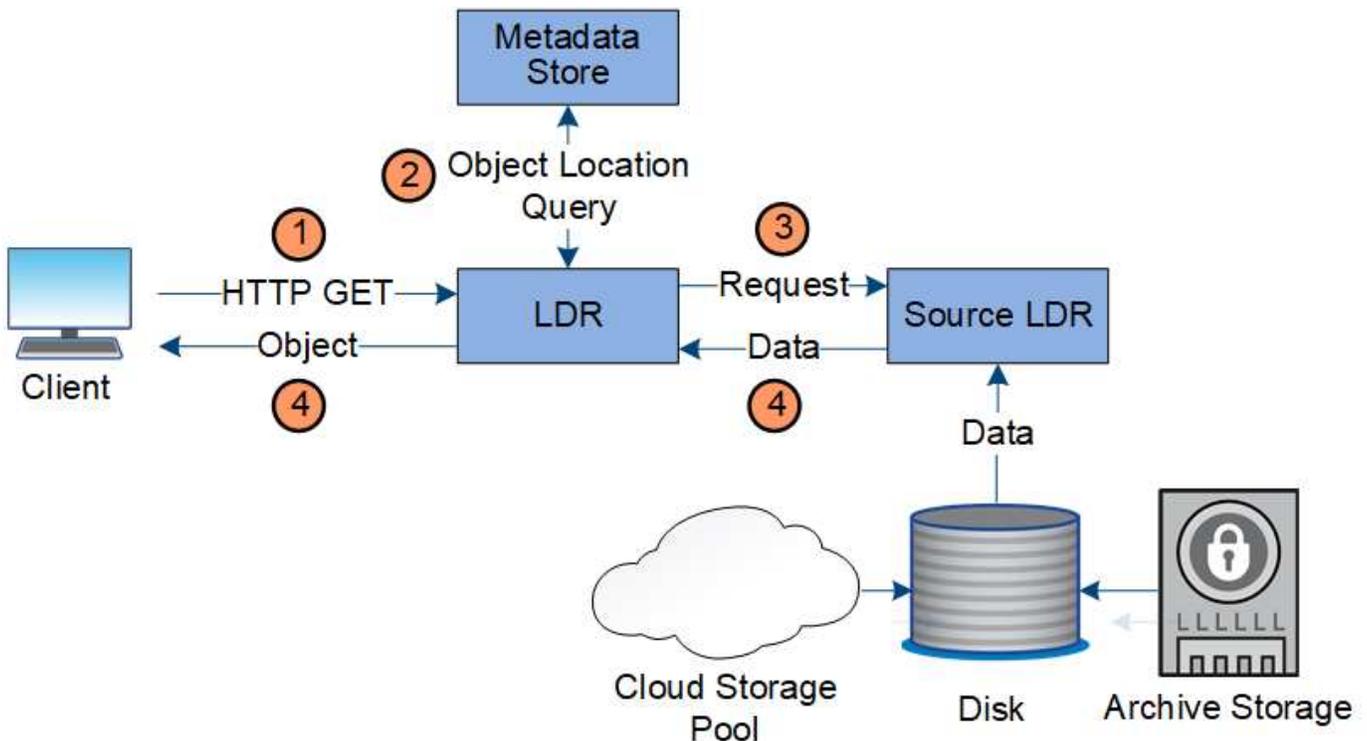
Abrufen des Datenflusses

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 Storage-Node oder ggf. einem Cloud-Storage-Pool oder Archiv-Node zu verfolgen.

Der LDR-Service des Storage Node fragt den Metadatenpeicher nach dem Speicherort der Objektdaten ab und ruft ihn vom Quell-LDR-Service ab. Bevorzugt wird der Abruf von einem Storage Node durchgeführt. Wenn das Objekt auf einem Speicherknoten nicht verfügbar ist, wird die Abfrage an einen Cloud-Speicherpool oder einen Archiv-Node geleitet.



Wenn sich die einzige Objektkopie auf AWS Glacier Storage oder in der Azure Archiveebene befindet, muss die Client-Applikation eine Anfrage zur Wiederherstellung NACH S3-Objekten stellen, um eine abrufbare Kopie in dem Cloud Storage Pool wiederherzustellen.



1. Der LDR-Service erhält eine Abrufanforderung von der Client-Anwendung.
2. Der LDR-Service fragt den Metadatenpeicher nach dem Objektdatenstandort und den Metadaten ab.
3. Der LDR-Service leitet die Abfrage an den Quell-LDR-Service weiter.
4. Der Quell-LDR-Dienst gibt die Objektdaten aus dem abgefragten LDR-Dienst zurück und das System gibt das Objekt an die Client-Anwendung zurück.

Löschen des Datenflusses

Alle Objektkopien werden aus dem StorageGRID System entfernt, wenn ein Client einen Löschvorgang durchführt oder die Lebensdauer des Objekts abgelaufen ist. Dies wird automatisch entfernt. Es gibt einen definierten Datenfluss zum Löschen von Objekten.

Löschhierarchie

StorageGRID bietet verschiedene Methoden zur Steuerung der Aufbewahrung oder Löschung von Objekten. Objekte können nach Client-Anforderung oder automatisch gelöscht werden. StorageGRID priorisiert alle S3 Object Lock-Einstellungen bei Löschanfragen von Clients, die nach ihrer Wichtigkeit über den S3-Bucket-Lebenszyklus und die Anweisungen zur ILM-Platzierung priorisiert werden.

- **S3 Object Lock:** Wenn die globale S3 Object Lock-Einstellung für das Grid aktiviert ist, können S3-Clients Buckets mit aktivierter S3-Objektsperre erstellen und dann über die S3-REST-API Aufbewahrungseinstellungen für jede Objektversion festlegen, die diesem Bucket hinzugefügt wurde.
 - Eine Objektversion, die sich unter einem Legal Hold befindet, kann mit keiner Methode gelöscht werden.
 - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version nicht mit einer Methode gelöscht werden.
 - Objekte in Buckets, für die S3 Objektsperre aktiviert ist, werden durch ILM „Forever“ beibehalten. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-

Anfrage oder den Ablauf des Bucket-Lebenszyklus gelöscht werden.

- Wenn S3-Clients ein Standarddatum für die Aufbewahrung bis auf den Bucket anwenden, müssen sie für jedes Objekt kein „bis zur Aufbewahrung“ angeben.
- **Client delete Request:** Ein S3- oder Swift-Client kann eine delete-Objekt-Anfrage stellen. Wenn ein Client ein Objekt löscht, werden alle Kopien des Objekts aus dem StorageGRID System entfernt.
- **Objekte in 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 eine Lebenszykluskonfiguration zu ihren Buckets hinzufügen, die eine Ablaufaktion angibt. Wenn ein Bucket-Lebenszyklus vorhanden ist, löscht StorageGRID automatisch alle Kopien eines Objekts, wenn das in der Aktion „Ablaufdatum“ angegebene Datum oder die Anzahl der Tage erfüllt werden, es sei denn, der Client löscht das Objekt zuerst.
- **ILM-Platzierungsanweisungen:** Vorausgesetzt, dass für den Bucket keine S3-Objektsperre aktiviert ist und es keinen Bucket-Lebenszyklus gibt, löscht StorageGRID automatisch ein Objekt, wenn der letzte Zeitraum der ILM-Regel endet und es keine weiteren Platzierungen für das Objekt gibt.

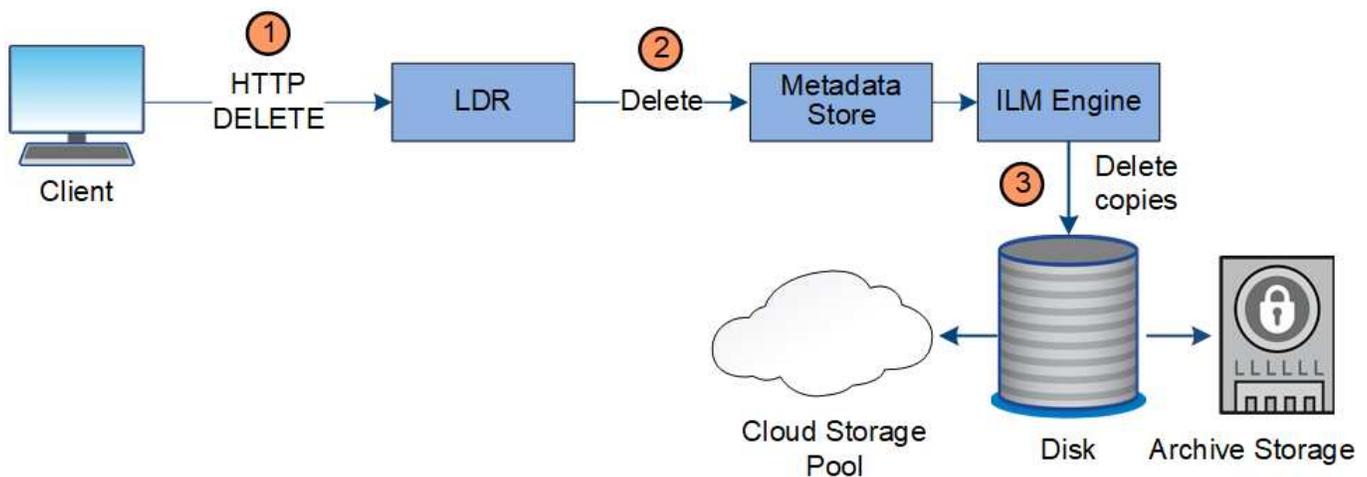


Die Aktion „Ablaufdatum“ in einem S3-Bucket-Lebenszyklus überschreibt immer die ILM-Einstellungen. Aus diesem Grund kann ein Objekt auch dann im Grid verbleiben, wenn ILM-Anweisungen zum Auflagen des Objekts verfallen sind.

Löschen von S3-Löschmarkierungen

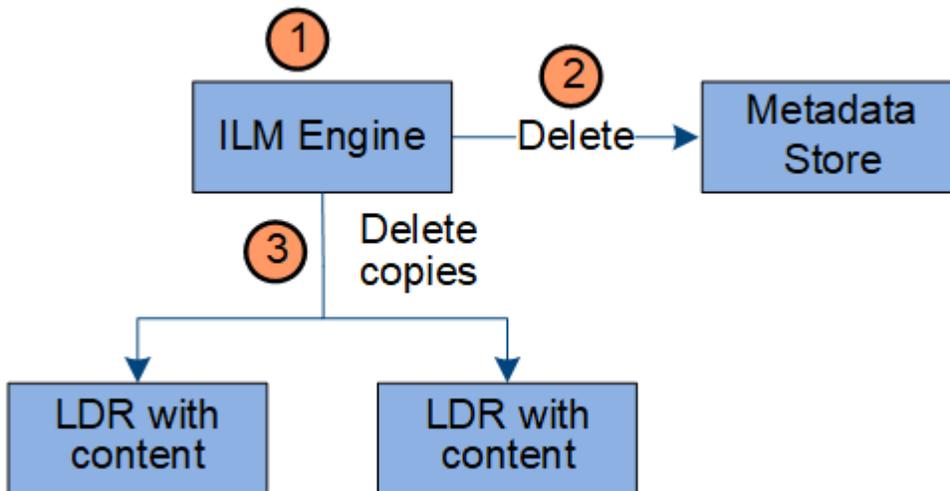
Wenn ein versioniertes Objekt gelöscht wird, erstellt StorageGRID als aktuelle Version des Objekts eine Löschmarkierung. Um die Null-Byte-Löschmarkierung aus dem Bucket zu entfernen, muss der S3-Client die Objektversion explizit löschen. Löschmarkierungen werden nicht durch ILM, Bucket-Lebenszyklusregeln oder Objekte in Bucket-Operationen gelöscht.

Datenfluss für Clientlöschungen



1. Der LDR-Dienst erhält eine Löschanforderung von der Client-Anwendung.
2. Der LDR-Service aktualisiert den Metadatenpeicher, sodass das Objekt auf die Client-Anforderungen gelöscht wird, und weist die ILM-Engine an, alle Kopien von Objektdaten zu entfernen.
3. Das Objekt wurde aus dem System entfernt. Der Metadatenpeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Datenfluss für ILM-Löschungen



1. Die ILM-Engine legt fest, dass das Objekt gelöscht werden muss.
2. Die ILM-Engine benachrichtigt den Metadatenpeicher. Der Metadatenpeicher aktualisiert Objektmetadaten, sodass das Objekt auf Client-Anforderungen gelöscht aussieht.
3. Die ILM-Engine entfernt alle Kopien des Objekts. Der Metadatenpeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Verwenden Sie das Information Lifecycle Management

Mithilfe von Information Lifecycle Management (ILM) können Sie die Platzierung, Dauer und das Aufnahmeverhalten für alle Objekte im StorageGRID System steuern. ILM-Regeln legen fest, wie StorageGRID Objekte im Laufe der Zeit speichert. Sie konfigurieren eine oder mehrere ILM-Regeln und fügen sie anschließend zu einer ILM-Richtlinie hinzu.

Ein Raster verfügt jeweils nur über eine aktive Richtlinie. Eine Richtlinie kann mehrere Regeln enthalten.

ILM-Regeln definieren:

- Welche Objekte sollten gespeichert werden. Eine Regel kann auf alle Objekte angewendet werden, oder Sie können Filter angeben, um zu identifizieren, 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 verbunden sind.
- Speichertyp und -Standort. Objekte können auf Storage-Nodes, in Cloud-Storage-Pools oder auf Archiv-Nodes gespeichert werden.
- Der Typ der Objektkopien, die erstellt wurden. Kopien können repliziert oder Erasure Coding ausgeführt werden.
- Für replizierte Kopien die Anzahl der Kopien, die erstellt werden.
- Für Kopien mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) wurde das Verfahren zur Einhaltung von Datenkonsistenz verwendet.
- Die Änderungen im Laufe der Zeit an dem Storage-Standort und den Koprototypen eines Objekts.
- Schutz von Objektdaten bei Aufnahme von Objekten in das Grid (synchrone Platzierung oder Dual-Commit)

Objekt-Metadaten werden nicht durch ILM-Regeln gemanagt. Stattdessen werden Objekt-Metadaten in einer Cassandra-Datenbank in einem sogenannten Metadaten-Speicher gespeichert. Drei Kopien von Objekt-Metadaten werden automatisch an jedem Standort aufbewahrt, um die Daten vor Verlust zu schützen.

Beispiel für eine ILM-Regel

Eine ILM-Regel könnte beispielsweise Folgendes angeben:

- Nur auf die Objekte anwenden, die zu Mandant A gehören
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Standort.
- Behalten Sie die beiden Kopien „Forever,“ bei, was bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte so lange bei, bis sie von einer Löschanfrage eines Clients oder nach Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die ausgewogene Option für das Aufnahmeverhalten: Die Anweisung zur Platzierung von zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, sofort beide erforderlichen Kopien zu erstellen.

Wenn z. B. Standort 2 nicht erreichbar ist, wenn Mandant A ein Objekt speichert, erstellt StorageGRID zwei Zwischenkopien auf Storage-Nodes an Standort 1. Sobald Standort 2 verfügbar wird, erstellt StorageGRID die erforderliche Kopie an diesem Standort.

Bewertung von Objekten durch eine ILM-Richtlinie

Die aktive ILM-Richtlinie für das StorageGRID System steuert die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte.

Wenn Clients Objekte in StorageGRID speichern, werden die Objekte anhand der bestellten ILM-Regeln in der aktiven Richtlinie bewertet:

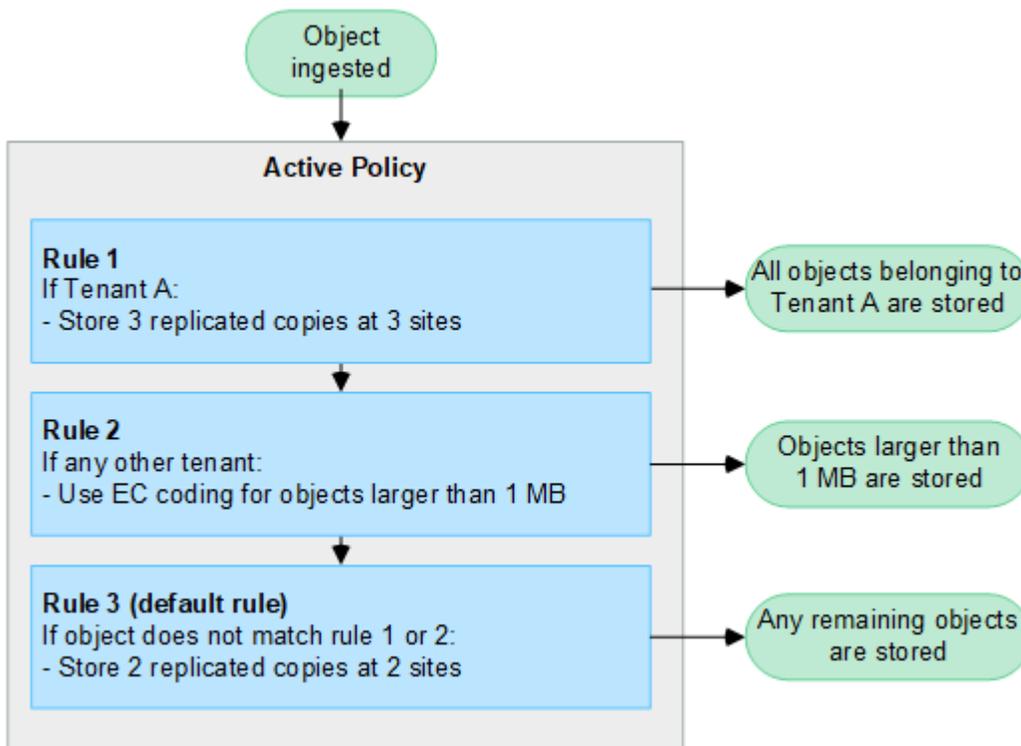
1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten der Regel aufgenommen und gemäß den Anweisungen zur Platzierung dieser Regel gespeichert.
2. Wenn die Filter für die erste Regel nicht mit dem Objekt übereinstimmen, wird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

Beispiel für eine ILM-Richtlinie

Eine ILM-Richtlinie könnte beispielsweise drei ILM-Regeln enthalten, die Folgendes angeben:

- **Regel 1: Replizierte Kopien für Mandant A**
 - Alle Objekte, die zu Mandant A gehören, abgleichen
 - Speichern Sie diese Objekte als drei replizierte Kopien an drei Standorten.
 - Objekte, die zu anderen Mandanten gehören, werden nicht mit Regel 1 abgeglichen, daher werden sie mit Regel 2 verglichen.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**

- Alle Objekte von anderen Mandanten abgleichen, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert.
- Entspricht nicht Objekten mit einer Größe von 1 MB oder weniger, daher werden diese Objekte mit Regel 3 verglichen.
- **Regel 3: 2 Exemplare 2 Rechenzentren** (Standard)
 - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
 - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und mindestens 1 MB groß sind).



Verwandte Informationen

- ["Objektmanagement mit ILM"](#)

Entdecken Sie StorageGRID

Entdecken Sie den Grid Manager

Der Grid Manager ist eine browserbasierte grafische Schnittstelle, mit der Sie Ihr StorageGRID System konfigurieren, managen und überwachen können.

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

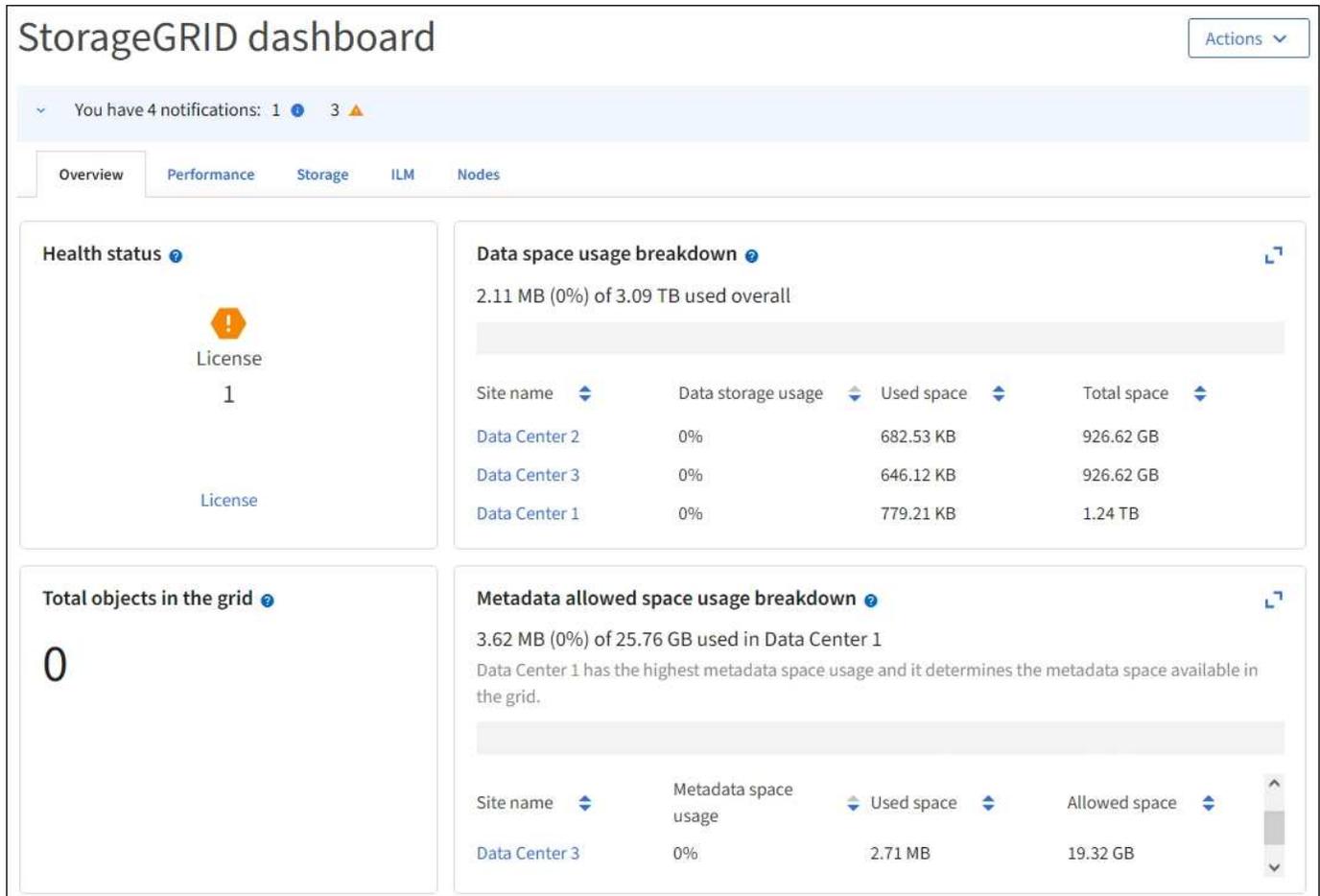
Sie können über ein auf den Grid Manager zugreifen ["Unterstützter Webbrowser"](#).

Grid Manager Dashboard

Wenn Sie sich zum ersten Mal beim Grid Manager anmelden, können Sie das Dashboard verwenden, um

Systemaktivitäten auf einen Blick zu überwachen.

Das Dashboard enthält Informationen zu Systemzustand und Performance, Storage-Verwendung, ILM-Prozessen, S3- und Swift-Vorgängen und den Nodes im Grid. Sie können das Dashboard konfigurieren, indem Sie aus einer Sammlung von Karten auswählen, die die Informationen enthalten, die Sie zur effektiven Überwachung Ihres Systems benötigen.



Um die Informationen auf jeder Karte zu erläutern, wählen Sie das Hilfesymbol Für diese Karte.

Weitere Informationen .

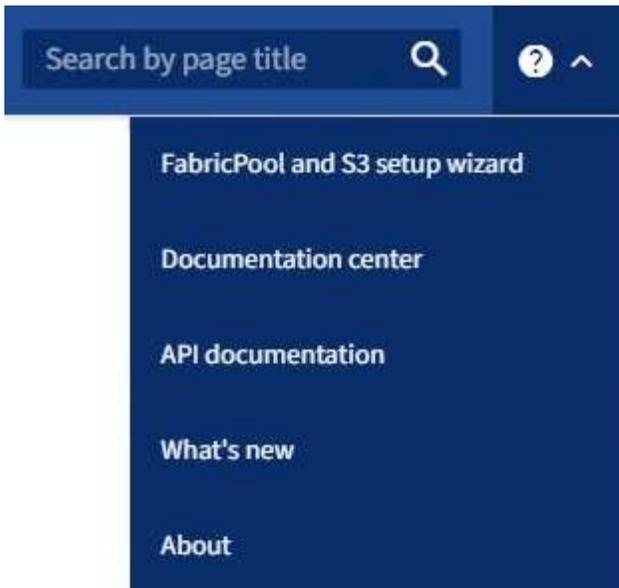
- ["Anzeigen und Konfigurieren des Dashboards"](#)

Suchfeld

Mit dem Feld **Suche** in der Kopfzeile können Sie schnell zu einer bestimmten Seite in Grid Manager navigieren. Sie können beispielsweise **km** eingeben, um auf die Seite Key Management Server (KMS) zuzugreifen. Sie können **Suche** verwenden, um Einträge in der Seitenleiste des Grid Managers sowie in den Menüs Konfiguration, Wartung und Support zu finden.

Hilfe-Menü

Das Hilfe-Menü Bietet Zugriff auf den Einrichtungsassistenten für FabricPool und S3, das StorageGRID Dokumentationscenter für die aktuelle Version und die API-Dokumentation. Sie bestimmen auch, welche Version von StorageGRID derzeit installiert ist.

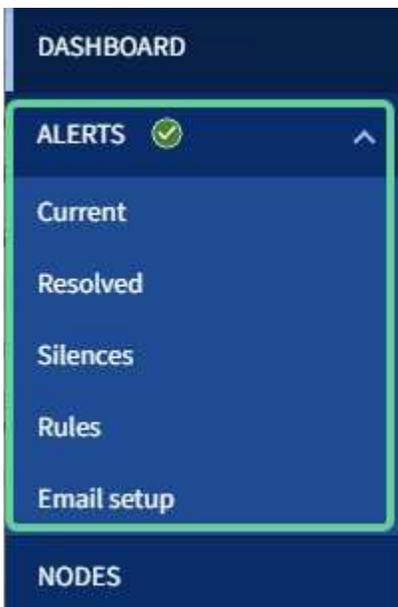


Weitere Informationen .

- ["Verwenden Sie den FabricPool-Einrichtungsassistenten"](#)
- ["Verwenden Sie den S3-Einrichtungsassistenten"](#)
- ["Verwenden Sie die Grid-Management-API"](#)

Menü „Meldungen“

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



Im Menü „Meldungen“ können Sie Folgendes tun:

- Überprüfen Sie aktuelle Warnmeldungen
- Überprüfen Sie behobene Warnmeldungen
- Konfigurieren Sie Stille, um Benachrichtigungen zu unterdrücken

- Definieren Sie Alarmregeln für Bedingungen, die Warnmeldungen auslösen
- Konfigurieren Sie den E-Mail-Server für Warnmeldungen

Weitere Informationen .

- ["Verwalten von Meldungen"](#)

Knoten Seite

Auf der Seite Knoten werden Informationen zum gesamten Raster, zu jedem Standort im Raster und zu jedem Node an einem Standort angezeigt.

Auf der Startseite Nodes werden die kombinierten Metriken für das gesamte Raster angezeigt. Um Informationen zu einem bestimmten Standort oder Node anzuzeigen, wählen Sie den Standort oder Node aus.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

Weitere Informationen .

- ["Zeigen Sie die Seite Knoten an"](#)

Mandanten werden gestartet

Auf der Seite Mandanten können Sie Storage-Mandantenkonten für Ihr StorageGRID System erstellen und überwachen. Sie müssen mindestens ein Mandantenkonto erstellen, um anzugeben, wer Objekte speichern und abrufen kann und welche Funktionen ihnen zur Verfügung stehen.

Die Seite „Mandanten“ stellt zudem Nutzungsdetails für die einzelnen Mandanten bereit, einschließlich der Anzahl der verwendeten Storage-Ressourcen und der Anzahl der Objekte. Wenn Sie beim Erstellen des Mandanten eine Quote festlegen, sehen Sie, wie viel von dieser Quote verwendet wurde.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 2 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	S3 Tenant	0 bytes	0%	100.00 GB	0	→ 📄
<input type="checkbox"/>	Swift Tenant	0 bytes	0%	100.00 GB	0	→ 📄

← Previous 1 Next →

Weitere Informationen .

- ["Verwalten von Mandanten"](#)
- ["Verwenden Sie ein Mandantenkonto"](#)

ILM-Menü

Über das ILM-Menü können Sie Regeln und Richtlinien für das Information Lifecycle Management (ILM) konfigurieren, die die Langlebigkeit und Verfügbarkeit von Daten regeln. Sie können auch eine Objekt-ID eingeben, um die Metadaten für das Objekt anzuzeigen.

DASHBOARD

ALERTS ✓

NODES

TENANTS

ILM ↑

- Rules
- Policies
- Storage pools
- Erasure coding
- Storage grades
- Regions
- Object metadata lookup

CONFIGURATION

Weitere Informationen .

- ["Verwenden Sie das Information Lifecycle Management"](#)
- ["Objektmanagement mit ILM"](#)

Konfigurationsmenü

Über das Konfigurationsmenü können Sie Netzwerkeinstellungen, Sicherheitseinstellungen, Systemeinstellungen, Überwachungsoptionen und Optionen für die Zugriffssteuerung festlegen.

Configuration				
Configure your StorageGRID system.				
Network	Security	System	Monitoring	Access control
High availability groups	Certificates	Grid federation	Audit and syslog server	Admin groups
Load balancer endpoints	Firewall control	Object compression	SNMP agent	Admin users
S3 endpoint domain names	Key management server	S3 Object Lock		Grid passwords
Traffic classification	Security settings	Storage options		Identity federation
VLAN interfaces	Proxy settings			Single sign-on

Netzwerkaufgaben

Zu den Netzwerkaufgaben gehören:

- ["Verwalten von Hochverfügbarkeitsgruppen"](#)
- ["Verwalten von Endpunkten des Load Balancer"](#)
- ["Konfigurieren von S3-Endpunkt-Domännennamen"](#)
- ["Verwalten von Richtlinien für die Verkehrsklassifizierung"](#)
- ["Konfigurieren von VLAN-Schnittstellen"](#)

Sicherheitsaufgaben

Zu den Sicherheitsaufgaben gehören:

- ["Verwalten von Sicherheitszertifikaten"](#)
- ["Management interner Firewall-Kontrollen"](#)
- ["Konfigurieren von Verschlüsselungsmanagement-Servern"](#)
- Konfigurieren von Sicherheitseinstellungen einschließlich des ["TLS- und SSH-Richtlinie"](#), ["Optionen für die Netzwerk- und Objektsicherheit"](#), Und das ["Zeitlimit für Inaktivität des Browsers"](#).
- Konfigurieren der Einstellungen für ein ["Storage-Proxy"](#) Oder an ["Admin-Proxy"](#)

Systemaufgaben

Zu den Systemaufgaben gehören:

- Wird verwendet **"Grid-Verbund"** Zum Klonen von Mandantenkontoinformationen und zum Replizieren von Objektdaten zwischen zwei StorageGRID-Systemen
- Aktivieren Sie optional das **"Gespeicherte Objekte komprimieren"** Option.
- **"Verwalten der S3-Objektsperre"**
- Allgemeines zu Storage-Optionen wie z. B. **"Objektsegmentierung"** Und **"Wasserzeichen für Storage-Volumes"**.

Überwachungsaufgaben

Zu den Überwachungsaufgaben gehören:

- **"Konfigurieren von Überwachungsmeldungen und Protokollzielen"**
- **"Verwendung von SNMP-Überwachung"**

Zugriffskontrollaufgaben

Zu den Aufgaben der Zugriffssteuerung gehören:

- **"Verwalten von Admin-Gruppen"**
- **"Verwalten von Administratorbenutzern"**
- Ändern der **"Provisionierungs-Passphrase"** Oder **"Passwörter für die Node-Konsole"**
- **"Identitätsföderation verwenden"**
- **"SSO wird konfiguriert"**

Menü Wartung

Im Menü Wartung können Sie Wartungsarbeiten, Systemwartung und Netzwerkwartung durchführen.

Maintenance

Perform maintenance procedures on your StorageGRID system.

Tasks	System	Network
Decommission	License	DNS servers
Expansion	Recovery package	Grid Network
Recovery	Software update	NTP servers
Rename grid, sites, or nodes		
Object existence check		
Volume restoration		

Aufgaben

Zu den Wartungsarbeiten gehören:

- ["Stilllegungsvorgänge"](#) Um nicht verwendete Grid-Nodes und -Standorte zu entfernen
- ["Erweiterungsoperationen"](#) Um neue Grid-Nodes und -Standorte hinzuzufügen
- ["Verfahren zur Recovery von Grid-Nodes"](#) Zum Ersetzen eines fehlerhaften Node und Wiederherstellen von Daten
- ["Verfahren umbenennen"](#) Ändern der Anzeigenamen des Rasters, der Standorte und Knoten
- ["Vorgänge zur Überprüfung der Objektexistenz"](#) Um das Vorhandensein von Objektdaten (wenn auch nicht die Richtigkeit) zu überprüfen
- ["Volume-Wiederherstellungsvorgänge"](#)

System

Sie können folgende Systemwartungsaufgaben ausführen:

- ["Anzeigen von StorageGRID-Lizenzinformationen"](#) Oder ["Lizenzinformationen werden aktualisiert"](#)
- Generieren und Herunterladen der ["Wiederherstellungspaket"](#)
- StorageGRID Software-Updates, einschließlich Software-Upgrades und Hotfixes, sowie Updates für die SANtricity OS Software auf ausgewählten Appliances
 - ["Upgrade-Verfahren"](#)
 - ["Hotfix-Verfahren"](#)
 - ["Aktualisieren Sie das SANtricity OS auf SG6000 Storage-Controllern über den Grid Manager"](#)
 - ["Aktualisieren Sie das SANtricity Betriebssystem auf SG5700 Storage Controllern mit Grid Manager"](#)

Netzwerk

Sie können folgende Aufgaben zur Netzwerkwartung ausführen:

- "DNS-Server werden konfiguriert"
- "Aktualisieren von Netznetzen"
- "Verwalten von NTP-Servern"

Menü „Support“

Das Menü Support enthält Optionen, die dem technischen Support bei der Analyse und Fehlerbehebung Ihres Systems helfen. Das Menü „Support“ enthält drei Teile: Tools, Alarme (Legacy) und andere.

Support

If a problem occurs, use Support options to help technical support analyze and troubleshoot your system.

Tools	Alarms (legacy)	Other
AutoSupport	Current alarms	Link cost
Diagnostics	Historical alarms	NMS entities
Grid topology	Custom events	
Logs	Global alarms	
Metrics	Legacy email setup	

Tools

Im Abschnitt Tools des Menüs Support können Sie folgende Aufgaben ausführen:

- "Konfigurieren Sie AutoSupport"
- "Führen Sie eine Diagnose aus" Auf den aktuellen Zustand des Rasters
- "Greifen Sie auf die Baumstruktur der Grid-Topologie zu" So zeigen Sie detaillierte Informationen zu Grid-Nodes, Services und Attributen an
- "Erfassen von Protokolldateien und Systemdaten"
- "Prüfen von Support-Kennzahlen"



Die Tools, die über die Option **Metrics** zur Verfügung stehen, sind für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig.

Alarme (alt)

Im Bereich Alarme (Legacy) des Menüs Support können Sie aktuelle, historische und globale Alarme überprüfen, benutzerdefinierte Ereignisse einrichten und E-Mail-Benachrichtigungen für ältere Alarme

einrichten. Siehe "[Verwalten von Alarmen \(Altsystem\)](#)".



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Entdecken Sie den Tenant Manager

Der MandantenManager ist die browserbasierte grafische Schnittstelle, die Mandantenbenutzer darauf zugreifen, um ihre Storage-Konten zu konfigurieren, zu managen und zu überwachen.

Wenn sich Mandantenbenutzer beim Mandanten-Manager anmelden, stellen sie eine Verbindung zu einem Admin-Node her.

Mandanten-Manager Dashboard

Nachdem ein Grid-Administrator ein Mandantenkonto erstellt hat, indem er den Grid Manager oder die Grid Management API verwendet, können sich Mandantenbenutzer beim Mandanten-Manager anmelden.

Über das Tenant Manager Dashboard können Mandantenbenutzer die Storage-Auslastung auf einen Blick überwachen. Im Bereich Storage-Nutzung finden Sie eine Liste der größten Buckets (S3) oder Container (Swift) für den Mandanten. Der Wert für „genutzter Speicherplatz“ ist die Gesamtmenge der Objektdaten im Bucket oder Container. Das Balkendiagramm stellt die relative Größe dieser Buckets oder Container dar.

Der über dem Balkendiagramm angezeigte Wert ist eine Summe des Speicherplatzes, der für alle Buckets oder Container des Mandanten verwendet wird. Wurde zum Zeitpunkt der Kontoerstellung die maximale Anzahl an Gigabyte, Terabyte oder Petabyte angegeben, so wird auch die Menge des verwendeten Kontingents und der verbleibenden Menge angezeigt.

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups

1 User
View users

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

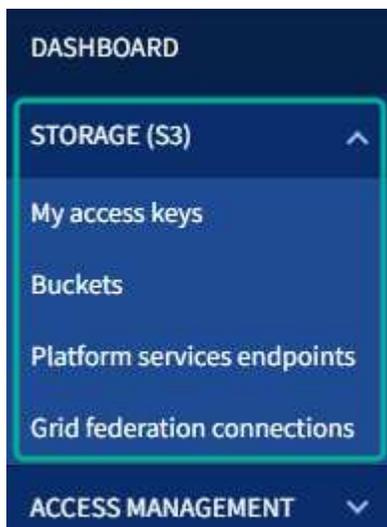
Tenant details [?](#)

Name: Tenant02
ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Speichermenü (S3)

Das Menü Storage wird nur für S3-Mandantenkonten angezeigt. In diesem Menü können S3 Benutzer Zugriffsschlüssel managen, Buckets erstellen, managen und löschen, Plattform-Services-Endpunkte managen und alle Grid-Verbindungen anzeigen, die sie verwenden dürfen.



Meine Zugriffsschlüssel

S3-Mandantenbenutzer können die Zugriffsschlüssel wie folgt managen:

- Benutzer, die über die Berechtigung eigene S3-Anmeldedaten verwalten verfügen, können ihre eigenen S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit Root-Zugriffsberechtigung können die Zugriffsschlüssel für das S3-Stammkonto, ihr eigenes Konto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel bieten auch vollständigen Zugriff auf die Buckets und Objekte des Mandanten, sofern nicht ausdrücklich von einer Bucket-Richtlinie deaktiviert wurde.



Die Verwaltung der Zugriffstasten für andere Benutzer erfolgt über das Menü Access Management.

Buckets

S3-Mandantenbenutzer mit entsprechenden Berechtigungen können für ihre Buckets die folgenden Aufgaben ausführen:

- Buckets erstellen
- Aktivieren der S3-Objektsperre für einen neuen Bucket (vorausgesetzt, dass die S3-Objektsperre für das StorageGRID-System aktiviert ist)
- Aktualisieren Sie die Einstellungen für die Konsistenzstufe
- Aktivieren und deaktivieren Sie die Zeitaktualisierungen für den letzten Zugriff
- Aktivieren oder Anhalten der Objektversionierung
- Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung
- Konfiguration der Cross-Origin Resource Sharing (CORS)
- Löschen aller Objekte in einem Bucket
- Leere Buckets löschen
- Verwenden Sie die "[Experimentelle S3 Konsole](#)" Zum Managen von Bucket-Objekten

Wenn ein Grid-Administrator die Nutzung von Plattform-Services für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit den entsprechenden Berechtigungen die folgenden Aufgaben ausführen:

- Konfigurieren Sie S3-Ereignisbenachrichtigungen, die an einen Zieldienst gesendet werden können, der den Amazon Simple Notification Service™ (Amazon SNS) unterstützt.
- Konfigurieren Sie die CloudMirror-Replizierung, mit der Mandanten Objekte automatisch in einen externen S3-Bucket replizieren können.
- Die Suchintegration konfiguriert: Sendet Objektmetadaten an einen Ziel-Suchindex, wenn ein Objekt erstellt, gelöscht oder seine Metadaten oder Tags aktualisiert werden.

Plattform-Services-Endpunkte

Wenn ein Grid-Administrator die Nutzung von Plattformservices für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit der Berechtigung zum Verwalten von Endpunkten für jeden Plattformservice einen Zielpunkt konfigurieren.

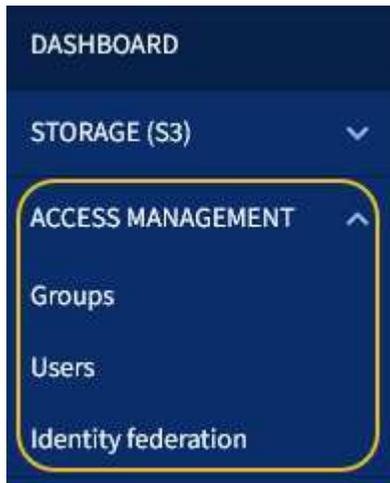
Netzverbundverbindungen

Wenn ein Grid-Administrator die Verwendung einer Grid-Verbundverbindung für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit Root-Zugriffsberechtigungen den Verbindungsnamen anzeigen und die Seite mit Bucket-Details für jeden Bucket aufrufen, für den die Grid-übergreifende Replizierung aktiviert ist,

Und zeigen Sie den letzten Fehler an, der beim Replizieren von Bucket-Daten in das andere Grid in der Verbindung auftritt. Siehe "[Anzeigen von Verbindungen mit Grid Federation](#)".

Öffnen Sie das Menü Management

Über das Menü Zugriffsmanagement können StorageGRID-Mandanten Benutzergruppen aus einer föderierten Identitätsquelle importieren und Verwaltungsberechtigungen zuweisen. Außerdem können Mandanten lokale Mandantengruppen und Benutzer managen, es sei denn, Single Sign On (SSO) gilt für das gesamte StorageGRID System.



Verwandte Informationen

- "[Verwenden Sie ein Mandantenkonto](#)"

Netzwerkrichtlinien

Netzwerkrichtlinien: Überblick

Mithilfe dieser Richtlinien lernen Sie die StorageGRID Architektur und Netzwerktopologien kennen und erfahren Sie mehr über die Anforderungen für Netzwerkkonfiguration und Provisionierung.

Informationen zu diesen Anweisungen

Diese Richtlinien stellen Informationen bereit, die zum Erstellen der StorageGRID Netzwerkinfrastruktur vor der Bereitstellung und Konfiguration von StorageGRID Nodes verwendet werden können. Verwenden Sie diese Richtlinien, um sicherzustellen, dass die Kommunikation zwischen allen Knoten im Netz und zwischen dem Netz und externen Clients und Diensten erfolgen kann.

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

- Speichern und Abrufen von Objektdaten
- Benachrichtigungen erhalten
- Zugriff auf die StorageGRID Management-Schnittstelle (Grid Manager und MandantenManager)
- Zugriff auf die Revisionsfreigabe (optional)
- Die Bereitstellung von Services wie:

- Network Time Protocol (NTP)
- Domain Name System (DNS)
- Verschlüsselungsmanagement-Server (KMS)

StorageGRID-Netzwerke müssen entsprechend konfiguriert werden, um den Datenverkehr für diese Funktionen und vieles mehr zu verarbeiten.

Bevor Sie beginnen

Die Konfiguration des Netzwerks für ein StorageGRID System erfordert eine hohe Erfahrung mit Ethernet-Switching, TCP/IP-Netzwerken, Subnetzen, Netzwerk-Routing und Firewalls.

Machen Sie sich vor dem Konfigurieren des Netzwerknetzwerks mit der StorageGRID-Architektur vertraut, wie in beschrieben ["Weitere Informationen zu StorageGRID"](#).

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

Installation softwarebasierter Nodes

- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)
- ["VMware installieren"](#)

Installieren Sie Appliance-Knoten

- ["Appliance-Hardware installieren"](#)

StorageGRID Software konfigurieren und verwalten

- ["StorageGRID verwalten"](#)
- ["Versionshinweise"](#)

StorageGRID-Netzwerktypen

Die Grid-Nodes in einem StorageGRID-Systemprozess *Grid Traffic*, *admin Traffic* und *Client Traffic*. Sie müssen das Netzwerk entsprechend konfigurieren, um diese drei Arten von Datenverkehr zu managen und um Kontrolle und Sicherheit zu bieten.

Verkehrstypen

Verkehrstyp	Beschreibung	Netzwerktyp
Grid-Traffic	Der interne StorageGRID-Datenverkehr zwischen allen Nodes im Grid. Alle Grid-Nodes müssen über dieses Netzwerk mit allen anderen Grid-Nodes kommunizieren können.	Grid-Netzwerk (erforderlich)
Admin-Datenverkehr	Der für die Systemadministration und -Wartung verwendete Datenverkehr.	Admin-Netzwerk (optional), VLAN-Netzwerk (optional)

Verkehrstyp	Beschreibung	Netzwerktyp
Client-Traffic	Der Datenverkehr zwischen externen Client-Applikationen und dem Grid, einschließlich aller Objekt-Storage-Anforderungen von S3 und Swift Clients	Client-Netzwerk (optional), VLAN-Netzwerk (optional)

Sie haben folgende Möglichkeiten zur Konfiguration des Netzwerks:

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

Das Grid-Netzwerk ist obligatorisch und kann den gesamten Grid-Verkehr verwalten. Die Admin- und Client-Netzwerke können zum Zeitpunkt der Installation hinzugefügt oder später hinzugefügt werden, um sich an Änderungen der 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 für den administrativen und Client-Datenverkehr verwenden.

Auf interne Ports kann nur über das Grid-Netzwerk zugegriffen werden. Auf externe Ports kann von allen Netzwerktypen zugegriffen werden. Diese Flexibilität bietet mehrere Optionen für den Entwurf einer StorageGRID-Implementierung sowie für die Einrichtung einer externen IP- und Portfilterung in Switches und Firewalls. Siehe "[Interne Kommunikation mit Grid-Nodes](#)" Und "[Externe Kommunikation](#)".

Netzwerkschnittstellen

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

Netzwerk	Schnittstellename
Grid-Netzwerk (erforderlich)	Eth0
Admin-Netzwerk (optional)	Eth1
Client-Netzwerk (optional)	Eth2

Weitere Informationen über die Zuordnung von virtuellen oder physischen Ports zu Node-Netzwerkschnittstellen finden Sie in den Installationsanweisungen:

Softwarebasierte Nodes

- "[Installieren Sie Red hat Enterprise Linux oder CentOS](#)"
- "[Installieren Sie Ubuntu oder Debian](#)"
- "[VMware installieren](#)"

Appliance-Nodes

- "[SGF6112 Storage Appliance](#)"
- "[SG6000 Storage Appliance](#)"
- "[SG5700 Storage-Appliance](#)"

- ["SG100- und SG1000-Services-Appliances"](#)

Netzwerkinformationen für jeden Node

Sie müssen für jedes auf einem Node zu konfigurierende Netzwerk Folgendes konfigurieren:

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

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

Hochverfügbarkeitsgruppen

Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) bieten die Möglichkeit, virtuelle IP-Adressen (VIP) zur Grid- oder Client-Netzwerkschnittstelle hinzuzufügen. Weitere Informationen finden Sie unter ["Management von Hochverfügbarkeitsgruppen"](#).

Grid-Netzwerk

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



StorageGRID unterstützt keine Network Address Translation (NAT) zwischen Knoten.

Das Grid-Netzwerk kann für den gesamten Admin-Datenverkehr und den gesamten Client-Datenverkehr verwendet werden, selbst wenn das Admin-Netzwerk und das Client-Netzwerk konfiguriert sind. Das Grid Network Gateway ist das Standard-Gateway des Nodes, es sei denn, der Knoten hat das Client Network konfiguriert.



Wenn Sie das Grid-Netzwerk konfigurieren, müssen Sie sicherstellen, dass das Netzwerk von nicht vertrauenswürdigen Clients, wie 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 es mehrere Grid-Subnetze gibt.
- Das Grid-Netzwerk-Gateway ist der Node-Standard-Gateway, bis die Grid-Konfiguration abgeschlossen ist.
- Statische Routen werden automatisch für alle Nodes zu allen Subnetzen generiert, die in der globalen Grid-Netzwerk-Subnetliste konfiguriert sind.
- 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. Bei der Konfiguration kann diese für die Systemadministration und für den Wartungs-Traffic verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss

nicht zwischen Knoten routingfähig sein.

Sie können auswählen, auf welchen Grid-Knoten das Admin-Netzwerk aktiviert sein soll.

Wenn Sie das Admin-Netzwerk verwenden, muss der Verwaltungs- und Wartungsverkehr nicht über das Grid-Netzwerk geleitet werden. Typische Anwendungen des Admin-Netzwerks umfassen Folgendes:

- Zugriff auf die Benutzeroberflächen von Grid Manager und Tenant Manager.
- Zugriff auf wichtige Services wie NTP-Server, DNS-Server, externe Verschlüsselungsmanagement-Server (KMS) und LDAP-Server (Lightweight Directory Access Protocol)
- Zugriff auf Prüfprotokolle an Admin-Nodes.
- Secure Shell Protocol (SSH)-Zugriff für Wartung und Support

Das Admin-Netzwerk wird nie für den internen Grid-Verkehr verwendet. Ein Admin-Netzwerk-Gateway wird bereitgestellt und ermöglicht dem Admin-Netzwerk die Kommunikation mit mehreren externen Subnetzen. Das Admin-Netzwerk-Gateway wird jedoch nie als Standard-Gateway für den Node verwendet.

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

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

Client-Netzwerk

Das Client-Netzwerk ist optional. Bei der Konfiguration ermöglicht er den Zugriff auf Grid-Services für Client-Applikationen wie S3 und Swift. Wenn Sie StorageGRID Daten für eine externe Ressource zugänglich machen möchten (z. B. einen Cloud-Speicherpool oder den StorageGRID CloudMirror Replikationsservice), kann die externe Ressource auch das Client-Netzwerk nutzen. 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 sein soll. Alle Knoten müssen sich nicht im gleichen Client-Netzwerk befinden, und Knoten kommunizieren nie über das Client-Netzwerk miteinander. Das Client-Netzwerk ist erst nach Abschluss der Grid-Installation betriebsbereit.

Für zusätzliche Sicherheit können Sie angeben, dass die Client-Netzwerk-Schnittstelle eines Node nicht vertrauenswürdig ist, sodass das Client-Netzwerk restriktiver ist, welche Verbindungen zulässig sind. Wenn die Client-Netzwerk-Schnittstelle eines Node nicht vertrauenswürdig ist, akzeptiert die Schnittstelle ausgehende Verbindungen, wie sie von der CloudMirror-Replikation verwendet werden, akzeptiert jedoch nur eingehende Verbindungen an Ports, die explizit als Load-Balancer-Endpunkte konfiguriert wurden. Siehe "[Management der Firewall-Kontrollen](#)" Und "[Konfigurieren von Load Balancer-Endpunkten](#)".

Wenn Sie ein Client-Netzwerk verwenden, muss der Client-Datenverkehr nicht über das Grid-Netzwerk geleitet werden. Der Netzwerkverkehr kann in ein sicheres, nicht routingbares Netzwerk getrennt werden. Die folgenden Node-Typen werden häufig mit einem Client-Netzwerk konfiguriert:

- Gateway-Nodes, da diese Nodes Zugriff auf den StorageGRID Load Balancer Service und S3- und Swift-Client-Zugriff auf das Grid bieten.
- Storage-Nodes, da diese Nodes Zugriff auf die S3- und Swift-Protokolle sowie auf Cloud Storage Pools und den CloudMirror-Replizierungsservice bieten.
- Admin-Nodes, um sicherzustellen, dass Mandantenbenutzer mit dem Tenant Manager verbinden können,

ohne das Admin Network 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 die Standardroute für den Grid-Node, wenn die Grid-Konfiguration abgeschlossen ist.

Optionale VLAN-Netzwerke

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

Zur Unterstützung der Verwendung von VLANs müssen Sie eine oder mehrere Schnittstellen auf einem Node als Trunk-Schnittstellen am Switch konfigurieren. Sie können die Grid-Netzwerkschnittstelle (eth0) oder die Client-Netzwerkschnittstelle (eth2) als Trunk konfigurieren oder dem Knoten Leitungsschnittstellen hinzufügen.

Wenn eth0 als Trunk konfiguriert ist, fließt Grid-Netzwerk-Traffic über die native Trunk-Schnittstelle, wie auf dem Switch konfiguriert. Wenn eth2 als Trunk konfiguriert ist und das Client-Netzwerk auch auf demselben Node konfiguriert ist, verwendet das Client-Netzwerk das native VLAN des Trunk-Ports wie auf dem Switch konfiguriert.

Nur eingehender Admin-Traffic, wie er für SSH, Grid Manager oder Tenant Manager-Datenverkehr verwendet wird, wird über VLAN-Netzwerke unterstützt. Outbound-Traffic, z. B. für NTP, DNS, LDAP, KMS und Cloud Storage-Pools, wird nicht über VLAN-Netzwerke unterstützt.



VLAN-Schnittstellen können nur zu Admin-Nodes und Gateway-Nodes hinzugefügt werden. Sie können keine VLAN-Schnittstelle für den Client- oder Administratorzugriff auf Storage Nodes oder Archive Nodes verwenden.

Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)" Anweisungen und Richtlinien.

VLAN-Schnittstellen werden nur in HA-Gruppen verwendet und auf dem aktiven Node werden VIP-Adressen zugewiesen. Siehe "[Management von Hochverfügbarkeitsgruppen](#)" Anweisungen und Richtlinien.

Beispiele für Netzwerktopologie

Grid-Netzwerktopologie

Die einfachste Netzwerktopologie wird nur durch die Konfiguration des Grid-Netzwerks erstellt.

Wenn Sie das Grid-Netzwerk konfigurieren, stellen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle für jeden Grid-Node ein.

Während der Konfiguration müssen Sie alle Grid-Netzwerk-Subnetze der Grid-Netzwerk-Subnetz-Liste (GNSL) hinzufügen. Diese Liste enthält alle Subnetze für alle Standorte und kann auch externe Subnetze enthalten, die den Zugriff auf kritische Services wie NTP, DNS oder LDAP bieten.

Bei der Installation wendet die Grid-Netzwerkschnittstelle statische Routen für alle Subnetze in der GNSL an und setzt die Standardroute des Knotens auf das Grid-Netzwerk-Gateway, wenn eine konfiguriert ist. Die GNSL ist nicht erforderlich, wenn kein Client-Netzwerk vorhanden ist und das Grid-Netzwerk-Gateway die

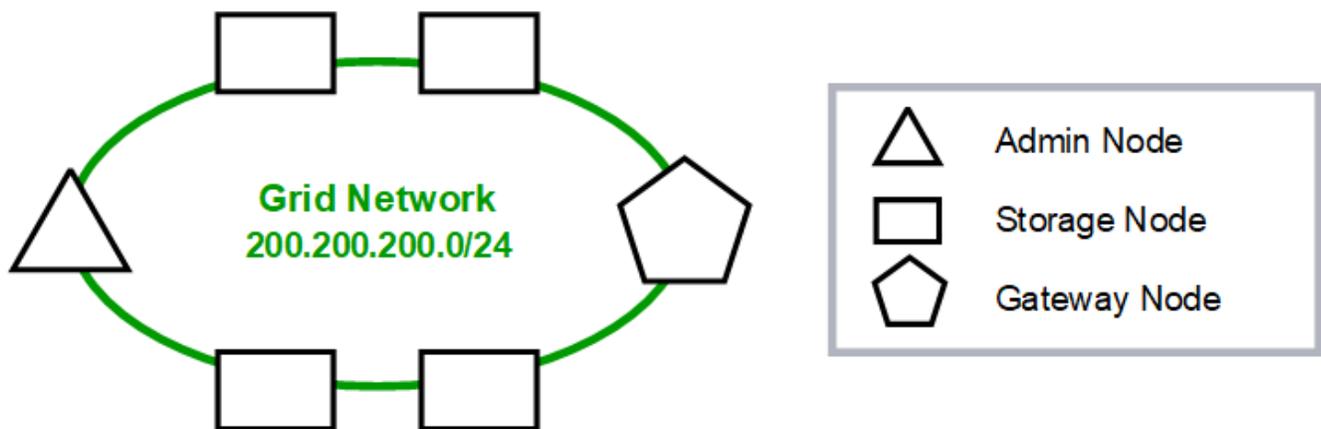
Standardroute des Knotens ist. Zudem werden Host-Routen zu allen anderen Knoten im Grid generiert.

In diesem Beispiel verwendet der gesamte Datenverkehr dasselbe Netzwerk, einschließlich des Datenverkehrs für S3- und Swift-Client-Anforderungen sowie Administrations- und Wartungsfunktionen.



Diese Topologie eignet sich für Implementierungen an einem einzigen Standort, die nicht extern verfügbar sind, Proof-of-Concept- oder Testbereitstellungen oder wenn ein Load Balancer eines Drittanbieters als Grenze für den Client-Zugriff fungiert. Wenn möglich, sollte das Grid-Netzwerk ausschließlich für den internen Datenverkehr verwendet werden. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk haben zusätzliche Firewall-Einschränkungen, die externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Datenverkehr wird unterstützt, aber diese Verwendung bietet weniger Schutzebenen.

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
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

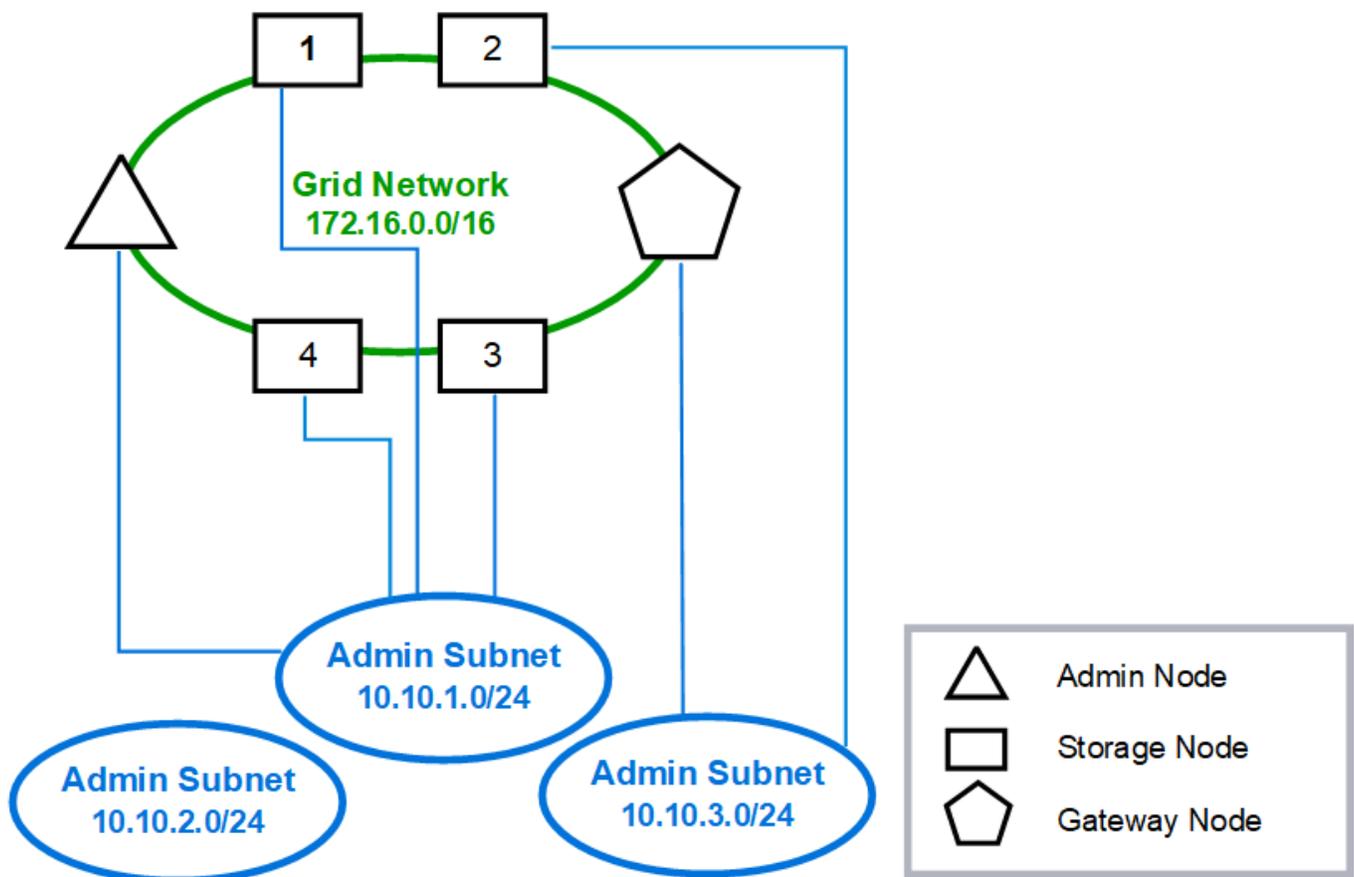
Die Verwendung eines Admin-Netzwerks ist optional. Eine Möglichkeit, wie Sie ein Admin-Netzwerk und ein Grid-Netzwerk verwenden können, besteht darin, ein routingbares Grid-Netzwerk und ein verbundenes Admin-Netzwerk für jeden Knoten zu konfigurieren.

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

Das Admin-Netzwerk kann für jeden Knoten eindeutig sein und aus mehreren Subnetzen bestehen. Jeder Node kann mit einer externen Subnetz-Liste (AESL) des Administrators konfiguriert werden. Die AESL listet die Subnetze auf, die über das Admin-Netzwerk für jeden Knoten erreichbar sind. Die AESL muss auch die Subnetze aller Dienste enthalten, auf die das Grid über das Admin-Netzwerk zugreifen kann, wie NTP, DNS, KMS und LDAP. Für jedes Subnetz in der AESL werden statische Routen angewendet.

In diesem Beispiel wird das Grid Network für Traffic verwendet, der mit S3- und Swift-Client-Anforderungen und Objektmanagement zusammenhängt. Während das Admin-Netzwerk für administrative Funktionen verwendet wird.

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

Nodes	Grid Network		Admin Network	
	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,	172.16.0.0/16 → eth0	Static	GNSL
Storage 1,	10.10.1.0/24 → eth1	Link	Interface IP/mask
3, and 4	10.10.2.0/24 → 10.10.1.1	Static	AESL
	10.10.3.0/24 → 10.10.1.1	Static	AESL
Storage 2,	172.16.0.0/16 → eth0	Static	GNSL
Gateway	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. Über ein Client-Netzwerk kann der Netzwerk-Traffic des Clients (z. B. S3 und Swift) vom internen Grid-Datenverkehr getrennt werden, wodurch die Sicherheit des Grid-Netzwerks erhöht wird. Wenn das Admin-Netzwerk nicht konfiguriert ist, kann der administrative Datenverkehr entweder vom Client oder vom Grid-Netzwerk verarbeitet werden.

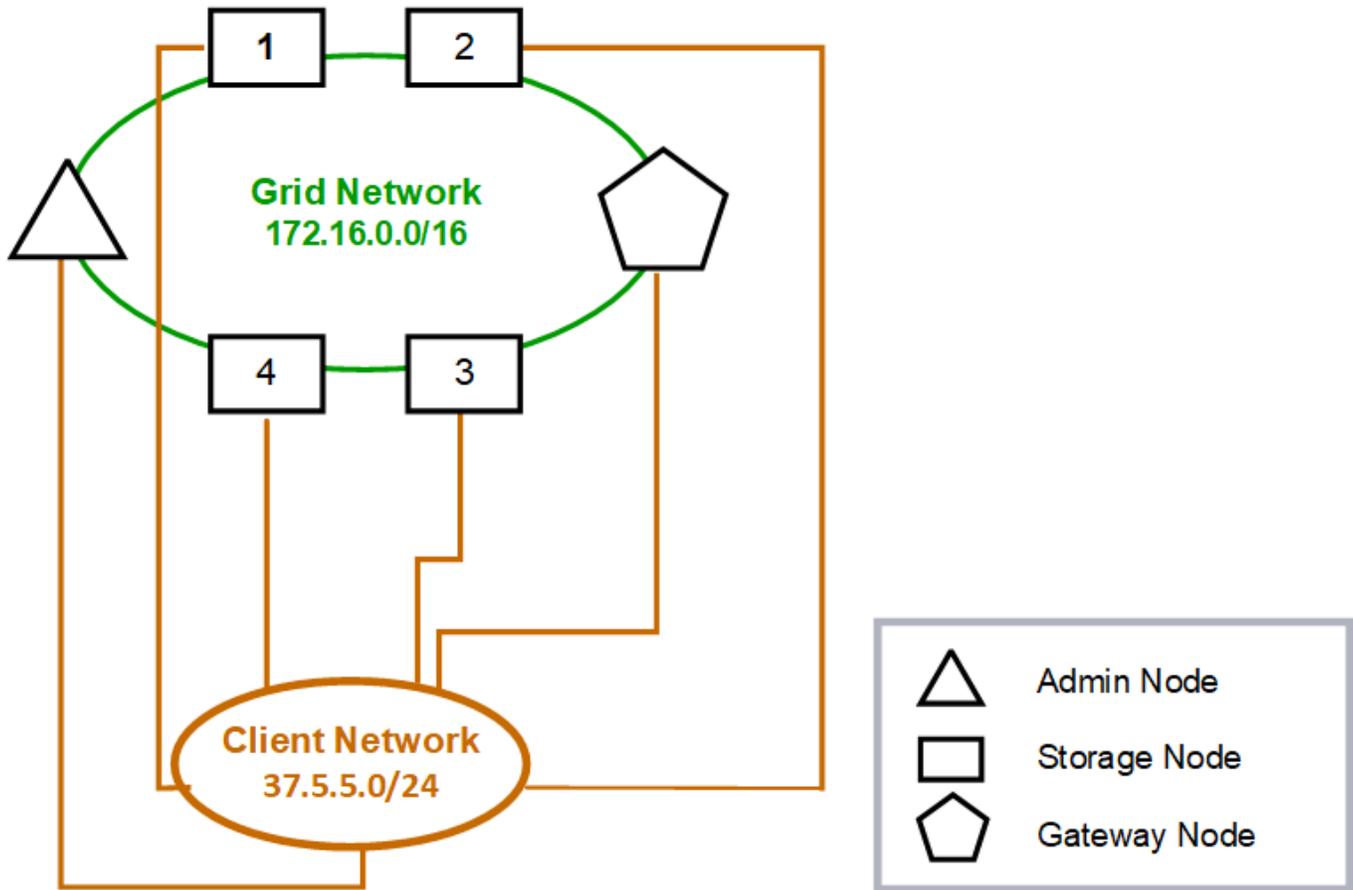
Wenn Sie das Client-Netzwerk konfigurieren, stellen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth2-Schnittstelle für den konfigurierten Node fest. Das Client-Netzwerk jedes Knotens kann unabhängig vom Client-Netzwerk auf jedem anderen Knoten sein.

Wenn Sie während der Installation ein Client-Netzwerk für einen Node konfigurieren, wechselt das Standard-Gateway des Node vom Grid Network Gateway zum Client Network Gateway, wenn die Installation abgeschlossen ist. Wenn später ein Client-Netzwerk hinzugefügt wird, wechselt das Standard-Gateway des Node auf die gleiche Weise.

In diesem Beispiel wird das Client-Netzwerk für S3- und Swift-Client-Anforderungen sowie für administrative

Funktionen verwendet, während das Grid-Netzwerk internen Objektmanagementvorgängen zugewiesen ist.

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	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

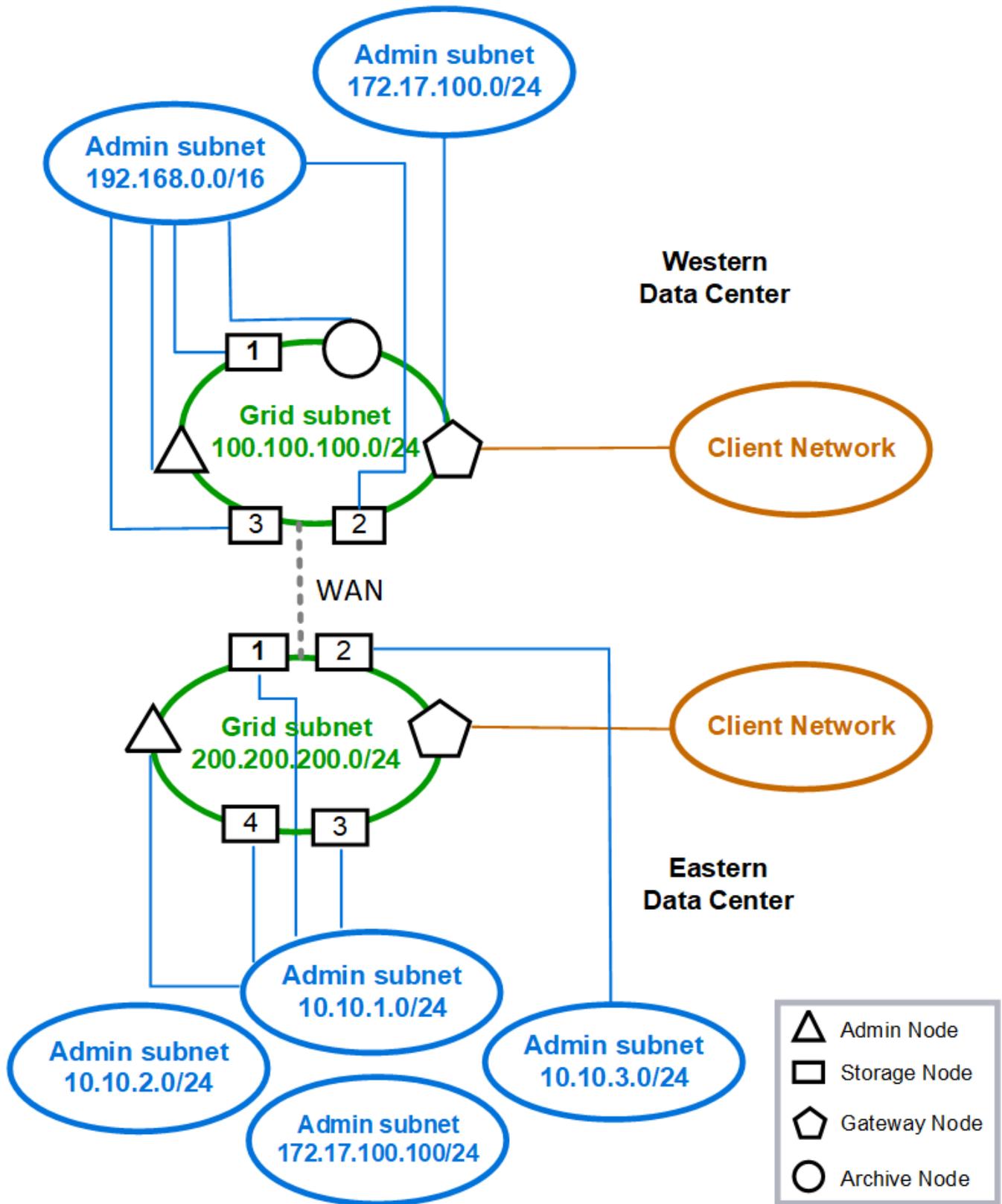
Topologie für alle drei Netzwerke

Sie können alle drei Netzwerke in einer Netzwerktopologie konfigurieren, die aus einem privaten Grid-Netzwerk, eingeschränkten 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 Netzwerkdatenverkehr verwendet, der mit internen Objektmanagementvorgängen in Verbindung steht.
- Das Admin-Netzwerk wird für den Datenverkehr in Verbindung mit administrativen Funktionen verwendet.
- Das Client-Netzwerk wird für Datenverkehr verwendet, der mit S3- und Swift-Client-Anforderungen verbunden ist.

Topology example: Grid, Admin, and Client Networks



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 die Grid-, Admin- oder Client-Netzwerke oder die Kombinationen dieser Netzwerke erfolgen, wie in den Beispielen der Netzwerktopologie dargestellt.

- **Management Connections:** Eingehende Verbindungen von einem Administrator zum Knoten, normalerweise über SSH. Zugriff über einen Webbrowser auf den Grid Manager, den Mandantenmanager und das Installationsprogramm der StorageGRID-Appliance.
- * NTP-Serververbindungen*: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.
Mindestens ein NTP-Server muss über den primären Admin-Node erreichbar sein.
- **DNS-Serververbindungen:** Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.
- **LDAP/Active Directory-Serververbindungen:** Ausgehende TCP-Verbindung vom Identitätsservice auf Speicherknoten.
- **AutoSupport:** Ausgehende TCP-Verbindung von den Admin-Knoten zu entweder `support.netapp.com` Oder einen vom Kunden konfigurierten Proxy.
- **Externer Schlüsselverwaltungsserver:** Ausgehende TCP-Verbindung von jedem Appliance-Knoten mit aktivierter Node-Verschlüsselung.
- Eingehende TCP-Verbindungen von S3 und Swift Clients.
- Ausgehende Anforderungen von StorageGRID Plattform-Services wie CloudMirror Replizierung oder von Cloud-Storage-Pools.

Wenn StorageGRID keinen der bereitgestellten NTP- oder DNS-Server unter Verwendung der standardmäßigen Routing-Regeln kontaktieren kann, versucht es automatisch, in allen Netzwerken (Grid, Admin und Client) Kontakt aufzunehmen, solange die IP-Adressen der DNS- und NTP-Server angegeben sind. Wenn die NTP- oder DNS-Server in einem Netzwerk erreicht werden können, erstellt StorageGRID automatisch zusätzliche Routingregeln, um sicherzustellen, dass das Netzwerk für alle zukünftigen Verbindungsversuche verwendet wird.



Obwohl Sie diese automatisch ermittelten Host-Routen verwenden können, sollten Sie die DNS- und NTP-Routen manuell konfigurieren, um die Verbindung zu gewährleisten, falls die automatische Erkennung fehlschlägt.

Wenn Sie während der Bereitstellung 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 Change IP-Tool konfigurieren (siehe "[Konfigurieren Sie IP-Adressen](#)").

Nur S3- und Swift-Client-Verbindungen sowie SSH-, Grid Manager- und Mandanten-Manager-Administratorverbindungen werden über VLAN-Schnittstellen unterstützt. Outbound-Verbindungen, z. B. zu NTP-, DNS-, LDAP-, AutoSupport- und KMS-Servern, muss die Client-, Admin- oder Grid-Netzwerkschnittstellen direkt überführen. Wenn die Schnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, fließt dieser Datenverkehr über das native VLAN der Schnittstelle, wie es am

Switch konfiguriert ist.

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/s in jeder Richtung aufweisen, bevor der Client-Datenverkehr berücksichtigt wird. Datenreplizierung oder Erasure Coding zwischen Standorten, Erweiterung von Nodes oder Standorten, Recovery von Nodes und anderen Vorgängen oder Konfigurationen erfordern zusätzliche Bandbreite.

Die tatsächlichen Anforderungen an die WAN-Mindestbandbreite hängen von der Client-Aktivität und dem ILM-Schutzschema ab. Wenden Sie sich an Ihren NetApp Professional Services Berater, um die Mindestanforderungen an die WAN-Bandbreite einschätzen zu können.

Verbindungen für Admin-Nodes und Gateway-Nodes

Admin-Knoten müssen immer von nicht vertrauenswürdigen Clients, wie denen im offenen Internet, gesichert werden. Sie müssen sicherstellen, dass kein nicht vertrauenswürdiger Client auf einen beliebigen Admin-Node im Grid-Netzwerk, auf das Admin-Netzwerk oder auf das Client-Netzwerk zugreifen kann.

Admin-Nodes und Gateway-Nodes, die Sie zu Hochverfügbarkeitsgruppen hinzufügen möchten, müssen mit einer statischen IP-Adresse konfiguriert werden. Weitere Informationen finden Sie unter "[Management von Hochverfügbarkeitsgruppen](#)".

Verwendung von NAT (Network Address Translation)

Verwenden Sie keine Network Address Translation (NAT) im Grid-Netzwerk zwischen Grid-Knoten oder zwischen StorageGRID-Standorten. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt routingfähig sein. Sie können jedoch bei Bedarf NAT zwischen externen Clients und Grid-Nodes verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway Node bereitzustellen. Die Verwendung von NAT zur Brücke eines öffentlichen Netzwerksegments wird nur unterstützt, wenn Sie eine Tunneling-Anwendung verwenden, die für alle Knoten im Netz transparent ist. Das bedeutet, dass die Grid-Knoten keine Kenntnisse über öffentliche IP-Adressen benötigen.

Netzwerkspezifische Anforderungen

Befolgen Sie die Anforderungen für jeden StorageGRID Netzwerktyp.

Netzwerk-Gateways und -Router

- Wenn gesetzt, muss sich das Gateway für ein bestimmtes Netzwerk im Subnetz des spezifischen Netzwerks befinden.
- Wenn Sie eine Schnittstelle mit statischer Adresse konfigurieren, müssen Sie eine andere Gateway-Adresse als 0.0.0.0 angeben.
- Wenn Sie kein Gateway haben, sollten Sie die Gateway-Adresse als IP-Adresse der Netzwerkschnittstelle festlegen.

Subnetze



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

Die folgenden Einschränkungen werden während der Bereitstellung durch den Grid Manager durchgesetzt. Sie werden hier zur Unterstützung bei der Netzwerkplanung vor der Implementierung bereitgestellt.

- Die Subnetzmaske für eine beliebige Netzwerk-IP-Adresse darf nicht 255.255.255.254 oder 255.255.255.255 sein (/31 oder /32 in CIDR-Notation).
- Das Subnetz, das durch eine IP-Adresse der Netzwerkschnittstelle und eine Subnetzmaske (CIDR) definiert ist, kann das Subnetz einer anderen Schnittstelle, die auf demselben Knoten konfiguriert ist, nicht überlappen.
- Das Grid-Netzwerk-Subnetz für jeden Node muss in der GNSL enthalten sein.
- Das Subnetz Admin Network darf sich nicht mit dem Subnetz Grid Network, dem Subnetz Client Network oder einem Subnetz im GNSL überlappen.
- Die Subnetze im AESL dürfen sich nicht mit Subnetzen im GNSL überlappen.
- Das Client-Netzwerk-Subnetz darf sich nicht mit dem Subnetz des Grid-Netzwerks, dem Subnetz des Admin-Netzwerks, einem beliebigen Subnetz im GNSL oder einem beliebigen Subnetz im AESL überlappen.

Grid-Netzwerk

- Bei der Bereitstellung muss jeder Grid-Node mit dem Grid-Netzwerk verbunden sein und mit dem primären Admin-Node über die bei der Bereitstellung des Node angegebene Netzwerkkonfiguration kommunizieren können.
- Während normaler Grid-Vorgänge muss jeder Grid-Node in der Lage sein, über das Grid-Netzwerk mit allen anderen Grid-Nodes zu kommunizieren.



Das Grid-Netzwerk muss direkt zwischen jedem Knoten routingfähig sein. Network Address Translation (NAT) zwischen Knoten wird nicht unterstützt.

- Wenn das Grid-Netzwerk aus mehreren Subnetzen besteht, fügen Sie sie der Grid Network Subnet List (GNSL) hinzu. Für jedes Subnetz in der GNSL werden auf allen Knoten statische Routen erstellt.
- Wenn die Grid-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, muss das Trunk-native VLAN das VLAN sein, das für Grid-Netzwerk-Traffic verwendet wird. Über das native Trunk-VLAN muss auf alle Grid-Nodes zugegriffen werden können.

Admin-Netzwerk

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

Typische Verwendungszwecke des Admin-Netzwerks sind Managementverbindungen, 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 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 aus externen Subnetzen zu aktivieren. Für jedes Subnetz in der AESL werden automatisch statische Routen auf jedem Knoten erzeugt.

Client-Netzwerk

Das Client-Netzwerk ist optional. Wenn Sie ein Client-Netzwerk konfigurieren möchten, beachten Sie die folgenden Überlegungen.

- Das Client Network unterstützt Datenverkehr von S3 und Swift Clients. Wenn konfiguriert, wird das Client-Netzwerk-Gateway zum Standard-Gateway des Node.
- Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Load Balancer-Endpunkten akzeptieren. Siehe "[Konfigurieren von Load Balancer-Endpunkten](#)".
- Wenn die Client-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, sollten Sie prüfen, ob die Konfiguration der Client-Netzwerkschnittstelle (eth2) erforderlich ist. Wenn konfiguriert, wird der Client-Netzwerk-Datenverkehr über das native Trunk-VLAN geleitet, wie es im Switch konfiguriert ist.

Implementierungs-spezifische Netzwerküberlegungen

Linux Implementierungen

Das StorageGRID System wird unter Linux als Sammlung von Container-Engines ausgeführt, um Effizienz, Zuverlässigkeit und Sicherheit zu gewährleisten. Die Container-Engine-bezogene Netzwerkkonfiguration ist bei einem StorageGRID System nicht erforderlich.

Verwenden Sie für die Container-Netzwerkschnittstelle ein Gerät ohne Bindung, z. B. ein VLAN- oder ein virtuelles Ethernet-Paar (Veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Node-Konfigurationsdatei an.



Verwenden Sie keine Bond- oder Bridge-Geräte direkt als Container-Netzwerkschnittstelle. Dies könnte den Start von Knoten verhindern, weil ein Kernel-Problem mit der Verwendung von macvlan mit Bond- und Bridge-Geräten im Container-Namespace vorliegt.

Siehe Installationsanweisungen für "[Red hat Enterprise Linux oder CentOS](#)" Oder "[Ubuntu oder Debian](#)" Implementierungen.

Hostnetzwerkkonfiguration für Container-Engine-Implementierungen

Bevor Sie Ihre StorageGRID-Implementierung auf einer Container-Engine-Plattform starten, ermitteln Sie, welche Netzwerke (Grid, Administrator, Client) jeder Node verwenden wird. Sie müssen sicherstellen, dass die Netzwerkschnittstelle jedes Node auf der richtigen virtuellen oder physischen Host-Schnittstelle konfiguriert ist und dass jedes Netzwerk über ausreichende Bandbreite verfügt.

Physische Hosts

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

- Stellen Sie sicher, dass alle Hosts für jede Node-Schnittstelle dieselbe Host-Schnittstelle verwenden. Diese Strategie vereinfacht die Host-Konfiguration und ermöglicht die zukünftige Node-Migration.
- Beziehen Sie eine IP-Adresse für den physischen Host selbst.



Eine physische Schnittstelle auf dem Host kann vom Host selbst und von einem oder mehreren Nodes verwendet werden, die auf dem Host ausgeführt werden. Alle IP-Adressen, die dem Host oder Knoten über diese Schnittstelle zugewiesen sind, müssen eindeutig sein. Der Host und der Node können keine IP-Adressen gemeinsam nutzen.

- Öffnen Sie die erforderlichen Ports zum Host.
- Wenn Sie beabsichtigen, VLAN-Schnittstellen in StorageGRID zu verwenden, 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 in den Node-Container übergeben werden. Informationen zum Hinzufügen von Trunk- oder Access-Schnittstellen finden Sie unter:
 - **RHEL oder CentOS (vor dem Installieren des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **Ubuntu oder Debian (vor der Installation des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens):** ["Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)

Empfehlungen für die minimale Bandbreite

Die folgende Tabelle enthält die Empfehlungen für die minimale LAN-Bandbreite für jeden StorageGRID-Node-Typ und jeden Netzwerktyp. Sie müssen jeden physischen oder virtuellen Host mit ausreichender Netzwerkbandbreite bereitstellen, um die Mindestanforderungen an die Bandbreite für das Aggregat für die Gesamtzahl und den Typ der StorageGRID Nodes, die auf diesem Host ausgeführt werden sollen, zu erfüllen.

Node-Typ	Netzwerktyp		
	Raster	Admin	Client
	Minimale LAN-Bandbreite	Admin	10 Gbit/S
1 Gbit/S	1 Gbit/S	Gateway	10 Gbit/S
1 Gbit/S	10 Gbit/S	Storage	10 Gbit/S
1 Gbit/S	10 Gbit/S	Archivierung	10 Gbit/S



Diese Tabelle enthält keine SAN-Bandbreite, die für den Zugriff auf Shared Storage erforderlich ist. Wenn Sie gemeinsam genutzten Storage verwenden, auf den Sie über Ethernet (iSCSI oder FCoE) zugreifen können, sollten Sie separate physische Schnittstellen für jeden Host bereitstellen, um ausreichend SAN-Bandbreite zur Verfügung zu stellen. Um einen Engpass zu vermeiden, sollte die SAN-Bandbreite für einen bestimmten Host in etwa der aggregierten Storage Node-Netzwerkbandbreite für alle Storage Nodes, die auf diesem Host ausgeführt werden, entsprechen.

Mithilfe der Tabelle können Sie die Mindestanzahl an Netzwerkschnittstellen bestimmen, die für jeden Host bereitgestellt werden sollen. Diese basieren auf der Anzahl und dem Typ der StorageGRID Nodes, die Sie auf diesem Host ausführen möchten.

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

- Verbinden Sie die Grid- und Admin-Netzwerke auf dem Admin-Node (erfordert $10 + 1 = 11$ Gbit/s).
- Verbinden der Grid- und Client-Netzwerke auf dem Gateway-Node (erfordert $10 + 10 = 20$ Gbit/s)
- Verbinden des Grid-Netzwerks mit dem Storage-Node (erfordert 10 Gbit/s)

In diesem Szenario sollten Sie mindestens $11 + 20 + 10 = 41$ GBit/s Netzwerkbandbreite angeben, Dies konnte von zwei 40 Gbps Schnittstellen oder fünf 10 Gbps Schnittstellen erreicht werden, die möglicherweise in Trunks aggregiert und dann von den drei oder mehr VLANs, die die Grid-, Admin- und Client-Subnetze lokal zum physischen Rechenzentrum mit dem Host übertragen, gemeinsam genutzt werden.

Einige empfohlene Möglichkeiten zur Konfiguration physischer und Netzwerkressourcen auf den Hosts in Ihrem StorageGRID Cluster zur Vorbereitung der StorageGRID-Bereitstellung finden Sie im folgenden:

- ["Konfiguration des Host-Netzwerks \(Red hat Enterprise Linux oder CentOS\)"](#)
- ["Konfigurieren des Hostnetzwerks \(Ubuntu oder Debian\)"](#)

Networking und Ports für Plattform-Services und Cloud Storage-Pools

Wenn Sie Vorhaben, StorageGRID Plattform-Services oder Cloud-Storage-Pools zu verwenden, müssen Sie Grid-Netzwerke und Firewalls konfigurieren, um sicherzustellen, dass die Ziel-Endpunkte erreicht werden können.

Networking für Plattform-Services

Wie in beschrieben ["Management von Plattform-Services für Mandanten"](#) Und ["Was sind Plattform-Services?"](#), Plattform-Services umfassen externe Services, die Integration von Suchvorgängen, Ereignisbenachrichtigung und CloudMirror Replikation bieten.

Plattform-Services benötigen Zugriff von Storage-Nodes, die den StorageGRID ADC-Service für die externen Service-Endpunkte hosten. Beispiele für die Bereitstellung des Zugriffs:

- Konfigurieren Sie auf den Speicherknoten mit ADC-Diensten eindeutige Admin-Netzwerke mit AESL-Einträgen, die zu den Ziel-Endpunkten weiterleiten.
- Verlassen Sie sich auf die Standardroute, die von einem Client-Netzwerk bereitgestellt wird. Wenn Sie die Standardroute verwenden, können Sie die verwenden ["Nicht vertrauenswürdige Client-Netzwerkfunktion"](#) So beschränken Sie eingehende Verbindungen.

Netzwerk für Cloud-Storage-Pools

Cloud-Storage-Pools erfordern außerdem Zugriff von Storage-Nodes auf die Endpunkte, die durch einen externen Service wie Amazon S3 Glacier oder Microsoft Azure Blob Storage bereitgestellt werden. Weitere Informationen finden Sie unter ["Was ist ein Cloud-Storage-Pool?"](#).

Ports für Plattform-Services und Cloud-Storage-Pools

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

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

Ein anderer Port kann angegeben werden, wenn der Endpunkt erstellt oder bearbeitet wird. Siehe ["Referenz für Netzwerk-Ports"](#).

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch ["Konfigurieren Sie Speicher-Proxy-Einstellungen"](#) Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

VLANs und Plattform-Services und Cloud-Storage-Pools

VLAN-Netzwerke können nicht für Plattformservices oder Cloud Storage-Pools verwendet werden. Die Zielpunkte müssen über das Raster, den Administrator oder das Client-Netzwerk erreichbar sein.

Appliance-Nodes

Die Netzwerk-Ports auf StorageGRID Applikationen können so konfiguriert werden, dass die Port Bond-Modi verwendet werden, die den Anforderungen an Durchsatz, Redundanz und Failover entsprechen.

Die 10/25-GbE-Ports auf den StorageGRID Appliances können im Bond-Modus „Fest“ oder „Aggregat“ für Verbindungen zum Grid-Netzwerk und zum Client-Netzwerk konfiguriert werden.

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

Weitere Informationen zu den Port-Bond-Modi Ihrer Appliance finden Sie unter:

- ["Port-Bond-Modi \(SGF6112\)"](#)
- ["Port-Bond-Modi \(SG6000-CN-Controller\)"](#)
- ["Port-Bond-Modi \(E5700SG Controller\)"](#)
- ["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 Node-Bereitstellung und der Grid-Konfiguration verwendet werden.

Erste Implementierung eines Node

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

Ein Grid-Netzwerk mit einem konfigurierten Gateway wird während der Bereitstellung zum Standard-Gateway für einen Node. Das Standard-Gateway ermöglicht Grid-Knoten in separaten Subnetzen, mit dem primären Admin-Node zu kommunizieren, bevor das Grid konfiguriert wurde.

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

Automatische Knotenregistrierung mit primärem Admin-Node

Nach der Bereitstellung der Nodes registrieren sie sich mit dem primären Admin-Node über das Grid-Netzwerk. Sie können dann den Grid Manager verwenden, das `configure-storagegrid.py` Python-Skript

oder die Installations-API, um das Grid zu konfigurieren und die registrierten Nodes zu genehmigen. Während der Grid-Konfiguration können Sie mehrere Grid-Subnetze konfigurieren. Beim Abschluss der Grid-Konfiguration werden auf jedem Knoten statische Routen zu diesen Subnetzen über das Grid-Netzwerk-Gateway erstellt.

Deaktivieren des Admin-Netzwerks oder des Client-Netzwerks

Wenn Sie das Admin-Netzwerk oder das Client-Netzwerk deaktivieren möchten, können Sie die Konfiguration während des Node-Genehmigungsprozesses von ihnen entfernen oder das Change IP-Tool verwenden, nachdem die Installation abgeschlossen ist (siehe "[Konfigurieren Sie IP-Adressen](#)").

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Implementierung und Konfiguration des Grid-Node die folgenden Richtlinien für DHCP-Adressen und Änderungen der Netzwerkkonfiguration.

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

Sie können DHCP nur während der Bereitstellungsphase einrichten. DHCP kann während der Konfiguration nicht eingerichtet werden.



Nodes werden neu gebootet, wenn sich ihre IP-Adressen ändern. Dies kann zu Ausfällen führen, wenn sich eine DHCP-Adresse gleichzeitig auf mehrere Nodes auswirkt.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmaske und Standard-Gateways für einen Grid-Node ändern möchten. Siehe "[Konfigurieren Sie IP-Adressen](#)".
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, geht die Client-Verbindung zum primären Admin-Node und anderen Grid-Nodes unter Umständen verloren. Je nach den vorgenommenen Änderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Referenz für Netzwerk-Ports

Sie müssen sicherstellen, dass die Netzwerkinfrastruktur interne und externe Kommunikation zwischen Knoten innerhalb des Grid und externen Clients und Services ermöglicht. Möglicherweise benötigen Sie Zugriff über interne und externe Firewalls, Switching-Systeme und Routing-Systeme.

Verwenden Sie die Details für "[Interne Kommunikation mit Grid-Nodes](#)" Und "[Externe Kommunikation](#)" Um zu bestimmen, wie die einzelnen erforderlichen Ports konfiguriert werden.

Interne Kommunikation mit Grid-Nodes

Die interne StorageGRID Firewall ermöglicht eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk. Verbindungen werden auch an Ports akzeptiert, die durch Load Balancer-Endpunkte definiert wurden.



NetApp empfiehlt, ICMP (Internet Control Message Protocol)-Datenverkehr zwischen den Grid-Knoten zu aktivieren. Wenn ICMP-Datenverkehr zugelassen wird, kann die Failover-Performance verbessert werden, 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 IP-Protokoll Nummer 112 verwendet. StorageGRID verwendet VRRP nur im Unicast-Modus. VRRP ist nur erforderlich, wenn ["Hochverfügbarkeitsgruppen"](#) Werden konfiguriert.

Richtlinien für Linux-basierte Knoten

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf einen dieser Ports einschränken, können Sie Ports während der Bereitstellung mithilfe eines Konfigurationsparameters neu zuordnen. Weitere Informationen über die Zuordnung von Ports und die Konfigurationsparameter für die Bereitstellung finden Sie unter:

- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)

Richtlinien für VMware-basierte Nodes

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

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf eine dieser Ports einschränken, können Sie bei der Implementierung von Nodes mit dem VMware vSphere Web Client Ports neu zuordnen oder bei der Automatisierung der Grid Node-Bereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen über die Zuordnung von Ports und die Konfigurationsparameter für die Bereitstellung finden Sie unter ["VMware installieren"](#).

Richtlinien für Appliance-Nodes

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf eine dieser Ports einschränken, können Sie Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Siehe ["Optional: Netzwerkports für Appliance neu zuordnen"](#).

Interne StorageGRID-Ports

Port	TCP oder UDP	Von	Bis	Details
22	TCP	Primärer Admin-Node	Alle Nodes	Bei Wartungsarbeiten muss der primäre Admin-Node mit SSH am Port 22 mit allen anderen Nodes kommunizieren können. Das Aktivieren von SSH-Datenverkehr von anderen Nodes ist optional.
80	TCP	Appliances	Primärer Admin-Node	Verwendet von StorageGRID-Appliances, um mit dem primären Admin-Knoten zu kommunizieren, um die Installation zu starten.
123	UDP	Alle Nodes	Alle Nodes	Netzwerkzeitprotokolldienst. Jeder Node synchronisiert seine Zeit mithilfe von NTP mit jedem anderen Node.
443	TCP	Alle Nodes	Primärer Admin-Node	Wird zur Kommunikation des Status an den primären Admin-Knoten während der Installation und anderen Wartungsverfahren verwendet.

Port	TCP oder UDP	Von	Bis	Details
1055	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
1139	TCP	Storage-Nodes	Storage-Nodes	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Nodes	Storage-Nodes mit ADC	Reporting-, Audit- und Konfigurationsdatenverkehr.
1502	TCP	Alle Nodes	Storage-Nodes	Interner S3- und Swift-Datenverkehr.
1504	TCP	Alle Nodes	Admin-Nodes	NMS-Service-Berichterstellung und interner Datenverkehr bei der Konfiguration.
1505	TCP	Alle Nodes	Admin-Nodes	AMS-Dienst internen Verkehr.
1506	TCP	Alle Nodes	Alle Nodes	Serverstatus interner Datenverkehr.
1507	TCP	Alle Nodes	Gateway-Nodes	Interner Datenverkehr des Load Balancer:
1508	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr im Konfigurationsmanagement.
1509	TCP	Alle Nodes	Archiv-Nodes	Interner Datenverkehr des Archivierungs-Knotens.
1511	TCP	Alle Nodes	Storage-Nodes	Interner Metadaten-Datenverkehr:
7001	TCP	Storage-Nodes	Storage-Nodes	Cassandra TLS zwischen Nodes-Cluster-Kommunikation
7443	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
8443	TCP	Primärer Admin-Node	Appliance-Nodes	Interner Datenverkehr im Zusammenhang mit dem Wartungsmodus.

Port	TCP oder UDP	Von	Bis	Details
9042	TCP	Storage-Nodes	Storage-Nodes	Cassandra-Client-Port:
9999	TCP	Alle Nodes	Alle Nodes	Interner Datenverkehr für mehrere Dienste. Beinhaltet Wartungsvorgänge, Kennzahlen und Netzwerk-Updates.
10226	TCP	Storage-Nodes	Primärer Admin-Node	Wird von StorageGRID Appliances verwendet, um AutoSupport Meldungen von E-Series SANtricity System Manager an den primären Admin-Node weiterzuleiten.
10342	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
11139	TCP	Archivierung /Storage-Nodes	Archivierung /Storage-Nodes	Interner Datenverkehr zwischen Speicherknoten und Archivknoten.
18000	TCP	Admin/Storage-Nodes	Storage-Nodes mit ADC	Kontodienst, interner Datenverkehr.
18001	TCP	Admin/Storage-Nodes	Storage-Nodes mit ADC	Interner Datenverkehr der Identitätsföderation.
18002	TCP	Admin/Storage-Nodes	Storage-Nodes	Interner API-Traffic im Zusammenhang mit Objektprotokollen.
18003	TCP	Admin/Storage-Nodes	Storage-Nodes mit ADC	Plattform Dienste internen Traffic.
18017	TCP	Admin/Storage-Nodes	Storage-Nodes	Interner Datenverkehr des Data Mover-Service für Cloud-Speicherpools.
18019	TCP	Storage-Nodes	Storage-Nodes	Interner Traffic beim Chunk-Service für Erasure Coding.
18082	TCP	Admin/Storage-Nodes	Storage-Nodes	Interner S3-Datenverkehr.
18083	TCP	Alle Nodes	Storage-Nodes	Swift-bezogener interner Traffic:

Port	TCP oder UDP	Von	Bis	Details
18086	TCP	Alle Grid-Nodes	Alle Storage-Nodes	Interner Datenverkehr im Zusammenhang mit dem LDR-Dienst.
18200	TCP	Admin/Storage-Nodes	Storage-Nodes	Weitere Statistiken zu Client-Anforderungen.
19000	TCP	Admin/Storage-Nodes	Storage-Nodes mit ADC	Keystone-Service: Interner Datenverkehr.

Verwandte Informationen

["Externe Kommunikation"](#)

Externe Kommunikation

Die Clients müssen mit den Grid-Nodes kommunizieren, um Inhalte aufzunehmen und abzurufen. Die verwendeten Ports hängen von den ausgewählten Objekt-Storage-Protokollen ab. Diese Ports müssen dem Client zugänglich sein.

Eingeschränkter Zugriff auf Ports

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf beliebige Ports einschränken, können Sie dies verwenden ["Load Balancer-Endpunkte"](#) Um den Zugriff auf benutzerdefinierte Ports zu erlauben. Sie können dann verwenden ["Nicht vertrauenswürdige Client-Netzwerke"](#) Um den Zugriff nur auf Endpunkt-Ports des Load Balancer zu erlauben.

Port-Neuzuordnung

Um Systeme und Protokolle wie SMTP, DNS, SSH oder DHCP verwenden zu können, müssen Sie beim Implementieren von Nodes Ports neu zuordnen. Sie sollten jedoch die Load Balancer-Endpunkte nicht neu zuordnen. Informationen zur Port-Neuzuordnung finden Sie in den Installationsanweisungen:

- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)
- ["VMware installieren"](#)
- ["Optional: Netzwerkports für Appliance neu zuordnen"](#)

Anschlüsse für externe Kommunikation

In der folgenden Tabelle werden die Ports für den Datenverkehr zu den Nodes aufgeführt.



Diese Liste enthält keine Ports, die als konfiguriert werden können ["Load Balancer-Endpunkte"](#) Oder verwendet für ["Syslog-Server"](#).

Port	TCP oder UDP	Protokoll	Von	Bis	Details
22	TCP	SSH	Service-Laptop	Alle Nodes	Für Verfahren mit Konsolenschritten ist ein SSH- oder Konsolenzugriff erforderlich. Optional können Sie statt 22 auch Port 2022 verwenden.
25	TCP	SMTP	Admin-Nodes	E-Mail-Server	Wird für Warnungen und E-Mail-basierte AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 über die Seite „E-Mail-Server“ außer Kraft setzen.
53	TCP/UDP	DNS	Alle Nodes	DNS-Server	Wird für DNS verwendet.
67	UDP	DHCP	Alle Nodes	DHCP-Service	Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für statisch konfigurierte Grids ausgeführt.
68	UDP	DHCP	DHCP-Service	Alle Nodes	Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für Raster ausgeführt, die statische IP-Adressen verwenden.
80	TCP	HTTP	Browser	Admin-Nodes	Port 80 wird für die Admin-Node-Benutzeroberfläche an Port 443 umgeleitet.
80	TCP	HTTP	Browser	Appliances	Port 80 wird für das Installationsprogramm der StorageGRID-Appliance an Port 8443 umgeleitet.
80	TCP	HTTP	Storage-Nodes mit ADC	AWS	Wird für Plattform-Services-Meldungen verwendet, die an AWS oder andere externe Services gesendet werden, die HTTP verwenden. Mandanten können bei der Erstellung eines Endpunkts die Standard-HTTP-Porteinstellung von 80 außer Kraft setzen.
80	TCP	HTTP	Storage-Nodes	AWS	An AWS Ziele mit HTTP gesendete Anfragen von Cloud-Storage-Pools Grid-Administratoren können die Standard-HTTP-Port-Einstellung von 80 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
111	TCP/UDP	Rpcbind	NFS Client	Admin-Nodes	<p>Wird vom NFS-basierten Audit-Export verwendet (Portmap).</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist.</p>
123	UDP	NTP	Primäre NTP-Knoten	Externe NTP	<p>Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Nodes synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.</p>
137	UDP	NetBIOS	SMB-Client	Admin-Nodes	<p>Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist.</p>
138	UDP	NetBIOS	SMB-Client	Admin-Nodes	<p>Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist.</p>
139	TCP	SMB	SMB-Client	Admin-Nodes	<p>Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist.</p>
161	TCP/UDP	SNMP	SNMP-Client	Alle Nodes	<p>Wird für SNMP-Abfrage verwendet. Alle Knoten stellen grundlegende Informationen zur Verfügung; Admin Nodes stellen auch Alarm- und Alarmdaten zur Verfügung. Standardmäßig auf UDP-Port 161 gesetzt, wenn konfiguriert.</p> <p>Hinweis: dieser Port ist nur erforderlich und wird nur auf der Knoten-Firewall geöffnet, wenn SNMP konfiguriert ist. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.</p> <p>Hinweis: um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.</p>

Port	TCP oder UDP	Protokoll	Von	Bis	Details
162	TCP/UDP	SNMP-Benachrichtigungen	Alle Nodes	Benachrichtigungsziele	<p>Ausgehende SNMP-Benachrichtigungen und Traps standardmäßig auf UDP-Port 162.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn SNMP aktiviert ist und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.</p> <p>Hinweis: um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.</p>
389	TCP/UDP	LDAP	Storage-Nodes mit ADC	Active Directory/LDAP	Wird zur Verbindung mit einem Active Directory- oder LDAP-Server für Identity Federation verwendet.
443	TCP	HTTPS	Browser	Admin-Nodes	<p>Wird von Webbrowsern und Management-API-Clients für den Zugriff auf Grid Manager und Tenant Manager verwendet.</p> <p>Hinweis: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port angeschlossen sind, einschließlich Ihnen, den Zugriff auf den Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt. Siehe "Konfigurieren Sie die Firewall-Steuer-elemente" So konfigurieren Sie privilegierte IP-Adressen:</p>
443	TCP	HTTPS	Admin-Nodes	Active Directory	Wird von Admin-Nodes verwendet, die eine Verbindung zu Active Directory herstellen, wenn Single Sign-On (SSO) aktiviert ist.
443	TCP	HTTPS	Archiv-Nodes	Amazon S3	Wird für den Zugriff von Archiv-Nodes auf Amazon S3 verwendet.
443	TCP	HTTPS	Storage-Nodes mit ADC	AWS	Wird für Plattform-Services-Nachrichten verwendet, die an AWS oder andere externe Services gesendet werden, die HTTPS verwenden. Mandanten können bei der Erstellung eines Endpunkts die Standard-HTTP-Porteinstellung von 443 außer Kraft setzen.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
443	TCP	HTTPS	Storage-Nodes	AWS	Cloud-Storage-Pools-Anfragen werden an AWS-Ziele mit HTTPS gesendet. Grid-Administratoren können die HTTPS-Porteinstellung von 443 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen.
445	TCP	SMB	SMB-Client	Admin-Nodes	Wird vom SMB-basierten Audit-Export verwendet. Hinweis: dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist.
903	TCP	NFS	NFS Client	Admin-Nodes	Wird vom NFS-basierten Audit-Export verwendet (<code>rpc.mountd</code>). Hinweis: dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist.
2022	TCP	SSH	Service-Laptop	Alle Nodes	Für Verfahren mit Konsolenschritten ist ein SSH- oder Konsolenzugriff erforderlich. Optional können Sie statt 2022 auch Port 22 verwenden.
2049	TCP	NFS	NFS Client	Admin-Nodes	Wird vom NFS-basierten Audit-Export verwendet (<code>nfs</code>). Hinweis: dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist.
5353	UDP	MDNS	Alle Nodes	Alle Nodes	Stellt den Multicast-DNS-Service (mDNS) bereit, der für vollständige IP-Änderungen am Grid und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird.
5696	TCP	KMIP	Appliance	KMS	KMIP (Key Management Interoperability Protocol): Externer Datenverkehr von Appliances, die für die Node-Verschlüsselung auf den Verschlüsselungsmanagement-Server (Key Management Interoperability Protocol) konfiguriert sind, es sei denn, ein anderer Port wird auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer angegeben.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
8022	TCP	SSH	Service-Laptop	Alle Nodes	SSH auf Port 8022 gewährt Zugriff auf das Betriebssystem auf Appliance- und virtuellen Node-Plattformen zur Unterstützung und Fehlerbehebung. Dieser Port wird nicht für Linux-basierte (Bare Metal-)Nodes verwendet und muss nicht zwischen Grid-Nodes oder während des normalen Betriebs zugänglich sein.
8443	TCP	HTTPS	Browser	Admin-Nodes	<p>Optional Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann zur Trennung der Kommunikation zwischen Grid Manager und Tenant Manager verwendet werden.</p> <p>Hinweis: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port angeschlossen sind, einschließlich Ihnen, den Zugriff auf den Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt. Siehe "Konfigurieren Sie die Firewall-Steuerelemente" So konfigurieren Sie privilegierte IP-Adressen:</p>
9022	TCP	SSH	Service-Laptop	Appliances	Gewährt Zugriff auf StorageGRID Appliances im Vorkonfigurationsmodus für Support und Fehlerbehebung. Dieser Port muss während des normalen Betriebs nicht zwischen Grid-Nodes oder auf diesen zugreifen können.
9091	TCP	HTTPS	Externer Grafana-Service	Admin-Nodes	<p>Wird von externen Grafana Services für sicheren Zugriff auf den StorageGRID Prometheus Service verwendet.</p> <p>Hinweis: dieser Port wird nur benötigt, wenn der zertifikatbasierte Prometheus-Zugriff aktiviert ist.</p>
9443	TCP	HTTPS	Browser	Admin-Nodes	Optional Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Mandanten-Manager verwendet. Kann zur Trennung der Kommunikation zwischen Grid Manager und Tenant Manager verwendet werden.
18082	TCP	HTTPS	S3-Clients	Storage-Nodes	S3-Client-Datenverkehr direkt zu Storage-Nodes (HTTPS).

Port	TCP oder UDP	Protokoll	Von	Bis	Details
18083	TCP	HTTPS	Swift Clients	Storage-Nodes	Schneller Client-Verkehr direkt zu Storage Nodes (HTTPS).
18084	TCP	HTTP	S3-Clients	Storage-Nodes	S3-Client-Traffic direkt zu Storage-Nodes (HTTP).
18085	TCP	HTTP	Swift Clients	Storage-Nodes	Schneller Client-Verkehr direkt zu Storage Nodes (HTTP).
23000-23999	TCP	HTTPS	Alle Nodes im Quell-Grid für die Grid-übergreifende Replizierung	Admin Nodes und Gateway Nodes im Ziel-Grid für Grid-übergreifende Replizierung	Dieser Port-Bereich ist für Grid Federation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden den gleichen Port.

Schnellstart für StorageGRID

Führen Sie die folgenden allgemeinen Schritte aus, um jedes StorageGRID System zu konfigurieren und zu verwenden.

1

Lernen, Planen und Sammeln von Daten

Erläutern Sie Ihrem NetApp Ansprechpartner die Optionen und planen Sie Ihr neues StorageGRID System. Berücksichtigen Sie folgende Fragen:

- Wie viele Objektdaten werden Sie voraussichtlich anfänglich oder über einen längeren Zeitraum speichern?
- Wie viele Websites benötigen Sie?
- Wie viele und welche Arten von Nodes benötigen Sie an den einzelnen Standorten?
- Welche StorageGRID-Netzwerke verwenden Sie?
- Wer wird Ihr Raster zum Speichern von Objekten verwenden? Welche Applikationen werden verwendet?
- Haben Sie spezielle Anforderungen an die Sicherheit oder den Storage?
- Müssen Sie gesetzliche oder behördliche Anforderungen erfüllen?

Optional können Sie zusammen mit Ihrem NetApp Professional Services Berater auf das NetApp ConfigBuilder Tool zugreifen, um ein Konfigurationshandbuch für die Installation und Implementierung des neuen Systems auszufüllen. Mit diesem Tool können Sie auch die Konfiguration jeder StorageGRID Appliance automatisieren. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

Prüfen "[Weitere Informationen zu StorageGRID](#)" Und das "[Netzwerkrichtlinien](#)".

2

Installieren Sie Nodes

Ein StorageGRID System besteht aus individuellen Hardware- und softwarebasierten Nodes. Sie installieren zuerst die Hardware für jeden Appliance-Node und konfigurieren jeden Linux- oder VMware-Host.

Um die Installation abzuschließen, installieren Sie die StorageGRID Software auf jeder Appliance oder jedem Software-Host und verbinden die Nodes mit einem Grid. Während dieses Schritts geben Sie Standort- und Node-Namen, Subnetzdetails und die IP-Adressen für Ihre NTP- und DNS-Server an.

Mehr erfahren:

- ["Appliance-Hardware installieren"](#)
- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)
- ["VMware installieren"](#)

3

Melden Sie sich an und prüfen Sie den Systemzustand

Sobald Sie den primären Admin-Knoten installieren, 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-Endpunkt-Domännennamen einrichten.

Mehr erfahren:

- ["Melden Sie sich beim Grid Manager an"](#)
- ["Systemzustand überwachen"](#)
- ["Konfigurieren Sie AutoSupport"](#)
- ["Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"](#)
- ["Konfigurieren Sie die Domännennamen des S3-Endpunkts"](#)

4

Konfiguration und Management

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

Mehr erfahren:

- ["Kontrolle über den StorageGRID-Zugriff"](#)
- ["Verwenden Sie den S3-Einrichtungsassistenten"](#)
- ["Verwenden Sie den FabricPool-Einrichtungsassistenten"](#)
- ["Sicherheitsmanagement"](#)
- ["Systemhärtung"](#)

5

Richten Sie ILM ein

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 erklären StorageGRID, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien über einen längeren Zeitraum gemanagt werden.

Mehr erfahren: ["Objektmanagement mit ILM"](#)

6

Verwenden Sie StorageGRID

Nach Abschluss der Erstkonfiguration können StorageGRID-Mandantenkonten Objekte mithilfe von S3 und Swift-Client-Applikationen aufnehmen, abrufen und löschen.

Mehr erfahren:

- ["Verwenden Sie ein Mandantenkonto"](#)
- ["Verwenden der S3-REST-API"](#)
- ["Verwenden der Swift-REST-API"](#)

7

Monitoring und Fehlerbehebung

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

Mehr erfahren:

- ["Monitoring von StorageGRID"](#)
- ["Fehler bei StorageGRID beheben"](#)

8

Erweiterung und Wartung

Sie können Nodes oder Standorte hinzufügen, um die Kapazität oder Funktionalität Ihres Systems zu erweitern. Sie können zudem verschiedene Wartungsverfahren zur Wiederherstellung nach Ausfällen oder zur Aktualisierung und effizienten Performance Ihres StorageGRID Systems durchführen.

Mehr erfahren:

- ["Erweitern Sie Ihr Raster"](#)
- ["Stellen Sie Nodes wieder her und warten Sie das Grid"](#)

Installation und Upgrade

Appliance-Hardware installieren

Schnellstart für die Hardwareinstallation

Führen Sie diese grundlegenden Schritte aus, um eine StorageGRID Appliance zu installieren und einzurichten und als Node in Ihrem StorageGRID System zu implementieren.

1

Installation vorbereiten

1. Automatisieren Sie zusammen mit Ihrem NetApp Professional Services Berater die Installation und Konfiguration. Siehe ["Automatisierung der Appliance-Installation und -Konfiguration"](#).

Dieser Schritt ist optional. Durch die Optimierung und Automatisierung von Konfigurationsschritten können jedoch Zeit eingespart und die Konfiguration mehrerer Appliances konsistent sein.

2. ["Standort vorbereiten"](#)
3. ["Packen Sie die Kartons aus"](#)
4. ["Beschaffen Sie sich zusätzliche Geräte und Werkzeuge"](#)
5. ["Überprüfen Sie die Anforderungen des Webbrowsers"](#)
6. ["Überprüfen Sie die Appliance-Netzwerkverbindungen"](#)
7. ["Sammeln Sie Installationsinformationen"](#)

2

Hardware installieren

1. ["Hardware registrieren"](#)
2. In Schrank oder Rack installieren
 - ["SGF6112"](#)
 - ["SG6000"](#)
 - ["SG5700"](#)
 - ["SG100 und SG1000"](#)
3. Kabelgerät
 - ["SGF6112"](#)
 - ["SG6000"](#)
 - ["SG5700"](#)
 - ["SG100 und SG1000"](#)
4. Stromkabel anschließen und Strom anschließen
 - ["SGF6112"](#)
 - ["SG6000"](#)

- "SG5700"
- "SG100 und SG1000"

5. "Statusanzeigen und -Codes anzeigen"

3

Richten Sie die Hardware ein

Wenn Sie mehr als eine Appliance konfigurieren und implementieren, automatisieren Sie mit dem NetApp ConfigBuilder Tool die folgenden Konfigurations- und Implementierungsschritte. Entsprechende Anleitungen erhalten Sie von Ihrem NetApp Professional Services Consultant. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

1. Konfigurieren Sie StorageGRID-Verbindungen

- "[Rufen Sie das Installationsprogramm für StorageGRID-Appliances auf](#)" Und überprüfen Sie, ob Sie die neueste Version verwenden
- "[Netzwerkverbindungen konfigurieren](#)"
- "[Konfigurieren Sie StorageGRID-IP-Adressen](#)"
- "[Netzwerkverbindungen prüfen](#)"
- "[Überprüfen Sie Netzwerkverbindungen auf Portebene](#)"

2. "[Aufrufen und Konfigurieren von SANtricity System Manager](#)" (SG6000 und SG5700)

3. "[Konfigurieren Sie die BMC-Schnittstelle](#)" (SGF6112, SG6000, SG100 UND SG1000)

4. Führen Sie optionale Einrichtungsschritte durch

- "[Aktivieren Sie die Node-Verschlüsselung](#)"
- "[Ändern des RAID-Modus \(SG6000 und SG5700\)](#)"
- "[Netzwerkports neu zuordnen](#)"

4

Implementieren des Appliance-Node

Implementieren Sie die Appliance als neuen Node in Ihrem StorageGRID-System.

- "[Appliance-Storage-Node implementieren](#)"
- "[Implementieren des Services-Appliance-Nodes](#)"

Hardware-Übersichten

SGF6112 Appliance: Überblick

Die StorageGRID SGF6112 Appliance wird als Storage-Node in einem StorageGRID System ausgeführt. Die Appliance kann in einer hybriden Grid-Umgebung verwendet werden, die Appliance Storage Nodes und virtuelle (softwarebasierte) Storage-Nodes kombiniert.

Die Appliance SGF6112 bietet folgende Funktionen:

- 12 NVMe-SSD-Laufwerke (Nonvolatile Memory Express) mit integrierten Computing- und Storage-Controllern.

- Integriert die Storage- und Computing-Elemente für einen StorageGRID Storage Node.
- Umfasst das Installationsprogramm von StorageGRID Appliance zur Vereinfachung der Bereitstellung und Konfiguration von Storage-Nodes.
- Umfasst einen Baseboard Management Controller (BMC) zur Überwachung und Diagnose der Hardware im Compute Controller.
- Unterstützt bis zu vier 10-GbE- oder 25-GbE-Verbindungen mit dem StorageGRID-Grid-Netzwerk und dem Client-Netzwerk.

Hardwarebeschreibung der SGF6112

Bei der StorageGRID SGF6112 handelt es sich um eine rein Flash-basierte Appliance mit einem kompakten Design und einem Computing-Controller und einem Storage-Controller, der in ein 1-HE-Chassis integriert ist. Die Appliance unterstützt 12 SSD-NVMe-Laufwerke mit einer Speicherkapazität von bis zu 15.3 TB pro Laufwerk.

Ausfallsicherer Objekt-Storage

Das SGF6112 wurde mit SSDs in einem RAID konzipiert, das folgende Datensicherungsfunktionen bietet:

- Funktionsfähigkeit nach Ausfall einer einzelnen SSD ohne Beeinträchtigung der Objektverfügbarkeit.
- Funktionsfähigkeit nach Ausfällen mehrerer SSDs mit einer minimalen erforderlichen Reduzierung der Objektverfügbarkeit (basierend auf dem Design des zugrunde liegenden RAID-Schemas).
- Während der Wartung ist die vollständige Recovery bei SSD-Ausfällen möglich, die keine extremen Schäden am RAID-Gehäuse des Root-Volumens des Nodes (des StorageGRID-Betriebssystems) zur Folge haben.

Hardwarekomponenten der SGF6112

Die Appliance SGF6112 umfasst die folgenden Komponenten:

Komponente	Beschreibung
Computing- und Storage-Plattform	<p>Ein Server mit einer Höheneinheit (1 HE), der Folgendes umfasst:</p> <ul style="list-style-type: none"> • Zwei 165-W-Prozessoren mit 2.1/2.6 GHz und 48 Kernen • 256 GB RAM • 2 × 1/10 GBase-T-Ports • 4 × 10/25-GbE-Ethernet-Ports • 1 × 256 GB internes Startlaufwerk (einschließlich StorageGRID-Software) • Baseboard Management Controller (BMC) der das Hardware-Management vereinfacht • Redundante Netzteile und Lüfter

SGF6112-Diagramme

SGF6112 – Vorderansicht

Diese Abbildung zeigt die Vorderseite des SGF6112 ohne Blende. Die Appliance verfügt über eine 1-HE-Computing- und Storage-Plattform mit 12 SSD-Laufwerken.

SGF6112 – Rückansicht

Diese Abbildung zeigt die Rückseite des SGF6112, einschließlich der Ports, Lüfter und Netzteile.

Legende	Port	Typ	Nutzung
1	Netzwerkanschlüsse 1-4	10/25-GbE, basierend auf Kabel- oder SFP-Transceiver-Typ (SFP28- und SFP+-Module werden unterstützt), Switch-Geschwindigkeit und konfigurierter Link-Geschwindigkeit.	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.
2	BMC-Management-Port	1 GbE (RJ-45)	Stellen Sie eine Verbindung mit dem Management Controller der Hauptplatine des Geräts her.
3	Diagnose- und Supportports	<ul style="list-style-type: none">• VGA• USB• Micro-USB-Konsolenport• Micro-SD-Steckplatzmodul	Nur zur Verwendung durch technischen Support reserviert.
4	Admin-Netzwerkport 1	1/10-GbE (RJ-45)	Schließen Sie die Appliance an das Admin-Netzwerk für StorageGRID an.

Legende	Port	Typ	Nutzung
5	Admin – Netzwerkanschluss 2	1/10-GbE (RJ-45)	<p>Optionen:</p> <ul style="list-style-type: none"> • Verbindung mit Admin-Netzwerk-Port 1 für eine redundante Verbindung zum Admin-Netzwerk für StorageGRID. • Lassen Sie die Verbindung getrennt und für den vorübergehenden lokalen Zugriff verfügbar (IP 169.254.0.1). • Verwenden Sie während der Installation Port 2 für die IP-Konfiguration, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

SG6060 und SG6060X Appliances: Überblick

Die StorageGRID SG6060 und SG6060X Appliances umfassen jeweils einen Computing-Controller und ein Storage-Controller-Shelf, das zwei Storage Controller und 60 Laufwerke enthält.

Optional können beide Appliances mit Erweiterungs-Shelfs für 60 Laufwerke ergänzt werden. Es gibt keine Spezifikationen oder funktionalen Unterschiede zwischen dem SG6060 und SG6060X, außer der Position der Interconnect-Ports am Storage Controller.

Komponenten SG6060 und SG6060X

Die SG6060 und SG6060X Appliances umfassen die folgenden Komponenten:

Komponente	Beschreibung
Computing-Controller	<p>SG6000-CN-Controller, ein 1U-Server (1 Rack-Einheit) mit folgenden Komponenten:</p> <ul style="list-style-type: none"> • 40 Cores (80 Threads) • 192 GB RAM • Bis zu 4 × 25 Gbit/s aggregierte Ethernet-Bandbreite • FC-Interconnect mit 4 × 16 GBit/s • Baseboard Management Controller (BMC) der das Hardware-Management vereinfacht • Redundante Netzteile

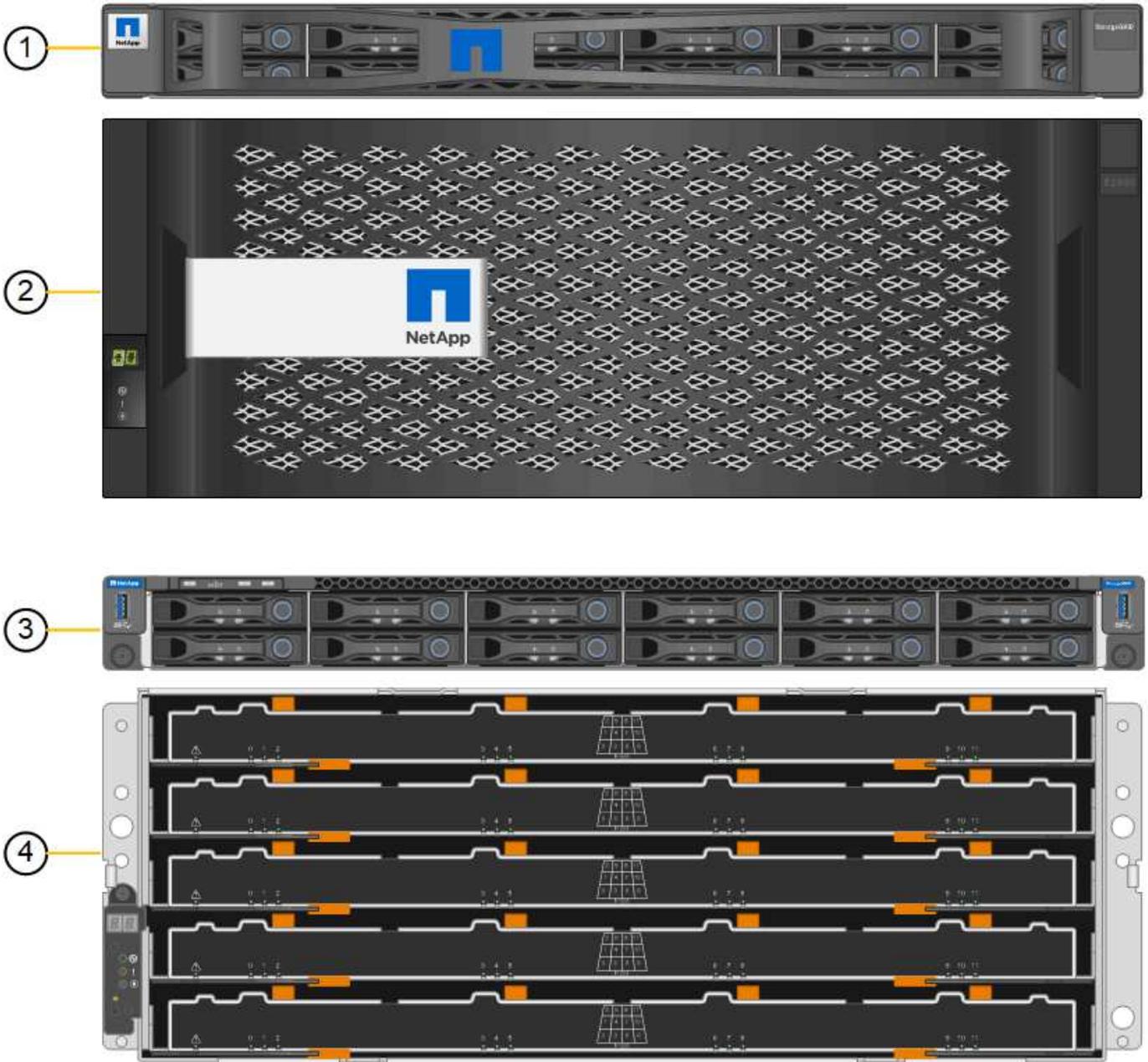
Komponente	Beschreibung
Storage Controller Shelf	<p>E-Series E2860 Controller-Shelf (Storage-Array), ein 4-HE-Shelf mit folgenden Komponenten:</p> <ul style="list-style-type: none"> • Zwei Controller der E2800 Serie (Duplexkonfiguration) für die Unterstützung von Storage Controller Failover <ul style="list-style-type: none"> ◦ Das SG6060 enthält E2800A Storage Controller ◦ Das SG6060X enthält E2800B Storage Controller • Shelf mit fünf Einschüben für Festplatten mit 60 3.5-Zoll-Laufwerken (2 Solid State-Laufwerke bzw. SSDs und 58 NL-SAS-Laufwerke) • Redundante Netzteile und Lüfter
<p>Optional: Storage-Erweiterungs-Shelfs</p> <p>Hinweis: Erweiterungseinschübe können bei der ersten Implementierung installiert oder später hinzugefügt werden.</p>	<p>E-Series DE460C Gehäuse, ein 4-HE-Shelf mit folgenden Komponenten:</p> <ul style="list-style-type: none"> • Zwei Eingangs-/Ausgangsmodule (IOMs) • Fünf Schubladen mit jeweils 12 NL-SAS-Laufwerken für insgesamt 60 Laufwerke • Redundante Netzteile und Lüfter <p>Jede SG6060 und SG6060X Appliance kann über ein oder zwei Erweiterungs-Shelfs für insgesamt 180 Laufwerke verfügen (zwei dieser Laufwerke sind für den E-Series Lese-Cache reserviert).</p>

Diagramme SG6060 und SG6060X

Die Fronten des SG6060 und des SG6060X sind identisch.

Vorderansicht des SG6060 oder SG6060X

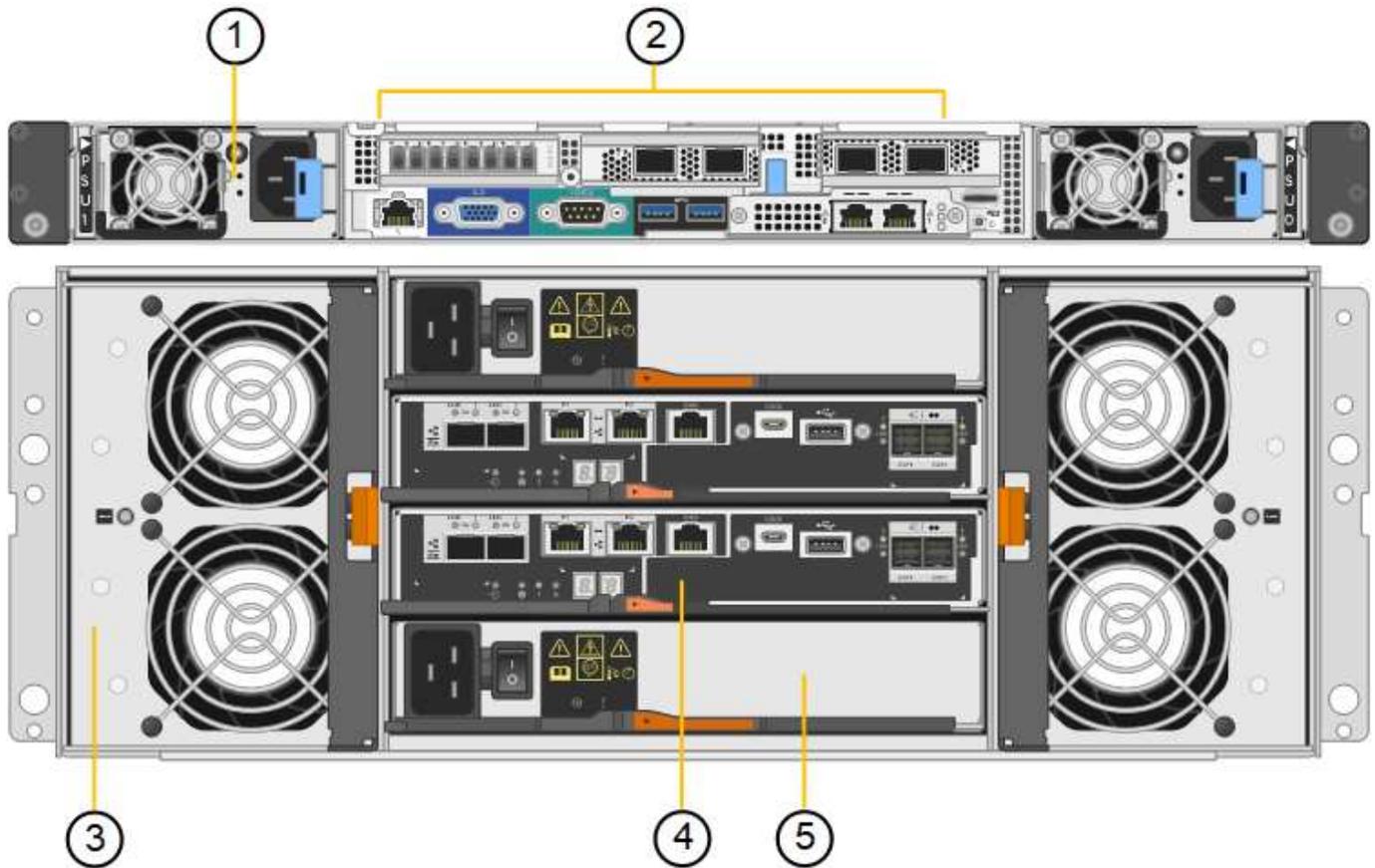
Diese Abbildung zeigt die Vorderseite des SG6060 oder SG6060X, der einen 1-HE-Computing-Controller und ein 4-HE-Shelf mit zwei Storage-Controllern und 60 Laufwerken in fünf Laufwerkseinschüben umfasst.



Legende	Beschreibung
1	SG6000-CN Computing Controller mit Frontblende
2	E2860 Controller-Shelf mit Frontblende (optionales Erweiterungs-Shelf erscheint identisch)
3	SG6000-CN Computing Controller mit abnehmbarer Frontblende
4	E2860 Controller-Shelf mit entfernter Frontblende (optionales Erweiterungs-Shelf erscheint identisch)

SG6060 – Rückansicht

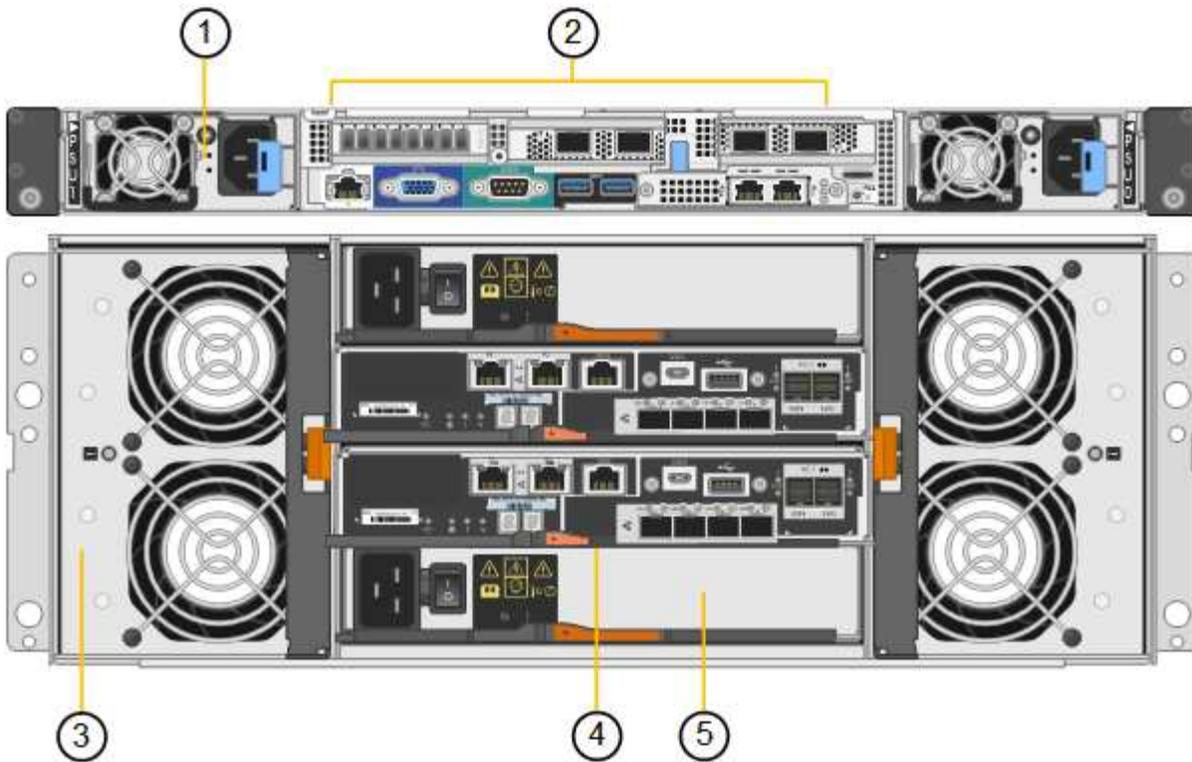
Diese Abbildung zeigt die Rückseite des SG6060, einschließlich der Computing- und Storage-Controller, Lüfter und Netzteile.



Legende	Beschreibung
1	Netzteil (1 von 2) für SG6000-CN Compute Controller
2	Anschlüsse für SG6000-CN Compute Controller
3	Lüfter (1 von 2) für E2860 Controller-Shelf
4	E-Series E2800A Storage-Controller (1 von 2) und Anschlüsse
5	Netzteil (1 von 2) für E2860 Controller-Shelf

SG6060X – Rückansicht

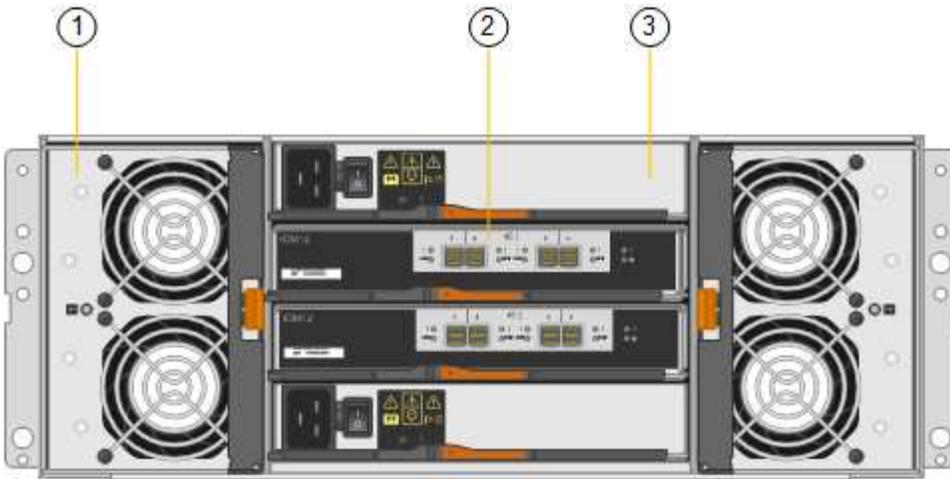
Diese Abbildung zeigt die Rückseite des SG6060X.



Legende	Beschreibung
1	Netzteil (1 von 2) für SG6000-CN Compute Controller
2	Anschlüsse für SG6000-CN Compute Controller
3	Lüfter (1 von 2) für E2860 Controller-Shelf
4	E-Series E2800B Storage-Controller (1 von 2) und Anschlüsse
5	Netzteil (1 von 2) für E2860 Controller-Shelf

Erweiterungs-Shelf

Diese Abbildung zeigt die Rückseite des optionalen Erweiterungs-Shelfs für SG6060 und SG6060X, einschließlich der ein-/Ausgabemodule (IOMs), Lüfter und Netzteile. Jeder SG6060 kann mit einem oder zwei Erweiterungs-Shelfs installiert werden. Dies kann bei der Erstinstallation oder einem späteren Zeitpunkt hinzugefügt werden.



Legende	Beschreibung
1	Lüfter (1 von 2) für Erweiterungs-Shelf
2	IOM (1 von 2) für Erweiterungs-Shelf
3	Netzteil (1 von 2) für Erweiterungs-Shelf

SG6000 Controller

Jedes Modell der StorageGRID SG6000 Appliance umfasst je nach Modell einen SG6000-CN Computing Controller in einem 1-HE-Gehäuse und E-Series Duplex Storage-Controller in einem 2-HE- oder 4-HE-Gehäuse. In den Diagrammen erfahren Sie mehr über die einzelnen Controller-Typen.

SG6000-CN Computing-Controller

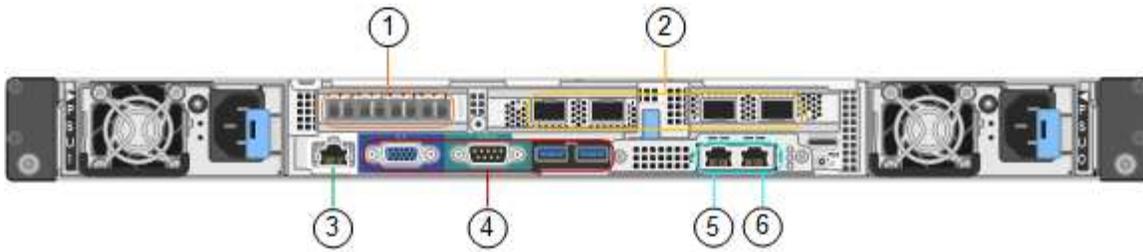
- Stellt für die Appliance Computing-Ressourcen bereit
- Schließt das Installationsprogramm für StorageGRID-Appliance ein.



Die StorageGRID-Software ist auf der Appliance nicht vorinstalliert. Diese Software wird beim Bereitstellen der Appliance vom Admin-Node abgerufen.

- Es kann eine Verbindung zu allen drei StorageGRID-Netzwerken hergestellt werden, einschließlich dem Grid-Netzwerk, dem Admin-Netzwerk und dem Client-Netzwerk.
- Stellt eine Verbindung zu den E-Series Storage Controllern her und arbeitet als Initiator.

SG6000-CN-Anschlüsse

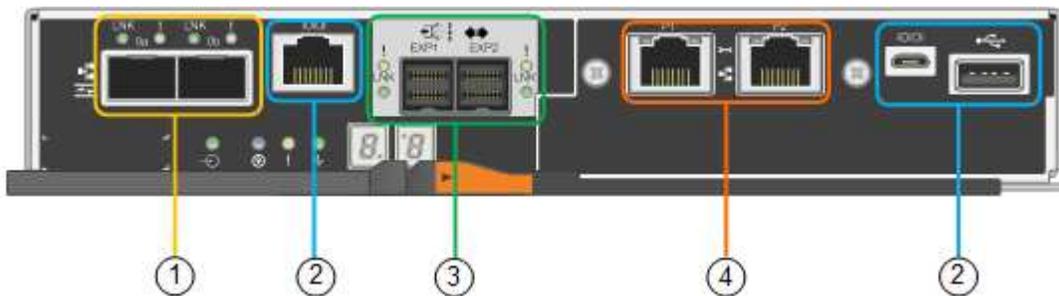


Legende	Port	Typ	Nutzung
1	Interconnect-Ports 1-4	16 Gbit/s Fibre Channel (FC) mit integrierter Optik	Verbinden Sie den SG6000-CN Controller mit den E2800 Controllern (zwei Verbindungen zu jedem E2800).
2	Netzwerkanschlüsse 1-4	10-GbE oder 25-GbE auf Basis von Kabel- oder SFP-Transceiver, Switch-Geschwindigkeit und konfigurierter Verbindungsgeschwindigkeit	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.
3	BMC-Management-Port	1 GbE (RJ-45)	Stellen Sie eine Verbindung mit dem SG6000-CN Baseboard Management Controller her.
4	Diagnose- und Supportports	<ul style="list-style-type: none"> • VGA • Seriell, 115200 8-N-1 • USB 	Nur zur Verwendung durch technischen Support reserviert.
5	Admin-Netzwerkport 1	1 GbE (RJ-45)	Verbinden Sie das SG6000-CN mit dem Admin-Netzwerk für StorageGRID.
6	Admin – Netzwerkanschluss 2	1 GbE (RJ-45)	Optionen: <ul style="list-style-type: none"> • Verbindung mit Management-Port 1 für eine redundante Verbindung zum Admin-Netzwerk für StorageGRID. • Lassen Sie nicht verdrahtet und für den vorübergehenden lokalen Zugang verfügbar (IP 169.254.0.1). • Verwenden Sie während der Installation Port 2 für die IP-Konfiguration, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

SGF6024 – EF570 Storage-Controller

- Zwei Controller für Failover-Support.
- Verwalten Sie den Speicher der Daten auf den Laufwerken.
- Funktion als standardmäßige E-Series Controller in einer Duplexkonfiguration.
- Schließen Sie die SANtricity OS Software (Controller-Firmware) an.
- Enthalten ist SANtricity System Manager für die Überwachung der Storage-Hardware und für das Warnmanagement, die AutoSupport Funktion und die Laufwerksicherheitsfunktion.
- Stellen Sie eine Verbindung zum SG6000-CN-Controller her und ermöglichen Sie den Zugriff auf den Flash-Speicher.

EF570 Connector



Legende	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	Optischer 16-Gbit/s-FC-SFP	Verbinden Sie jeden EF570 Controller mit dem SG6000-CN Controller. Es sind vier Verbindungen zum SG6000-CN Controller vorhanden (zwei von jedem EF570).
2	Diagnose- und Supportports	<ul style="list-style-type: none"> • Serieller RJ-45-Anschluss • Serieller Micro-USB-Anschluss • USB-Anschluss 	Nur zur Verwendung durch technischen Support reserviert.
3	Ports zur Laufwerkserweiterung	12 GB/s SAS	Nicht verwendet. Die SGF6024 Appliance unterstützt keine Festplatten-Shelfs zur Erweiterung.
4	Management-Ports 1 und 2	1-GB-Ethernet (RJ-45)	<ul style="list-style-type: none"> • Port 1 stellt eine Verbindung zum Netzwerk her, in dem Sie in einem Browser auf SANtricity System Manager zugreifen. • Port 2 ist für den technischen Support reserviert.

SG6060 und SG6060X: E2800 Storage-Controller

- Zwei Controller für Failover-Support.
- Verwalten Sie den Speicher der Daten auf den Laufwerken.
- Funktion als standardmäßige E-Series Controller in einer Duplexkonfiguration.
- Schließen Sie die SANtricity OS Software (Controller-Firmware) an.
- Enthalten ist SANtricity System Manager für die Überwachung der Storage-Hardware und für das Warnmanagement, die AutoSupport Funktion und die Laufwerksicherheitsfunktion.
- Stellen Sie eine Verbindung zum SG6000-CN-Controller her und ermöglichen Sie den Zugriff auf den Speicher.

Die SG6060 und SG6060X verwenden E2800 Storage-Controller.

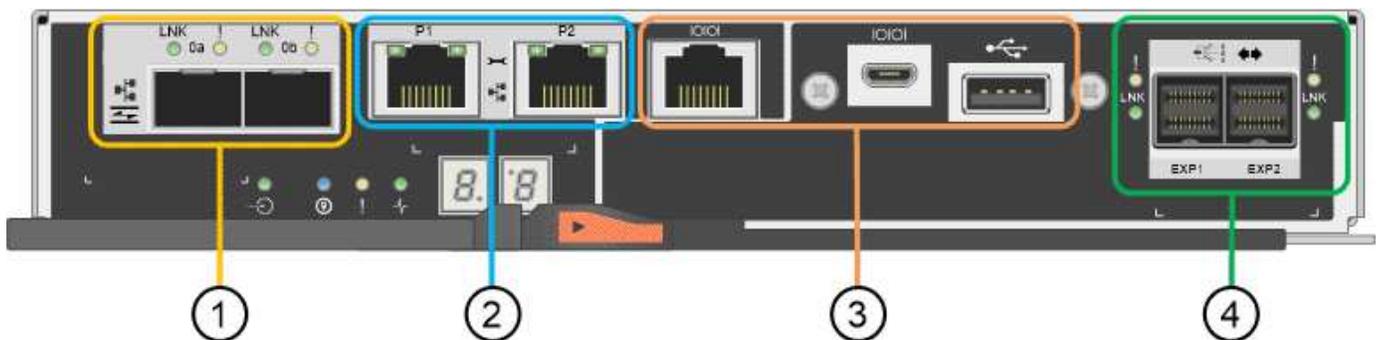
Appliance	Controller	Controller-HIC
SG6060	Zwei E2800A Storage Controller	Keine
SG6060X	Zwei E2800B Storage Controller	HIC mit vier Ports

Die E2800A und E2800B Storage Controller sind in den Spezifikationen und Funktionen identisch, außer an der Position der Interconnect-Ports.



Verwenden Sie kein E2800A und kein E2800B im selben Gerät.

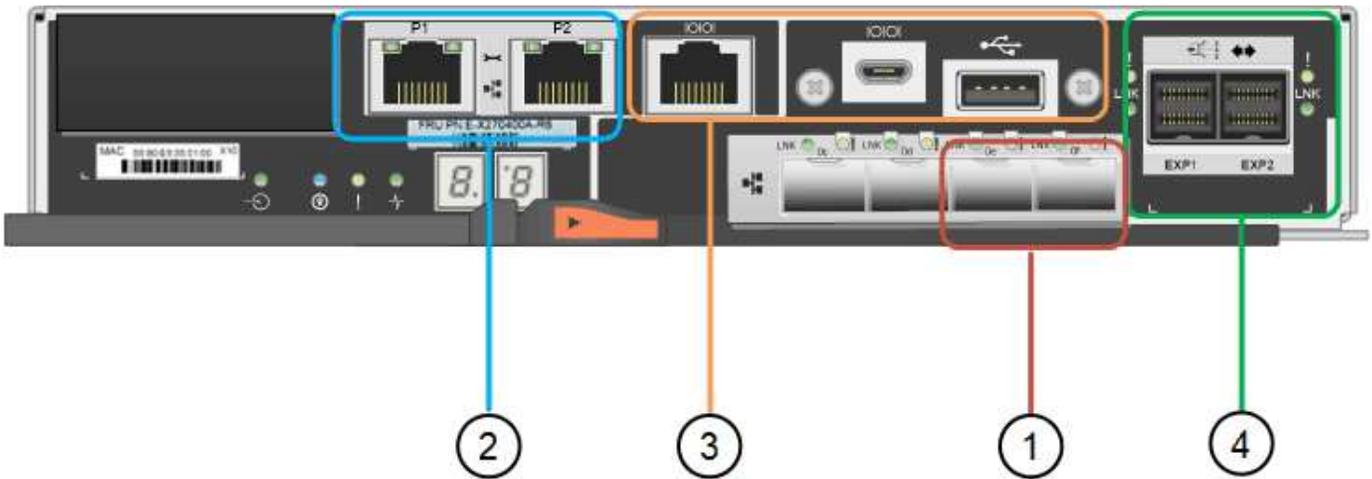
E2800A-Anschlüsse



Legende	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	Optischer 16-Gbit/s-FC-SFP	Schließen Sie alle E2800A-Controller an den SG6000-CN-Controller an. Es gibt vier Verbindungen zum SG6000-CN Controller (zwei von jedem E2800A).

Legende	Port	Typ	Nutzung
2	Management-Ports 1 und 2	1-GB-Ethernet (RJ-45)	<ul style="list-style-type: none"> • Port 1-Optionen: <ul style="list-style-type: none"> ◦ Stellen Sie eine Verbindung zu einem Managementnetzwerk her, um direkten TCP/IP-Zugriff auf SANtricity System Manager zu ermöglichen ◦ Lassen Sie die Kabel, um einen Switch-Port und eine IP-Adresse zu speichern. Greifen Sie über die Grid Manager- oder Speicher Grid Appliance Installer-UIs auf den SANtricity System Manager zu. <p>Hinweis: Einige optionale SANtricity-Funktionen, wie z.B. NTP Sync für genaue Log-Zeitstempel, sind nicht verfügbar, wenn Sie Port 1 unverdrahtet lassen.</p> <p>Hinweis: StorageGRID 11.5 oder höher und SANtricity 11.70 oder höher sind erforderlich, wenn Sie Port 1 unverdrahtet verlassen.</p> <ul style="list-style-type: none"> • Port 2 ist für den technischen Support reserviert.
3	Diagnose- und Supportports	<ul style="list-style-type: none"> • Serieller RJ-45-Anschluss • Serieller Micro-USB-Anschluss • USB-Anschluss 	Nur zur Verwendung durch technischen Support reserviert.
4	Festplattenerweiterungs-Ports 1 und 2	12 GB/s SAS	Verbinden Sie die Ports mit den Laufwerkserweiterungsports der IOMs im Erweiterungs-Shelf.

E2800B-Anschlüsse



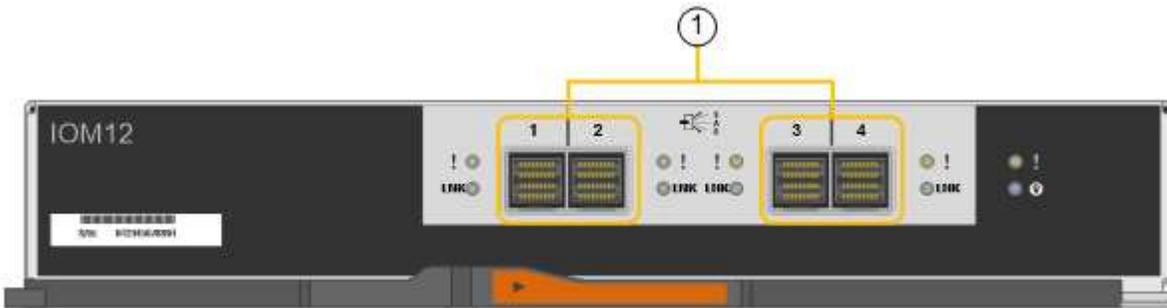
Legende	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	Optischer 16-Gbit/s-FC-SFP	<p>Schließen Sie alle E2800B-Controller an den SG6000-CN-Controller an.</p> <p>Es gibt vier Verbindungen zum SG6000-CN Controller (zwei von jedem E2800B).</p>
2	Management-Ports 1 und 2	1-GB-Ethernet (RJ-45)	<ul style="list-style-type: none"> • Port 1-Optionen: <ul style="list-style-type: none"> ◦ Stellen Sie eine Verbindung zu einem Managementnetzwerk her, um direkten TCP/IP-Zugriff auf SANtricity System Manager zu ermöglichen ◦ Lassen Sie die Kabel, um einen Switch-Port und eine IP-Adresse zu speichern. Greifen Sie über die Grid Manager- oder Speicher Grid Appliance Installer-UIs auf den SANtricity System Manager zu. <p>Hinweis: Einige optionale SANtricity-Funktionen, wie z.B. NTP Sync für genaue Log-Zeitstempel, sind nicht verfügbar, wenn Sie Port 1 unverdrahtet lassen.</p> <p>Hinweis: StorageGRID 11.5 oder höher und SANtricity 11.70 oder höher sind erforderlich, wenn Sie Port 1 unverdrahtet verlassen.</p> <ul style="list-style-type: none"> • Port 2 ist für den technischen Support reserviert.

Legende	Port	Typ	Nutzung
3	Diagnose- und Supportports	<ul style="list-style-type: none"> • Serieller RJ-45-Anschluss • Serieller Micro-USB-Anschluss • USB-Anschluss 	Nur zur Verwendung durch technischen Support reserviert.
4	Festplattenerweiterungs-Ports 1 und 2	12 GB/s SAS	Verbinden Sie die Ports mit den Laufwerkserweiterungsports der IOMs im Erweiterungs-Shelf.

SG6060 und SG6060X: IOMs für optionale Erweiterungs-Shelfs

Das Erweiterungs-Shelf enthält zwei I/O-Module (IOMs), die mit den Storage-Controllern oder anderen Erweiterungs-Shelfs verbunden sind.

IOM-Anschlüsse



Legende	Port	Typ	Nutzung
1	Ports zur Laufwerkserweiterung 1-4	12 GB/s SAS	Verbinden Sie die einzelnen Ports mit den Storage-Controllern oder mit einem zusätzlichen Erweiterungs-Shelf (falls vorhanden).

SG5700 Appliance: Überblick

Die SG5700 StorageGRID Appliance ist eine integrierte Storage- und Computing-Plattform, die als Storage-Node in einem StorageGRID Grid ausgeführt wird. Die Appliance kann in einer hybriden Grid-Umgebung verwendet werden, die Appliance Storage Nodes und virtuelle (softwarebasierte) Storage-Nodes kombiniert.

Die Appliance der StorageGRID SG5700 Serie bietet folgende Funktionen:

- Integrieren Sie die Storage- und Computing-Elemente für einen StorageGRID Storage Node.
- Schließen Sie das Installationsprogramm für StorageGRID Appliance an, um die Implementierung und Konfiguration von Storage-Nodes zu vereinfachen.
- Umfasst E-Series SANtricity System Manager für Hardware-Management und Monitoring.

- Unterstützung für bis zu vier 10-GbE- oder 25-GbE-Verbindungen mit dem StorageGRID-Grid-Netzwerk und dem Client-Netzwerk.
- Unterstützung für Full Disk Encryption (FDE)-Laufwerke oder FIPS-Laufwerke Wenn diese Laufwerke mit der Laufwerksicherheitsfunktion in SANtricity System Manager verwendet werden, wird ein nicht autorisierter Zugriff auf die Daten verhindert.

Das SG5700-Appliance ist in vier Modellen verfügbar: SG5712 und SG5712X sowie SG5760 und SG5760X. Es gibt keine Spezifikations- oder Funktionsunterschiede zwischen dem SG5712 und SG5712X außer der Lage der Interconnect-Ports auf dem Storage Controller. Ebenso gibt es keine Spezifikations- oder Funktionsunterschiede zwischen dem SG5760 und dem SG5760X, außer dem Standort der Interconnect Ports am Storage Controller.

SG5700 Komponenten

Die SG5700 Modelle umfassen die folgenden Komponenten:

Komponente	SG5712	SG5712X	SG5760	SG5760X
Computing-Controller	E5700SG Controller	E5700SG Controller	E5700SG Controller	E5700SG Controller
Storage Controller	E2800A-Controller	E2800B-Controller	E2800A-Controller	E2800B-Controller
Chassis	E-Series DE212C-Gehäuse, ein 2-HE-Gehäuse (Rack-Unit)	E-Series DE212C-Gehäuse, ein 2-HE-Gehäuse (Rack-Unit)	E-Series DE460C Gehäuse, ein 4-HE-Gehäuse (Rack-Unit)	E-Series DE460C Gehäuse, ein 4-HE-Gehäuse (Rack-Unit)
Laufwerke	12 NL-SAS-Laufwerke (3.5 Zoll)	12 NL-SAS-Laufwerke (3.5 Zoll)	60 NL-SAS-Laufwerke (3.5 Zoll)	60 NL-SAS-Laufwerke (3.5 Zoll)
Redundante Netzteile und Lüfter	Zwei Power-Fan-Kanister	Zwei Power-Fan-Kanister	Zwei Leistungskanister und zwei Lüfterkanister	Zwei Leistungskanister und zwei Lüfterkanister

Der maximale Rohkapazität, der in der StorageGRID-Appliance verfügbar ist, richtet sich nach der Anzahl der Laufwerke in jedem Gehäuse. Sie können den verfügbaren Speicher nicht erweitern, indem Sie ein Shelf mit zusätzlichen Laufwerken hinzufügen.

SG5700-Diagramme

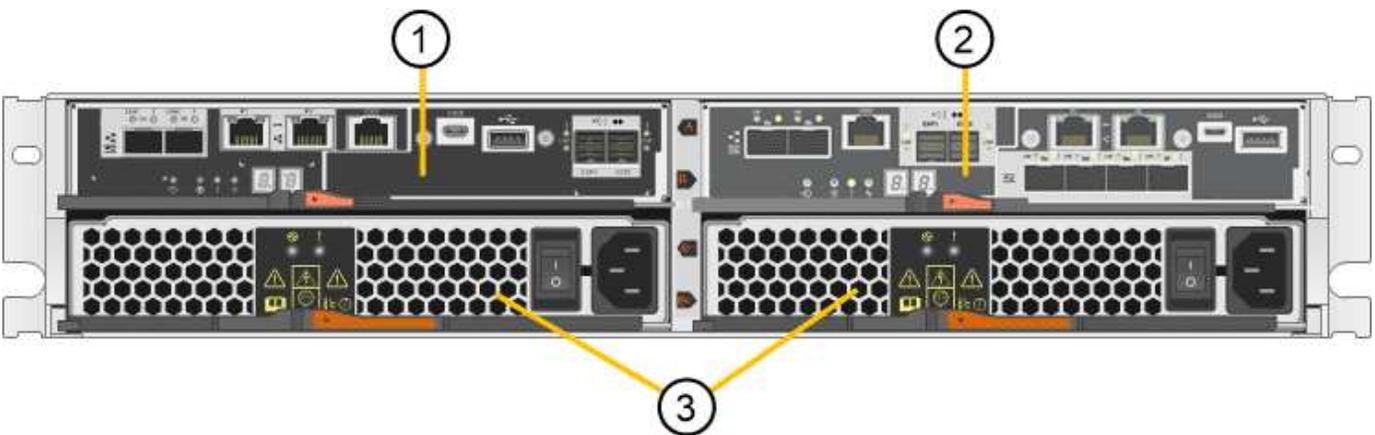
SG5712 Vorder- und Rückansicht

Die Abbildungen zeigen die Vorder- und Rückseite des SG5712, einem 2-HE-Gehäuse für 12 Laufwerke.



SG5712 Komponenten

Die SG5712 umfasst zwei Controller und zwei Power-Fan-Kanister.



Legende	Beschreibung
1	E2800A-Controller (Storage-Controller)
2	E5700SG Controller (Compute-Controller)
3	Power-Fan-Behälter

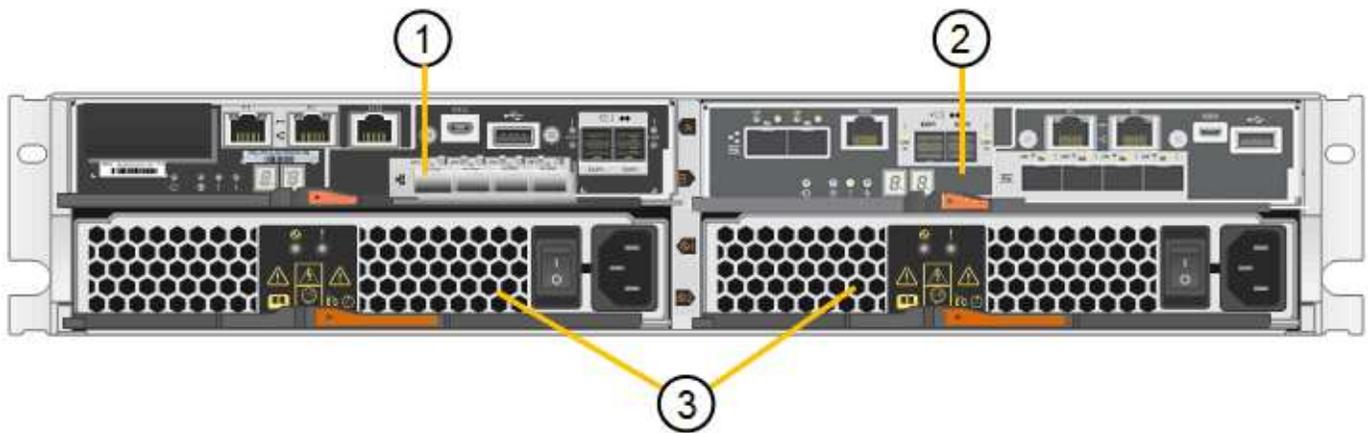
SG5712X Vorder- und Rückansicht

Die Abbildungen zeigen die Vorder- und Rückseite des SG5712X, einem 2U-Gehäuse für 12 Laufwerke.



SG5712X Komponenten

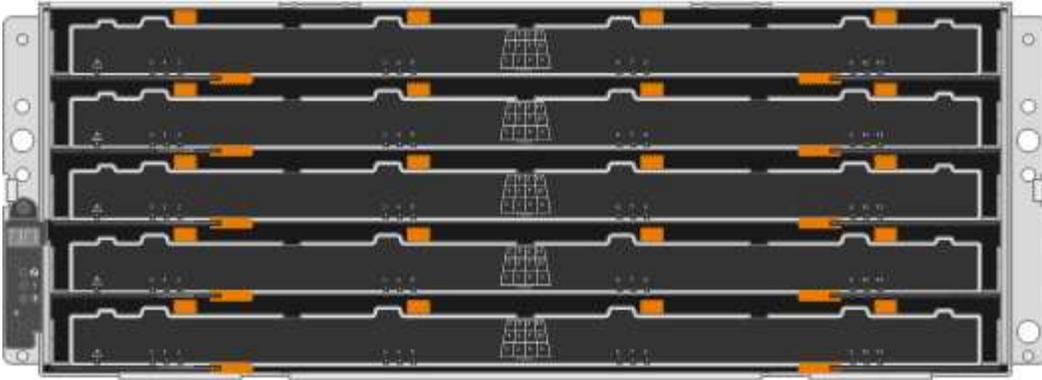
Das SG5712X besteht aus zwei Controllern und zwei Power-Fan-Kanistern.



Legende	Beschreibung
1	E2800B-Controller (Storage-Controller)
2	E5700SG Controller (Compute-Controller)
3	Power-Fan-Behälter

Vorder- und Rückansicht des SG5760

Die Abbildungen zeigen die Vorder- und Rückseite des SG5760-Modells, ein 4-HE-Gehäuse für 60 Laufwerke in 5 Laufwerkseinschüben.



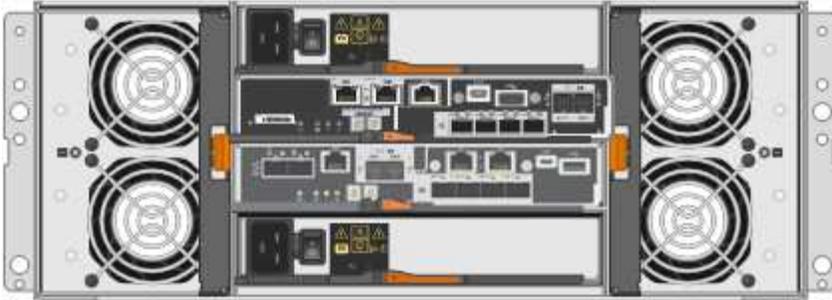
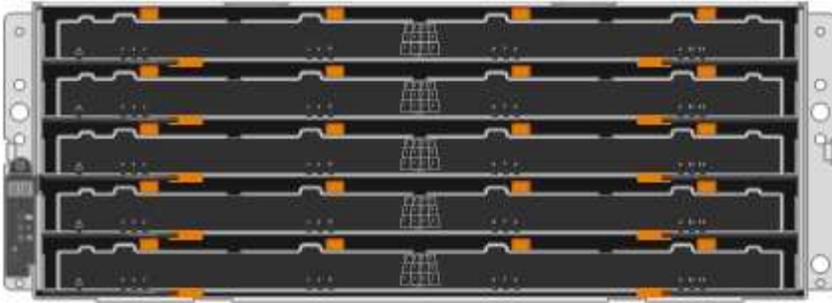
SG5760 Komponenten

Die SG5760 verfügt über zwei Controller, zwei Lüfterbehälter und zwei Strombehälter.

Legende	Beschreibung
1	E2800A-Controller (Storage-Controller)
2	E5700SG Controller (Compute-Controller)
3	Gebälsebehälter (1 von 2)
4	Leistungsbehälter (1 von 2)

SG5760X Vorder- und Rückansicht

Die Abbildungen zeigen die Vorder- und Rückseite des Modells SG5760X, einem 4U-Gehäuse, das 60 Laufwerke in 5 Laufwerkseinschüben aufnehmen kann.



SG5760X Komponenten

Die SG5760X enthält zwei Controller, zwei Lüfterzangen und zwei Leistungszangen.

Legende	Beschreibung
1	E2800B-Controller (Storage-Controller)
2	E5700SG Controller (Compute-Controller)
3	Gebälsebehälter (1 von 2)
4	Leistungsbehälter (1 von 2)

Verwandte Informationen

["NetApp E-Series Systems Documentation Site"](#)

SG5700 Controller

Sowohl die SG5712 und SG5712X mit 12 Laufwerken als auch die SG5760 und SG5760X Modelle mit 60 Laufwerken der StorageGRID Appliance umfassen einen E5700SG Computing-Controller und einen E-Series E2800 Storage-Controller.

- Das SG5712 und SG5760 verwenden einen E2800A-Controller.
- Das SG5712X und das SG5760 verwenden einen E2800B-Controller.

Die E2800A- und E2800B-Controller sind in der Spezifikation und Funktion identisch, mit Ausnahme des Standorts der Interconnect-Ports.

E5700SG Compute-Controller

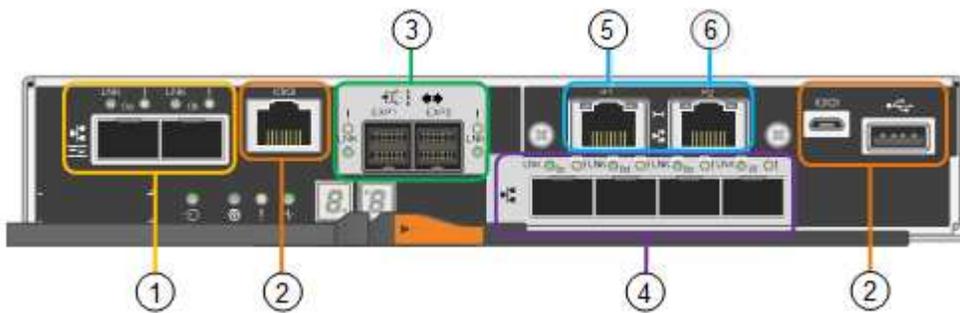
- Arbeitet als Computing-Server für die Appliance.
- Schließt das Installationsprogramm für StorageGRID-Appliance ein.



Die StorageGRID-Software ist auf der Appliance nicht vorinstalliert. Auf diese Software wird über den Admin-Node zugegriffen, wenn Sie die Appliance bereitstellen.

- Es kann eine Verbindung zu allen drei StorageGRID-Netzwerken hergestellt werden, einschließlich dem Grid-Netzwerk, dem Admin-Netzwerk und dem Client-Netzwerk.
- Stellt eine Verbindung zum E2800 Controller her und arbeitet als Initiator.

E5700SG-Steckverbinder



Legende	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	16 Gbit/s Fibre Channel (FC), optischer SFP	Verbinden Sie den E5700SG Controller mit dem E2800 Controller.
2	Diagnose- und Supportports	<ul style="list-style-type: none"> • Serieller RJ-45-Anschluss • Serieller Micro-USB-Anschluss • USB-Anschluss 	Reserviert für technischen Support.
3	Ports zur Laufwerkserweiterung	12 GB/s SAS	Nicht verwendet. StorageGRID Appliances unterstützen keine Erweiterungs-Festplatten-Shelfs.
4	Netzwerkanschlüsse 1-4	10-GbE oder 25-GbE, basierend auf SFP-Transceiver, Switch-Geschwindigkeit und konfigurierter Link-Geschwindigkeit	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.

Legende	Port	Typ	Nutzung
5	Management-Port 1	1-GB-Ethernet (RJ-45)	Stellen Sie eine Verbindung zum Admin-Netzwerk für StorageGRID her.
6	Management-Port 2	1-GB-Ethernet (RJ-45)	Optionen: <ul style="list-style-type: none"> • Verbindung mit Management-Port 1 für eine redundante Verbindung zum Admin-Netzwerk für StorageGRID. • Lassen Sie nicht verdrahtet und für den vorübergehenden lokalen Zugang verfügbar (IP 169.254.0.1). • Verwenden Sie während der Installation Port 2 für die IP-Konfiguration, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

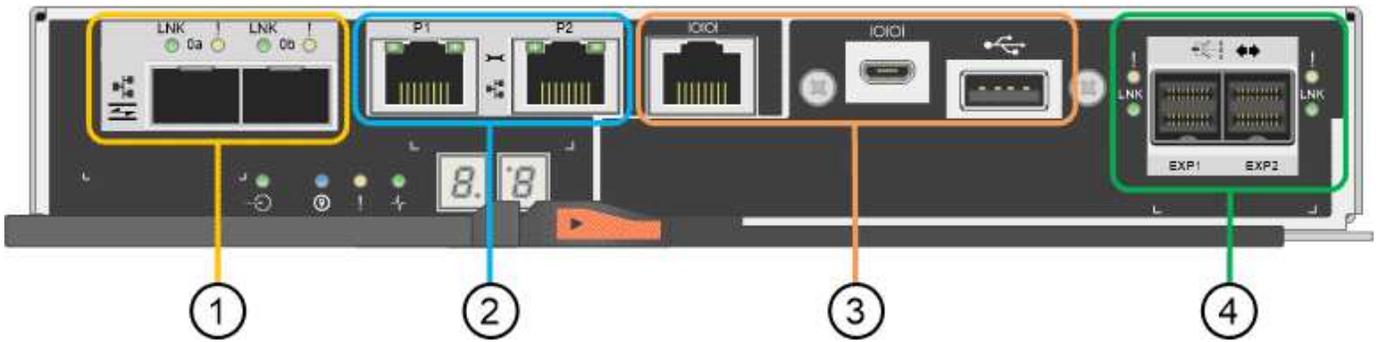
E2800 Storage-Controller

Der E2800 Storage-Controller wurde in den SG5700 Appliances in zwei Versionen verwendet: E2800A und E2800B. Das E2800A hat keine HIC und das E2800B hat eine HIC mit vier Ports. Die beiden Controller-Versionen haben die gleichen Spezifikationen und Funktionen, mit Ausnahme der Lage der Interconnect-Ports.

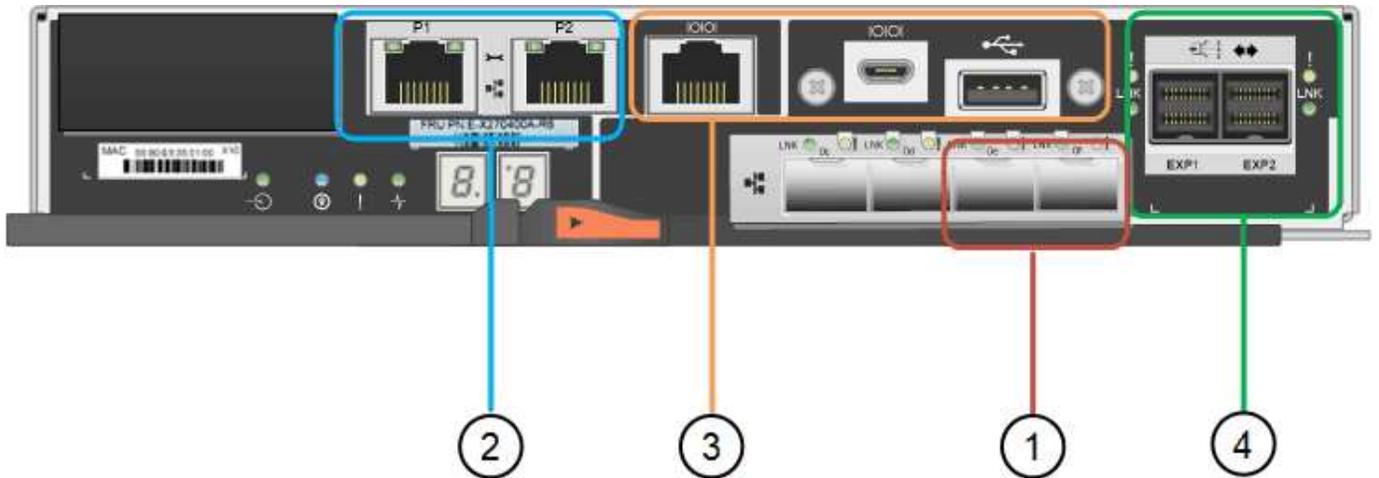
Der Storage Controller der E2800 Serie verfügt über folgende Spezifikationen:

- Fungiert als Storage Controller für die Appliance.
- Verwaltet den Storage der Daten auf den Laufwerken.
- Funktioniert als Standard-E-Series-Controller im Simplexmodus.
- Beinhaltet SANtricity OS Software (Controller-Firmware)
- Enthält SANtricity System Manager für die Überwachung der Appliance-Hardware und für das Verwalten von Warnmeldungen, die AutoSupport Funktion und die Laufwerksicherheitsfunktion.
- Stellt eine Verbindung zum E5700SG-Controller her und arbeitet als Ziel.

E2800A-Anschlüsse



E2800B-Anschlüsse



Legende	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	Optischer 16 Gbit/s FC SFP	Verbinden Sie den E2800 Controller mit dem E5700SG Controller.

Legende	Port	Typ	Nutzung
2	Management-Ports 1 und 2	1-GB-Ethernet (RJ-45)	<ul style="list-style-type: none"> • Port 1-Optionen: <ul style="list-style-type: none"> ◦ Stellen Sie eine Verbindung zu einem Managementnetzwerk her, um direkten TCP/IP-Zugriff auf SANtricity System Manager zu ermöglichen ◦ Lassen Sie die Kabel, um einen Switch-Port und eine IP-Adresse zu speichern. Greifen Sie über die Grid Manager- oder Speicher Grid Appliance Installer-UIs auf den SANtricity System Manager zu. <p>Hinweis: Einige optionale SANtricity-Funktionen, wie z.B. NTP Sync für genaue Log-Zeitstempel, sind nicht verfügbar, wenn Sie Port 1 unverdrahtet lassen.</p> <p>Hinweis: StorageGRID 11.5 oder höher und SANtricity 11.70 oder höher sind erforderlich, wenn Sie Port 1 unverdrahtet verlassen.</p> <ul style="list-style-type: none"> • Port 2 ist für den technischen Support reserviert.
3	Diagnose- und Supportports	<ul style="list-style-type: none"> • Serieller RJ-45-Anschluss • Serieller Micro-USB-Anschluss • USB-Anschluss 	Nur zur Verwendung durch technischen Support reserviert.
4	Ports zur Laufwerkserweiterung:	12 GB/s SAS	Nicht verwendet.

SG100- und SG1000-Geräte: Überblick

Die StorageGRID SG100 Services Appliance und die SG1000 Services Appliance

können als Gateway-Node und als Admin-Node ausgeführt werden, um hochverfügbare Load-Balancing-Services in einem StorageGRID System bereitzustellen. Beide Appliances können gleichzeitig als Gateway-Nodes und Admin-Nodes (primär oder nicht primär) betrieben werden.

Funktionen der Appliance

Beide Modelle der Service Appliance bieten die folgenden Funktionen:

- Gateway-Knoten oder Admin-Knoten Funktionen für ein StorageGRID-System.
- StorageGRID Appliance Installer zur Vereinfachung der Implementierung und Konfiguration von Nodes.
- Bei der Bereitstellung kann über einen vorhandenen Admin-Node oder über auf ein lokales Laufwerk heruntergeladene Software auf die StorageGRID-Software zugegriffen werden. Um den Implementierungsprozess weiter zu vereinfachen, wird während der Fertigung eine aktuelle Version der Software vorinstalliert.
- Ein Baseboard Management Controller (BMC) für das Monitoring und die Diagnose einiger Hardware des Geräts.
- Die Möglichkeit, eine Verbindung zu allen drei StorageGRID-Netzwerken herzustellen, einschließlich Grid-Netzwerk, Admin-Netzwerk und Client-Netzwerk:
 - Das SG100 unterstützt bis zu vier 10- oder 25-GbE-Verbindungen mit dem Grid-Netzwerk und dem Client-Netzwerk.
 - Das SG1000 unterstützt bis zu vier 10-, 25-, 40- oder 100-GbE-Verbindungen zum Grid-Netzwerk und dem Client-Netzwerk.

SG100- und SG1000-Diagramme

Diese Abbildung zeigt die Vorderseite des SG100 und des SG1000 mit entfernter Blende. Von der Vorderseite sind die beiden Geräte identisch, mit Ausnahme des Produktnamens auf der Blende.

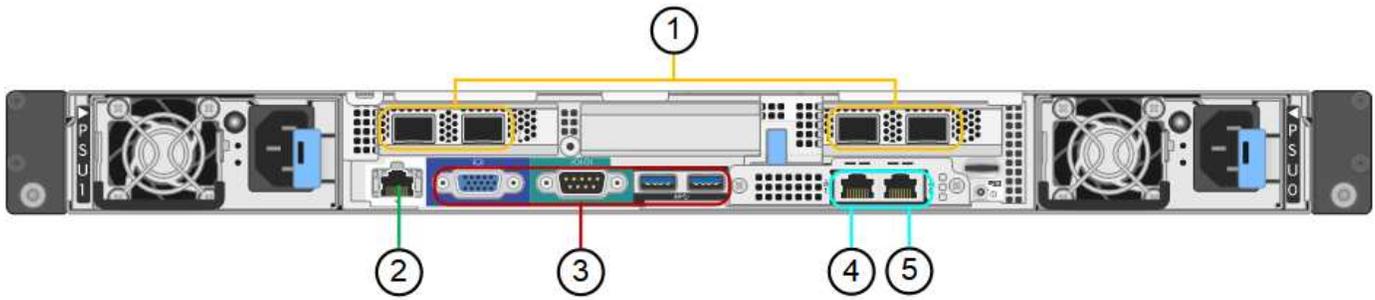


Die beiden durch die orangefarbene Umrandung gekennzeichneten Solid State-Laufwerke (SSDs) werden zur Speicherung des StorageGRID-Betriebssystems verwendet und aus Redundanzgründen mit RAID 1 gespiegelt. Wenn die SG100- oder SG1000-Services-Appliance als Admin-Node konfiguriert ist, werden diese Laufwerke zum Speichern von Audit-Protokollen, Kennzahlen und Datenbanktabellen verwendet.

Die übrigen Laufwerksschächte sind leer.

SG100-Anschlüsse

Diese Abbildung zeigt die Anschlüsse auf der Rückseite des SG100.

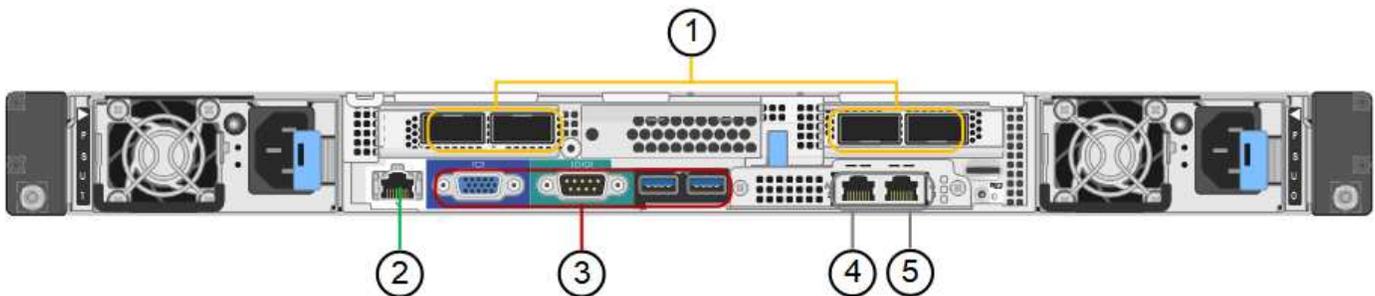


Legende	Port	Typ	Nutzung
1	Netzwerkanschlüsse 1-4	10/25-GbE, basierend auf Kabel- oder SFP-Transceiver-Typ (SFP28 und SFP+ Module werden unterstützt), Switch-Geschwindigkeit und konfigurierter Link-Geschwindigkeit	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.
2	BMC-Management-Port	1 GbE (RJ-45)	Stellen Sie eine Verbindung mit dem Management Controller der Hauptplatine des Geräts her.
3	Diagnose- und Supportports	<ul style="list-style-type: none"> • VGA • Seriell, 115200 8-N-1 • USB 	Nur zur Verwendung durch technischen Support reserviert.
4	Admin-Netzwerkport 1	1 GbE (RJ-45)	Schließen Sie die Appliance an das Admin-Netzwerk für StorageGRID an.

Legende	Port	Typ	Nutzung
5	Admin – Netzwerkanschluss 2	1 GbE (RJ-45)	<p>Optionen:</p> <ul style="list-style-type: none"> • Verbindung mit Management-Port 1 für eine redundante Verbindung zum Admin-Netzwerk für StorageGRID. • Lassen Sie die Verbindung getrennt und für den vorübergehenden lokalen Zugriff verfügbar (IP 169.254.0.1). • Verwenden Sie während der Installation Port 2 für die IP-Konfiguration, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

SG1000-Anschlüsse

Diese Abbildung zeigt die Anschlüsse auf der Rückseite des SG1000.



Legende	Port	Typ	Nutzung
1	Netzwerkanschlüsse 1-4	10/25/40/100-GbE, basierend auf Kabel- oder Transceiver-Typ, Switch-Geschwindigkeit und konfigurierter Verbindungsgeschwindigkeit. QSFP28 und QSFP+ (40/100GbE) werden nativ unterstützt und SFP28/SFP+ Transceiver können mit einem QSA (separat erhältlich) für 10/25-GbE-Geschwindigkeiten verwendet werden.	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.

Legende	Port	Typ	Nutzung
2	BMC-Management-Port	1 GbE (RJ-45)	Stellen Sie eine Verbindung mit dem Management Controller der Hauptplatine des Geräts her.
3	Diagnose- und Supportports	<ul style="list-style-type: none"> • VGA • Seriell, 115200 8-N-1 • USB 	Nur zur Verwendung durch technischen Support reserviert.
4	Admin-Netzwerkport 1	1 GbE (RJ-45)	Schließen Sie die Appliance an das Admin-Netzwerk für StorageGRID an.
5	Admin – Netzwerkanschluss 2	1 GbE (RJ-45)	<p>Optionen:</p> <ul style="list-style-type: none"> • Verbindung mit Management-Port 1 für eine redundante Verbindung zum Admin-Netzwerk für StorageGRID. • Lassen Sie die Verbindung getrennt und für den vorübergehenden lokalen Zugriff verfügbar (IP 169.254.0.1). • Verwenden Sie während der Installation Port 2 für die IP-Konfiguration, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

SG100- und SG1000-Applikationen

Die StorageGRID Services Appliances können auf unterschiedliche Weise konfiguriert werden, um Gateway Services oder Redundanz einiger Grid-Administrations-Services bereitzustellen.

Appliances können wie folgt eingesetzt werden:

- Zu einem neuen oder vorhandenen Grid als Gateway-Node hinzufügen
- Fügen Sie zu einem neuen Grid als primären oder nicht-primären Admin-Node oder zu einem vorhandenen Grid als nicht-primärer Admin-Node hinzu
- Arbeiten Sie gleichzeitig als Gateway Node und Admin Node (primär oder nicht primär)

Die Appliance erleichtert die Nutzung von Hochverfügbarkeitsgruppen (HA) und intelligentem Lastausgleich für S3- oder Swift-Datenpfadverbindungen.

In den folgenden Beispielen wird beschrieben, wie Sie die Funktionen der Appliance maximieren können:

- Verwenden Sie zwei SG100- oder zwei SG1000-Appliances, um Gateway-Services bereitzustellen, indem Sie sie als Gateway-Nodes konfigurieren.



Implementieren Sie die SG100 und SG1000 Service Appliances nicht am selben Standort. Das kann zu einer unvorhersehbaren Performance führen.

- Verwenden Sie zwei SG100- oder zwei SG1000-Appliances, um die Redundanz einiger Grid-Verwaltungsdienste zu gewährleisten. Konfigurieren Sie dazu jedes Gerät als Admin-Nodes.
- Verwenden Sie zwei SG100- oder zwei SG1000-Appliances, um hochverfügbare Lastausgleichs- und Traffic Shaping-Services bereitzustellen, auf die über eine oder mehrere virtuelle IP-Adressen zugegriffen wird. Konfigurieren Sie die Appliances als beliebige Kombination aus Admin-Nodes oder Gateway-Nodes und fügen Sie beide Nodes derselben HA-Gruppe hinzu.



Wenn Sie Admin-Nodes und Gateway-Nodes in derselben HA-Gruppe verwenden, erfolgt kein Failover für den nur-Admin-Node-Port. Siehe Anweisungen für "[Konfigurieren von HA-Gruppen](#)".

Bei der Verwendung mit StorageGRID Storage Appliances ermöglichen sowohl die SG100- als auch die SG1000-Service-Appliances die Implementierung von gerätebasierten Grids ohne Abhängigkeiten von externen Hypervisoren oder Computing-Hardware.

Installation vorbereiten

Standort vorbereiten

Vor der Installation der Appliance müssen Sie sicherstellen, dass der Standort und das Rack, das Sie verwenden möchten, die Spezifikationen einer StorageGRID Appliance erfüllen.

Schritte

1. Vergewissern Sie sich, dass der Standort die Anforderungen an Temperatur, Luftfeuchtigkeit, Höhenbereich, Luftstrom, Wärmeableitung, Verkabelung, Strom und Erdung. Siehe "[NetApp Hardware Universe](#)" Finden Sie weitere Informationen.
2. Vergewissern Sie sich, dass Ihr Standort die richtige Wechselstromspannung liefert:

Modell	Anforderungen
SGF6112	100 bis 240 Volt Wechselstrom
SG6060	240-Volt-Wechselspannung
SGF6024	120-Volt-Wechselspannung
SG5760	240-Volt-Wechselspannung
SG100 und SG1000	120 bis 240 Volt Wechselstrom

3. Beziehen Sie einen 19-Zoll-Schrank (48.3 cm) für die folgenden Regale (ohne Kabel).

SGF6112

Höhe	Breite	Tiefe	Maximales Gewicht
1.70 Zoll (4.31 cm)	18.98 Zoll (48.2 cm)	33.11 Zoll (84.1 cm)	43.83 lb. (19.88 kg)

SG6000

Typ des Shelves	Höhe	Breite	Tiefe	Maximales Gewicht
E2860 Controller-Shelf (SG6060)	6.87 Zoll (17.46 cm)	17.66 Zoll (44.86 cm)	38.25 Zoll (97.16 cm)	250 lb. (113 kg)
Erweiterungs-Shelf (SG6060) - optional	6.87 Zoll (17.46 cm)	17.66 Zoll (44.86 cm)	38.25 Zoll (97.16 cm)	250 lb. (113 kg)
EF570 Controller-Shelf (SGF6024)	3.35 Zoll (8.50 cm)	17.66 Zoll (44.86 cm)	19.00 Zoll (48.26 cm)	51.74 lb. (23.47 kg)
SG6000-CN Computing- Controller	1.70 Zoll (4.32 cm)	17.32 Zoll (44.0 cm)	32.0 Zoll (81.3 cm)	39 lb. (17.7 kg)

SG5700

Appliance-Modell	Höhe	Breite	Tiefe	Maximales Gewicht
SG5712 (12 Festplatten)	3.41 Zoll (8.68 cm)	17.6 Zoll (44.7 cm)	21.1 Zoll (53.6 cm)	63.9 lb (29.0 kg)
SG5760 (60 Festplatten)	6.87 Zoll (17.46 cm)	17.66 Zoll (44.86 cm)	38.25 Zoll (97.16 cm)	250 lb. (113 kg)

SG100 und SG1000

Höhe	Breite	Tiefe	Maximales Gewicht
1.70 Zoll (4.32 cm)	17.32 Zoll (44.0 cm)	32.0 Zoll (81.3 cm)	39 lb. (17.7 kg)

4. Entscheiden Sie, wo Sie das Gerät installieren möchten.



Installieren Sie bei der Installation des E2860 Controller-Shelfs oder optionaler Erweiterungs-Shelfs die Hardware von unten nach oben im Rack oder Schrank, um zu vermeiden, dass das System umkippt. Installieren Sie den SG6000-CN Controller über dem E2860 Controller-Shelf und Erweiterungs-Shelfs, um sicherzustellen, dass sich die schwersten Geräte unten im Rack oder Rack befinden.



Stellen Sie vor der Installation sicher, dass die mit einem SG6000-Gerät gelieferten 0,5-m-Glasfaserkabel oder die von Ihnen gelieferten Kabel lang genug für das geplante Layout sind.

5. Installieren Sie alle erforderlichen Netzwerk-Switches. Siehe ["NetApp Interoperabilitäts-Matrix-Tool"](#) Informationen zur Kompatibilität.

Packen Sie die Kartons aus

Packen Sie vor der Installation des StorageGRID-Geräts alle Kartons aus, und vergleichen Sie den Inhalt mit den Artikeln auf dem Packzettel.

SGF6112 Appliances

Trennt

Element	Wie es aussieht
SGF6112	
Schienensatz mit Anleitung	
Frontblende	

Stromkabel

Im Lieferumfang eines SGF6112-Geräts sind die folgenden Netzkabel enthalten:

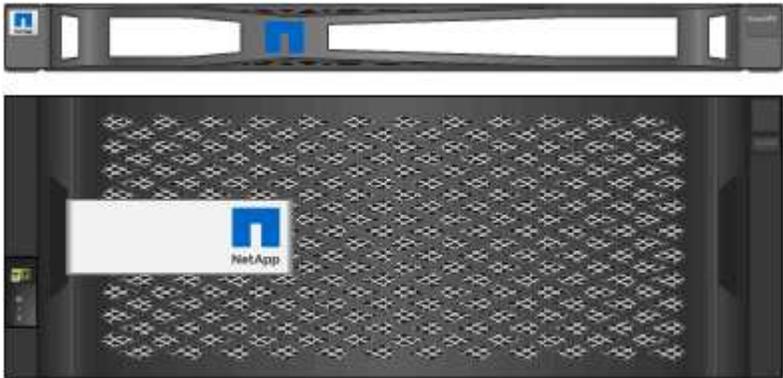
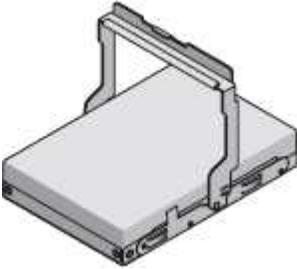
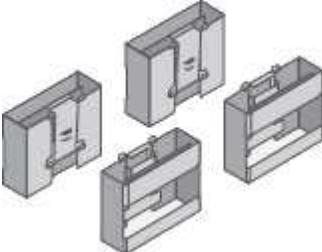


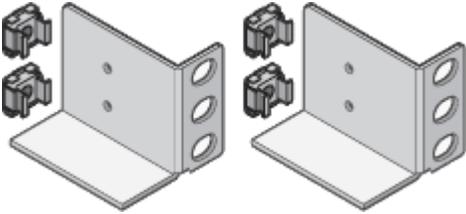
Ihr Schrank verfügt möglicherweise über spezielle Netzkabel, die Sie anstelle der Netzkabel verwenden, die Sie zur Einheit mit dem Gerät anschließen.

Element	Wie es aussieht
Zwei Netzkabel für dein Land	

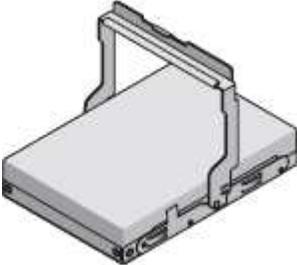
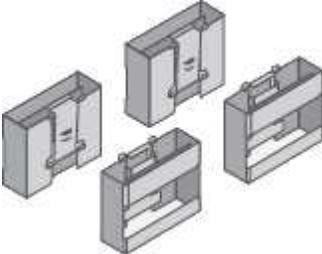
SG6000 Appliances

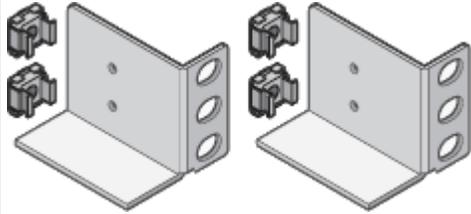
SG6060-Hardware

Element	Wie es aussieht
SG6000-CN Controller	 A long, thin, black server controller unit with multiple drive bays and a front panel.
E2860 Controller-Shelf ohne installierte Laufwerke	 A black server shelf with multiple drive bays, shown without installed drives.
Zwei Frontrahmen	 Two front frames: one is a long, thin metal frame with a blue handle, and the other is a larger, black metal frame with a perforated front panel and a NetApp logo.
Zwei Schienensätze mit Anweisungen	 Two sets of metal rails with screws and instructions for installation.
60 Laufwerke (2 SSD und 58 NL-SAS)	 A single drive tray, shown in a perspective view, with a handle and a latch.
Vier Griffe	 Four metal handles of different shapes and sizes, used for the front frames.

Element	Wie es aussieht
Rückhalterungen und Käfigmuttern für Rack-Montage mit Vierkantloch	

SG6060 Erweiterungs-Shelf

Element	Wie es aussieht
Erweiterungs-Shelf ohne Laufwerke installiert	
Frontblende	
60 NL-SAS-Laufwerke	
Ein Schienensatz mit Anweisungen	
Vier Griffe	

Element	Wie es aussieht
Rückhalterungen und Käfigmuttern für Rack-Montage mit Vierkantloch	

SGF6024 Hardware

Element	Wie es aussieht
SG6000-CN Controller	
EF570 Flash-Array mit 24 installierten Solid State-Laufwerken (Flash	
Zwei Frontrahmen	
Zwei Schienensätze mit Anweisungen	
Endkappen für die Ablage	

Kabel und Anschlüsse

Im Lieferumfang einer SG6000 Appliance sind die folgenden Kabel und Anschlüsse enthalten.



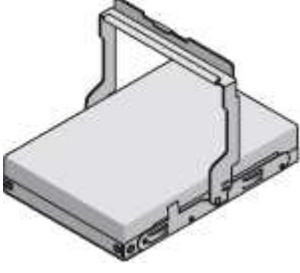
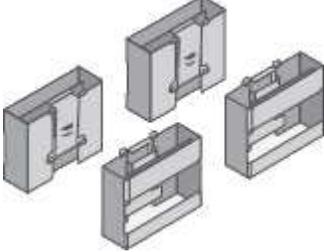
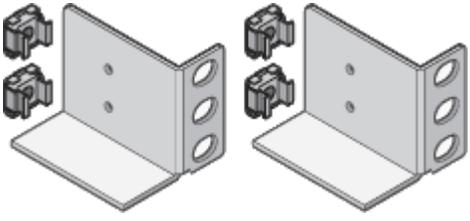
Ihr Schrank verfügt möglicherweise über spezielle Netzkabel, die Sie anstelle der Netzkabel verwenden, die Sie zur Einheit mit dem Gerät anschließen.

Element	Wie es aussieht
Vier Netzkabel für Ihr Land	
Optische Kabel und SFP-Transceiver	  <ul style="list-style-type: none"> • Vier optische Kabel für die FC Interconnect Ports • Vier SFP+-Transceiver, die 16 Gbit/s FC unterstützen
Optional: Zwei SAS-Kabel zum Anschluss jedes SG6060-Erweiterungs-Shelfs	

SG5700 Appliances

Trennt

Element	Wie es aussieht
SG5712 Appliance mit installierten 12 Laufwerken	
SG5760 Appliance ohne installierte Laufwerke	
Frontverkleidung für das Gerät	 

Element	Wie es aussieht
Schienensatz mit Anleitung	
SG5760: Sechzig Laufwerke	
SG5760: Griffe	
SG5760: Rückenhalterungen und Käfigmuttern für Rack-Montage mit Vierkantloch	

Kabel und Anschlüsse

Der Versand für eine SG5700 Appliance umfasst die folgenden Kabel und Anschlüsse.



Ihr Schrank verfügt möglicherweise über spezielle Netzkabel, die Sie anstelle der Netzkabel verwenden, die Sie zur Einheit mit dem Gerät anschließen.

Element	Wie es aussieht
Zwei Netzkabel für dein Land	

Element	Wie es aussieht
Optische Kabel und SFP-Transceiver	 <ul style="list-style-type: none"> • Zwei optische Kabel für die FC Interconnect Ports • Acht SFP+-Transceiver, kompatibel mit den vier 16-Gbit/s-FC-Interconnect-Ports und den vier 10-GbE-Netzwerkports

SG100 und SG1000 Appliances

Trennt

Element	Wie es aussieht
SG100 oder SG1000	
Schienensatz mit Anleitung	

Stromkabel

Im Lieferumfang einer SG100 oder SG1000 Appliance sind die folgenden Netzkabel enthalten:



Ihr Schrank verfügt möglicherweise über spezielle Netzkabel, die Sie anstelle der Netzkabel verwenden, die Sie zur Einheit mit dem Gerät anschließen.

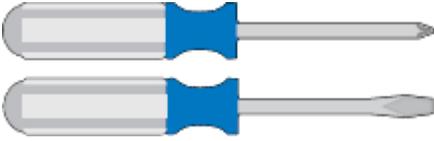
Element	Wie es aussieht
Zwei Netzkabel für dein Land	

Beschaffen Sie sich zusätzliche Geräte und Werkzeuge

Vergewissern Sie sich vor der Installation eines StorageGRID-Geräts, dass Sie über alle zusätzlichen Geräte und Werkzeuge verfügen, die Sie benötigen.

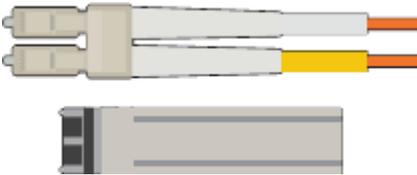
Alle Geräte

Für die Installation und Konfiguration aller Appliances benötigen Sie die folgenden Geräte:

Element	Wie es aussieht
Schraubendreher	 <ul style="list-style-type: none"> • Phillips Nr. 2 Schraubendreher • Mittlerer Schlitzschraubendreher
ESD-Handgelenkschlaufe	
Service-Laptop	 <ul style="list-style-type: none"> • "Unterstützter Webbrowser" • SSH-Client, z. B. PuTTY • 1-GbE-Port (RJ-45) <p> Einige Ports unterstützen möglicherweise keine 10/100 Ethernet-Geschwindigkeiten.</p>
Optionale Werkzeuge	 <ul style="list-style-type: none"> • Kraftbohrer mit Kreuzschlitz • Taschenlampe

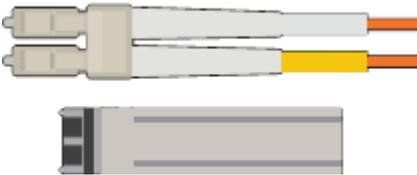
SGF6112

Für die Installation und Konfiguration der SGF6112-Hardware benötigen Sie die folgenden zusätzlichen Geräte.

Element	Wie es aussieht
Optische Kabel und Transceiver	 <ul style="list-style-type: none">• Ein bis vier dieser Kabeltypen:<ul style="list-style-type: none">◦ Twinax/Kupfer◦ Glasfaser/Optisch• Je ein bis vier dieser Transceiver/Adapter auf Basis der Verbindungsgeschwindigkeit (gemischte Geschwindigkeiten werden nicht unterstützt):<ul style="list-style-type: none">◦ 10-GbE SFP+◦ 25-GbE-SFP28
RJ-45-Ethernet-Kabel (Cat5/Cat5e/Cat6/Cat6a)	

SG6000

Für die Installation und Konfiguration der SG6000-Hardware benötigen Sie die folgenden zusätzlichen Geräte:

Element	Wie es aussieht
Optische Kabel und SFP-Transceiver	 <ul style="list-style-type: none">• Ein bis vier dieser Kabeltypen:<ul style="list-style-type: none">◦ Twinax/Kupfer◦ Glasfaser/Optisch• Je ein bis vier dieser Transceiver/Adapter, basierend auf der Verbindungsgeschwindigkeit (gemischte Geschwindigkeiten werden nicht unterstützt):<ul style="list-style-type: none">◦ 10-GbE SFP+◦ 25-GbE-SFP28

Element	Wie es aussieht
RJ-45-Ethernet-Kabel (Cat5/Cat5e/Cat6)	
Optionale Werkzeuge	Mechanisierter Lift für 60-Laufwerk-Shelfs

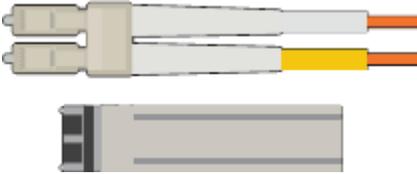
SG5700

Für die Installation und Konfiguration der SG5700-Hardware benötigen Sie die folgenden zusätzlichen Geräte:

Element	Wie es aussieht
Optische Kabel und SFP-Transceiver	 <ul style="list-style-type: none"> • Optische Kabel für die 10/25-GbE-Ports, die Sie verwenden möchten • Optional: SFP28 Transceiver, wenn Sie 25-GbE-Verbindungsgeschwindigkeit verwenden möchten
Ethernet-Kabel	
Optionale Werkzeuge	Mechanisierter Lift für SG5760

SG100 und SG1000

Für die Installation und Konfiguration der SG100- und SG1000-Hardware benötigen Sie die folgenden zusätzlichen Geräte.

Element	Wie es aussieht
Optische Kabel und Transceiver	 <ul style="list-style-type: none"> • Ein bis vier dieser Kabeltypen: <ul style="list-style-type: none"> ◦ Twinax/Kupfer ◦ Glasfaser/Optisch • Je ein bis vier dieser Transceiver/Adapter auf Basis der Verbindungsgeschwindigkeit (gemischte Geschwindigkeiten werden nicht unterstützt): <ul style="list-style-type: none"> ◦ SG100: <ul style="list-style-type: none"> ▪ 10-GbE SFP+ ▪ 25-GbE-SFP28 ◦ SG1000: <ul style="list-style-type: none"> ▪ 10-GbE QSFP-to-SFP-Adapter (QSA) und SFP+ ▪ 25-GbE QSFP-zu-SFP-Adapter (QSA) und SFP28 ▪ 40-GbE QSFP+ ▪ 100-GbE-QFSP28
RJ-45-Ethernet-Kabel (Cat5/Cat5e/Cat6/Cat6a)	

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

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

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024

Browserbreite	Pixel
Optimal	1280

Überprüfen Sie die Appliance-Netzwerkverbindungen

Überprüfen Sie die Appliance-Netzwerkverbindungen

Vor der Installation der StorageGRID Appliance sollten Sie wissen, welche Netzwerke mit der Appliance verbunden werden können und wie die Ports auf den einzelnen Controllern verwendet werden. Die Netzwerkanforderungen von StorageGRID werden im ausführlich erläutert "[Netzwerkrichtlinien](#)".

Wenn Sie eine StorageGRID Appliance als Node in einem StorageGRID System implementieren, können Sie eine Verbindung mit folgenden Netzwerken herstellen:

- **Grid-Netzwerk für StorageGRID:** Das Grid-Netzwerk wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das System bietet Konnektivität zwischen allen Nodes im Grid und allen Standorten und Subnetzen. Das Grid-Netzwerk ist erforderlich.
- **Admin-Netzwerk für StorageGRID:** Das Admin-Netzwerk ist ein geschlossenes Netzwerk, das zur Systemadministration und Wartung verwendet wird. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Standorten routingfähig sein. Das Admin-Netzwerk ist optional.
- **Client-Netzwerk für StorageGRID:** das Client-Netzwerk ist ein offenes Netzwerk, das für den Zugriff auf Client-Anwendungen, einschließlich S3 und Swift, verwendet wird. Das Client-Netzwerk ermöglicht den Zugriff auf das Grid-Protokoll, sodass das Grid-Netzwerk isoliert und gesichert werden kann. Sie können das Client-Netzwerk so konfigurieren, dass über dieses Netzwerk nur über die Ports zugegriffen werden kann, die Sie öffnen möchten. Das Client-Netzwerk ist optional.
- **Managementnetzwerk für SANtricity** (optional für Speichergeräte, nicht für SGF6112 erforderlich): Dieses Netzwerk bietet Zugriff auf SANtricity System Manager, mit dem Sie die Hardwarekomponenten im Appliance- und Speicher-Controller-Shelf überwachen und verwalten können. Dieses Managementnetzwerk kann das gleiche sein wie das Admin-Netzwerk für StorageGRID, oder es kann ein unabhängiges Managementnetzwerk sein.
- **BMC-Managementnetzwerk** (optional für SG100, SG1000, SG6000 und SGF6112): Dieses Netzwerk bietet Zugriff auf den Baseboard Management Controller in den SG100, SG1000, SG6000 und SGF6112 Appliances, sodass Sie die Hardwarekomponenten in der Appliance überwachen und verwalten können. Dieses Managementnetzwerk kann das gleiche sein wie das Admin-Netzwerk für StorageGRID, oder es kann ein unabhängiges Managementnetzwerk sein.

Wenn das optionale BMC-Managementnetzwerk nicht verbunden ist, sind einige Support- und Wartungsverfahren schwieriger zu bewältigen. Sie können das BMC-Managementnetzwerk außer zu Supportzwecken unverbunden lassen.

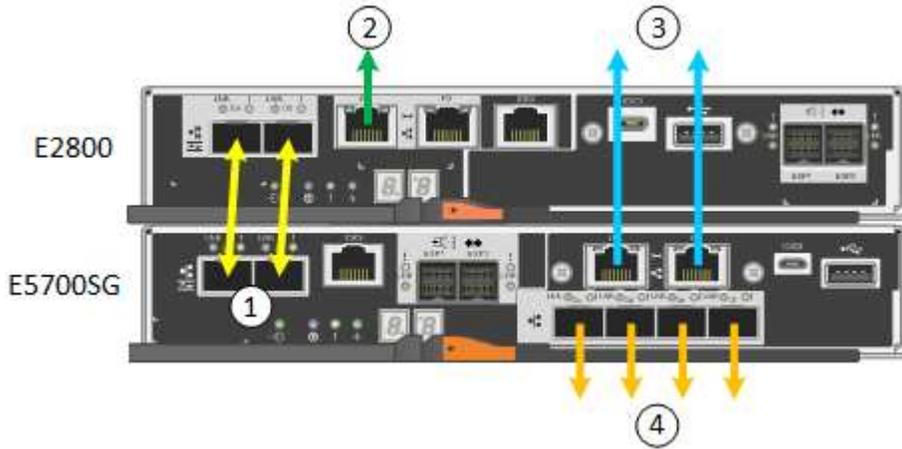


Ausführliche Informationen zu StorageGRID-Netzwerken finden Sie im "[StorageGRID-Netzwerktypen](#)".

Netzwerkverbindungen (SG5700)

Wenn Sie eine SG5700 StorageGRID Appliance installieren, verbinden Sie die beiden Controller miteinander und mit den erforderlichen Netzwerken.

Die Abbildung zeigt die beiden Controller der SG5760: Der E2800 Controller oben und der E5700SG Controller unten. In der SG5712 befindet sich der E2800 Controller links vom E5700SG Controller.



Legende	Port	Typ des Ports	Nutzung
1	Zwei Interconnect-Ports an jedem Controller	16 Gbit/s FC optisch SFP+	Verbinden Sie die beiden Controller miteinander.
2	Management-Port 1 am E2800-Controller	1 GbE (RJ-45)	Stellt eine Verbindung mit dem Netzwerk her, in dem Sie auf SANtricity System Manager zugreifen. Sie können das Admin-Netzwerk für StorageGRID oder ein unabhängiges Managementnetzwerk verwenden.
Management-Port 2 am E2800 Controller	1 GbE (RJ-45)	Reserviert für technischen Support.	3
Management-Port 1 am E5700SG Controller	1 GbE (RJ-45)	Verbindet den E5700SG-Controller mit dem Admin-Netzwerk für StorageGRID.	Management-Port 2 am E5700SG Controller

Legende	Port	Typ des Ports	Nutzung
1 GbE (RJ-45)	<ul style="list-style-type: none"> • Kann mit Verwaltungspport 1 verbunden werden, wenn Sie eine redundante Verbindung zum Admin-Netzwerk wünschen. • Kann verkabelt und für temporären lokalen Zugang verfügbar sein (IP 169.254.0.1). • Kann während der Installation verwendet werden, um den E5700SG-Controller mit einem Service-Laptop zu verbinden, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind. 	4	10/25-GbE-Ports 1-4 auf dem E5700SG Controller

Port-Bond-Modi (SGF6112)

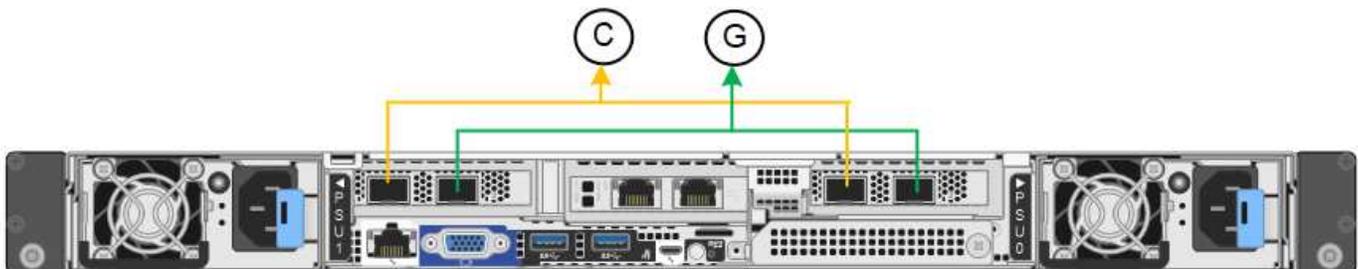
Wenn "[Netzwerk-Links werden konfiguriert](#)" Für die SGF6112-Appliance können Sie Port-Bonding für die Ports verwenden, die mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk verbunden sind, sowie für die 1/10-GbE-Management-Ports, die mit dem optionalen Admin-Netzwerk verbunden sind. Mit Port-Bonding sichern Sie Ihre Daten, indem Sie redundante Pfade zwischen StorageGRID-Netzwerken und der Appliance bereitstellen.

Netzwerk-Bond-Modi

Die Netzwerk-Ports auf der Appliance unterstützen den Bond-Modus für feste Ports oder den Bond-Modus für aggregierte Ports für Grid-Netzwerk- und Client-Netzwerkverbindungen.

Bond-Modus mit festem Port

Der Fixed-Port-Bond-Modus ist die Standardkonfiguration für die Netzwerk-Ports.



Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

Bei Verwendung des Bond-Modus mit festem Port können die Ports über den aktiv-Backup-Modus oder den Link Aggregation Control Protocol-Modus (LACP 802.3ad) verbunden werden.

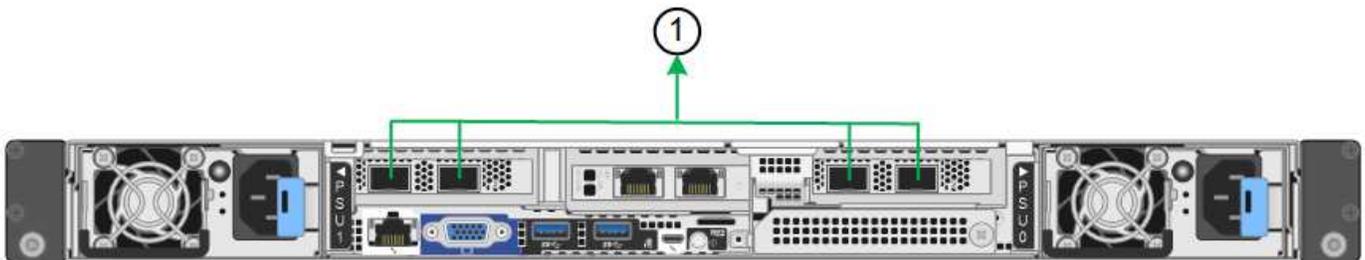
- Im aktiv-Backup-Modus (Standard) ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Port 4 bietet einen Sicherungspfad für Port 2 (Grid Network), und Port 3 stellt einen Sicherungspfad für Port 1 (Client Network) bereit.
- Im LACP-Modus bildet jedes Port-Paar einen logischen Channel zwischen der Appliance und dem Netzwerk, der einen höheren Durchsatz ermöglicht. Wenn ein Port ausfällt, stellt der andere Port den Kanal weiterhin bereit. Der Durchsatz wird verringert, die Konnektivität wird jedoch nicht beeinträchtigt.



Wenn Sie keine redundanten Verbindungen benötigen, können Sie für jedes Netzwerk nur einen Port verwenden. Beachten Sie jedoch, dass die Warnung **Storage Appliance Link down** nach der Installation von StorageGRID im Grid Manager ausgelöst werden kann, was darauf hinweist, dass ein Kabel nicht angeschlossen ist. Sie können diese Warnungsregel sicher deaktivieren.

Bond-Modus für aggregierten Ports

Im Aggregat-Port-Bond-Modus wird der Durchsatz jedes StorageGRID-Netzwerks deutlich erhöht und zusätzliche Failover-Pfade bereitgestellt.



Legende	Welche Ports sind verbunden
1	Alle verbundenen Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Datenverkehr verwendet werden können.

Wenn Sie planen, den aggregierten Port Bond-Modus zu verwenden:

- Sie müssen LACP Network Bond-Modus verwenden.
- Sie müssen für jedes Netzwerk ein eindeutiges VLAN-Tag angeben. Dieses VLAN-Tag wird zu jedem Netzwerkpaket hinzugefügt, um sicherzustellen, dass der Netzwerkverkehr an das richtige Netzwerk weitergeleitet wird.
- Die Ports müssen mit Switches verbunden sein, die VLAN und LACP unterstützen können. Wenn mehrere Switches an der LACP-Verbindung beteiligt sind, müssen die Switches MLAG (Multi-Chassis Link Aggregation Groups) oder eine vergleichbare Position unterstützen.

- Sie wissen, wie Sie die Switches für die Verwendung von VLAN, LACP und MLAG oder gleichwertig konfigurieren.

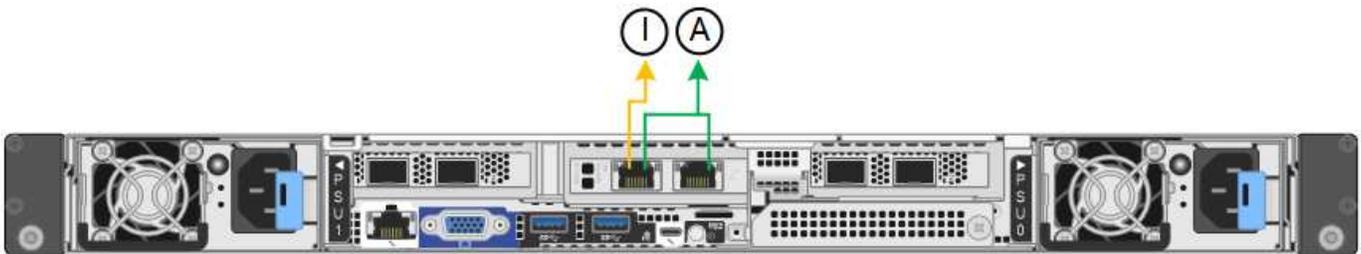
Wenn Sie nicht alle vier Ports verwenden möchten, können Sie einen, zwei oder drei Ports verwenden. Durch die Verwendung von mehr als einem Port wird die Wahrscheinlichkeit maximiert, dass einige Netzwerkverbindungen verfügbar bleiben, wenn einer der Ports ausfällt.



Wenn Sie weniger als vier Netzwerkanschlüsse verwenden möchten, beachten Sie, dass nach der Installation des Appliance-Knotens im Grid Manager möglicherweise eine Warnmeldung für die **Services-Appliance-Verbindung aus** ausgelöst wird, was darauf hinweist, dass ein Kabel nicht angeschlossen ist. Sie können diese Warnungsregel für die ausgelöste Warnmeldung sicher deaktivieren.

Network Bond-Modi für Management-Ports

Für die beiden 1/10-GbE-Management-Ports können Sie den Independent Network Bond-Modus oder den Active-Backup-Netzwerk-Bond-Modus wählen, um eine Verbindung zum optionalen Admin-Netzwerk herzustellen.



Im Independent-Modus ist nur der Management-Port links mit dem Admin-Netzwerk verbunden. Dieser Modus stellt keinen redundanten Pfad bereit. Der Management-Port auf der rechten Seite ist nicht verbunden und steht für temporäre lokale Verbindungen zur Verfügung (verwendet IP-Adresse 169.254.0.1).

Im Active-Backup-Modus sind beide Management-Ports mit dem Admin-Netzwerk verbunden. Es ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Die Verbindung dieser beiden physischen Ports zu einem logischen Management-Port bietet einen redundanten Pfad zum Admin-Netzwerk.



Wenn Sie eine temporäre lokale Verbindung zum Gerät herstellen müssen, wenn die 1/10-GbE-Managementports für den Active-Backup-Modus konfiguriert sind, entfernen Sie die Kabel von beiden Management-Ports, schließen Sie das temporäre Kabel an den Management-Port auf der rechten Seite an und greifen Sie über die IP-Adresse 169.254.0 auf die Appliance zu.

Legende	Netzwerk-Bond-Modus
A	Aktiv-Backup-Modus. Beide Management-Ports sind mit einem logischen Management-Port verbunden, der mit dem Admin-Netzwerk verbunden ist.
ICH	Unabhängiger Modus. Der Port auf der linken Seite ist mit dem Admin-Netzwerk verbunden. Der Anschluss rechts ist für temporäre lokale Verbindungen verfügbar (IP-Adresse 169.254.0.1).

Port-Bond-Modi (SG6000-CN-Controller)

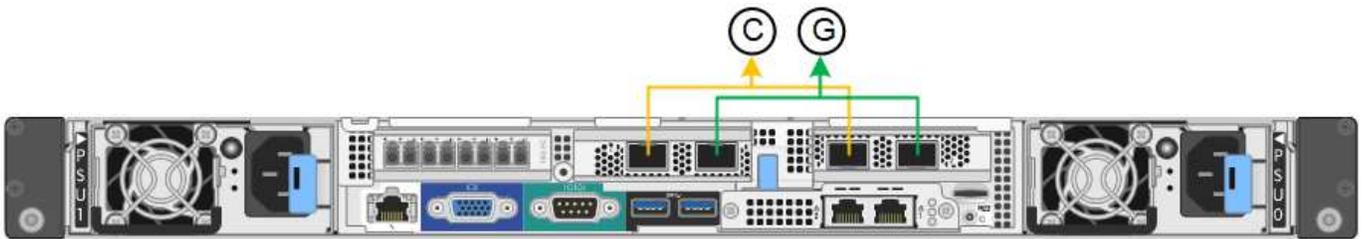
Wenn "**Netzwerk-Links werden konfiguriert**" Für den SG6000-CN-Controller können Sie Port-Bonding für die 10/25-GbE-Ports verwenden, die mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk verbunden sind, sowie für die 1-GbE-Management-Ports, die mit dem optionalen Admin-Netzwerk verbunden werden. Mit Port-Bonding sichern Sie Ihre Daten, indem Sie redundante Pfade zwischen StorageGRID-Netzwerken und der Appliance bereitstellen.

Netzwerk-Bond-Modi für 10/25-GbE-Ports

Die 10/25-GbE-Netzwerk-Ports des SG6000-CN-Controllers unterstützen den Bond-Modus Fixed Port oder den Bond-Modus für aggregierte Ports für Grid-Netzwerk- und Client-Netzwerk-Verbindungen.

Bond-Modus mit festem Port

Der Fixed-Modus ist die Standardkonfiguration für 10/25-GbE-Netzwerkports.



Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

Bei Verwendung des Bond-Modus mit festem Port können die Ports über den aktiv-Backup-Modus oder den Link Aggregation Control Protocol-Modus (LACP 802.3ad) verbunden werden.

- Im aktiv-Backup-Modus (Standard) ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Port 4 bietet einen Sicherungspfad für Port 2 (Grid Network), und Port 3 stellt einen Sicherungspfad für Port 1 (Client Network) bereit.
- Im LACP-Modus bildet jedes Port-Paar einen logischen Kanal zwischen dem Controller und dem Netzwerk, wodurch ein höherer Durchsatz ermöglicht wird. Wenn ein Port ausfällt, stellt der andere Port den Kanal weiterhin bereit. Der Durchsatz wird verringert, die Konnektivität wird jedoch nicht beeinträchtigt.

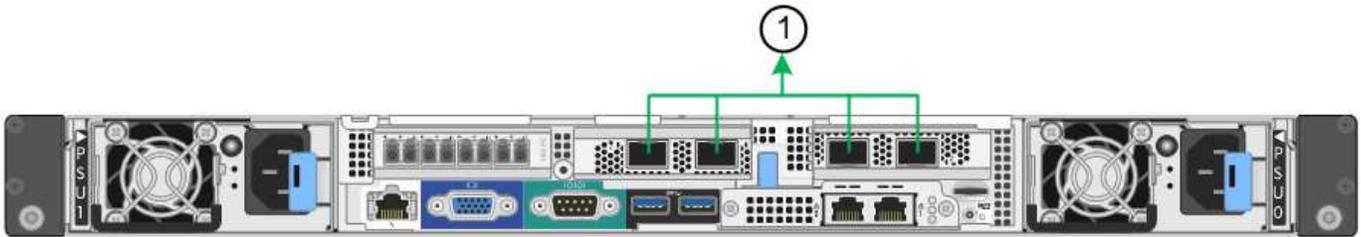


Wenn Sie keine redundanten Verbindungen benötigen, können Sie für jedes Netzwerk nur einen Port verwenden. Beachten Sie jedoch, dass nach der Installation von StorageGRID im Grid Manager eine Warnmeldung ausgelöst wird, die angibt, dass der Link nicht verfügbar ist. Da dieser Port speziell getrennt ist, können Sie diese Warnmeldung sicher deaktivieren.

Wählen Sie im Grid Manager die Option **Warnung > Regeln**, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen **aktiviert**.

Bond-Modus für aggregierten Ports

Der Aggregat-Port-Bond-Modus erhöht das ganze für jedes StorageGRID-Netzwerk deutlich und bietet zusätzliche Failover-Pfade.



Legende	Welche Ports sind verbunden
1	Alle verbundenen Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Datenverkehr verwendet werden können.

Wenn Sie planen, den aggregierten Port Bond-Modus zu verwenden:

- Sie müssen LACP Network Bond-Modus verwenden.
- Sie müssen für jedes Netzwerk ein eindeutiges VLAN-Tag angeben. Dieses VLAN-Tag wird zu jedem Netzwerkpaket hinzugefügt, um sicherzustellen, dass der Netzwerkverkehr an das richtige Netzwerk weitergeleitet wird.
- Die Ports müssen mit Switches verbunden sein, die VLAN und LACP unterstützen können. Wenn mehrere Switches an der LACP-Verbindung beteiligt sind, müssen die Switches MLAG (Multi-Chassis Link Aggregation Groups) oder eine vergleichbare Position unterstützen.
- Sie wissen, wie Sie die Switches für die Verwendung von VLAN, LACP und MLAG oder gleichwertig konfigurieren.

Wenn Sie nicht alle vier 10/25-GbE-Ports verwenden möchten, können Sie einen, zwei oder drei Ports verwenden. Durch die Verwendung mehrerer Ports wird die Wahrscheinlichkeit maximiert, dass einige Netzwerkverbindungen verfügbar bleiben, wenn einer der 10/25-GbE-Ports ausfällt.



Wenn Sie weniger als vier Ports verwenden, beachten Sie, dass nach der Installation von StorageGRID ein oder mehrere Alarime im Grid Manager angehoben werden, was darauf hinweist, dass die Kabel nicht angeschlossen sind. Sie können die Alarime sicher bestätigen, um sie zu löschen.

Netzwerk-Bond-Modi für 1-GbE-Management-Ports

Für die beiden 1-GbE-Management-Ports des SG6000-CN-Controllers können Sie den unabhängigen Netzwerk-Bond-Modus oder den aktiv-Backup-Netzwerk-Bond-Modus wählen, um eine Verbindung zum optionalen Admin-Netzwerk herzustellen.

Im Independent-Modus ist nur der Management-Port links mit dem Admin-Netzwerk verbunden. Dieser Modus stellt keinen redundanten Pfad bereit. Der Management Port auf der rechten Seite ist nicht verbunden und für temporäre lokale Verbindungen verfügbar (verwendet IP-Adresse 169.254.0.1)

Im Active-Backup-Modus sind beide Management-Ports mit dem Admin-Netzwerk verbunden. Es ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung

bereit. Die Verbindung dieser beiden physischen Ports zu einem logischen Management-Port bietet einen redundanten Pfad zum Admin-Netzwerk.



Wenn Sie eine temporäre lokale Verbindung zum SG6000-CN-Controller herstellen müssen, wenn die 1-GbE-Management-Ports für den aktiv-Backup-Modus konfiguriert sind, entfernen Sie die Kabel von beiden Management-Ports, schließen Sie das temporäre Kabel an den Managementport auf der rechten Seite an und greifen Sie über die IP-Adresse 169.254.0 auf das Gerät zu.



Legende	Netzwerk-Bond-Modus
A	Beide Management-Ports sind mit einem logischen Management-Port verbunden, der mit dem Admin-Netzwerk verbunden ist.
ICH	Der Port auf der linken Seite ist mit dem Admin-Netzwerk verbunden. Der Anschluss rechts ist für temporäre lokale Verbindungen verfügbar (IP-Adresse 169.254.0.1).

Port-Bond-Modi (E5700SG Controller)

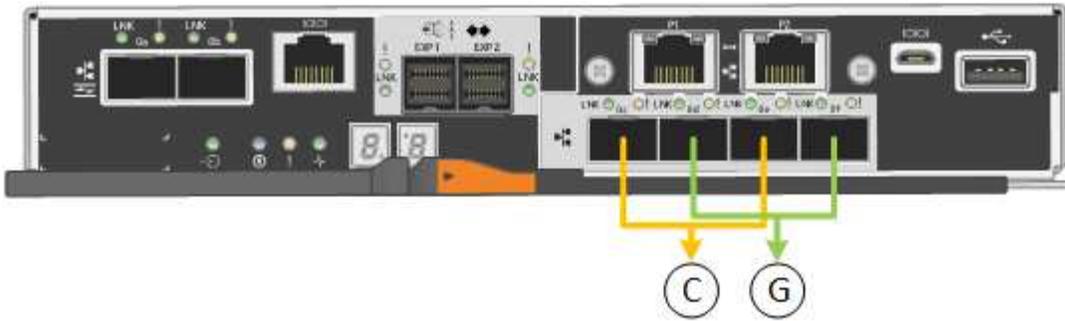
Wenn "[Netzwerk-Links werden konfiguriert](#)" Für den E5700SG-Controller können Sie Port-Bonding für die 10/25-GbE-Ports verwenden, die mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk verbunden sind, sowie für die 1-GbE-Management-Ports, die mit dem optionalen Admin-Netzwerk verbunden werden. Mit Port-Bonding sichern Sie Ihre Daten, indem Sie redundante Pfade zwischen StorageGRID-Netzwerken und der Appliance bereitstellen.

Netzwerk-Bond-Modi für 10/25-GbE-Ports

Die 10/25-GbE-Netzwerk-Ports auf dem E5700SG Controller unterstützen den Bond-Modus für festen Port oder aggregierten Port für die Grid-Netzwerk- und Client-Netzwerkverbindungen.

Bond-Modus mit festem Port

Der Fixed-Modus ist die Standardkonfiguration für 10/25-GbE-Netzwerkports.



Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

Bei Verwendung des Fixed Port Bond-Modus können Sie einen von zwei Netzwerk-Bond-Modi nutzen: Active-Backup oder Link Aggregation Control Protocol (LACP).

- Im aktiv-Backup-Modus (Standard) ist immer nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Port 4 bietet einen Sicherungspfad für Port 2 (Grid Network), und Port 3 stellt einen Sicherungspfad für Port 1 (Client Network) bereit.
- Im LACP-Modus bildet jedes Port-Paar einen logischen Kanal zwischen dem Controller und dem Netzwerk, wodurch ein höherer Durchsatz ermöglicht wird. Wenn ein Port ausfällt, stellt der andere Port den Kanal weiterhin bereit. Der Durchsatz wird verringert, die Konnektivität wird jedoch nicht beeinträchtigt.



Wenn Sie keine redundanten Verbindungen benötigen, können Sie für jedes Netzwerk nur einen Port verwenden. Beachten Sie jedoch, dass nach der Installation von StorageGRID im Grid Manager ein Alarm ausgelöst wird, was darauf hinweist, dass ein Kabel nicht angeschlossen ist. Sie können diesen Alarm sicher bestätigen, um ihn zu löschen.

Bond-Modus für aggregierten Ports

Der Aggregat-Port-Bond-Modus erhöht das ganze für jedes StorageGRID-Netzwerk deutlich und bietet zusätzliche Failover-Pfade.

Legende	Welche Ports sind verbunden
1	Alle verbundenen Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Datenverkehr verwendet werden können.

Wenn Sie planen, den aggregierten Port Bond-Modus zu verwenden:

- Sie müssen LACP Network Bond-Modus verwenden.
- Sie müssen für jedes Netzwerk ein eindeutiges VLAN-Tag angeben. Dieses VLAN-Tag wird zu jedem Netzwerkpaket hinzugefügt, um sicherzustellen, dass der Netzwerkverkehr an das richtige Netzwerk weitergeleitet wird.

- Die Ports müssen mit Switches verbunden sein, die VLAN und LACP unterstützen können. Wenn mehrere Switches an der LACP-Verbindung beteiligt sind, müssen die Switches MLAG (Multi-Chassis Link Aggregation Groups) oder eine vergleichbare Position unterstützen.
- Sie wissen, wie Sie die Switches für die Verwendung von VLAN, LACP und MLAG oder gleichwertig konfigurieren.

Wenn Sie nicht alle vier 10/25-GbE-Ports verwenden möchten, können Sie einen, zwei oder drei Ports verwenden. Durch die Verwendung mehrerer Ports wird die Wahrscheinlichkeit maximiert, dass einige Netzwerkverbindungen verfügbar bleiben, wenn einer der 10/25-GbE-Ports ausfällt.



Wenn Sie weniger als vier Ports verwenden, beachten Sie, dass nach der Installation von StorageGRID ein oder mehrere Alarme im Grid Manager angehoben werden, was darauf hinweist, dass die Kabel nicht angeschlossen sind. Sie können die Alarme sicher bestätigen, um sie zu löschen.

Netzwerk-Bond-Modi für 1-GbE-Management-Ports

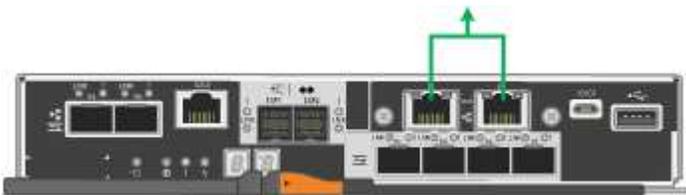
Für die beiden 1-GbE-Management-Ports des E5700SG-Controllers können Sie den Independent Network Bond-Modus oder den Active-Backup-Netzwerk-Bond-Modus wählen, um eine Verbindung zum optionalen Admin-Netzwerk herzustellen.

Im Independent-Modus ist nur Management-Port 1 mit dem Admin-Netzwerk verbunden. Dieser Modus stellt keinen redundanten Pfad bereit. Management-Port 2 bleibt unverkabelt und für temporäre lokale Verbindungen verfügbar (verwenden Sie IP-Adresse 169.254.0.1)

Im Active-Backup-Modus sind beide Management-Ports 1 und 2 mit dem Admin-Netzwerk verbunden. Es ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Die Verbindung dieser beiden physischen Ports zu einem logischen Management-Port bietet einen redundanten Pfad zum Admin-Netzwerk.



Wenn Sie eine temporäre lokale Verbindung zum E5700SG-Controller herstellen müssen, wenn die 1-GbE-Management-Ports für den aktiv-Backup-Modus konfiguriert sind, entfernen Sie die Kabel von beiden Management-Ports, schließen Sie das temporäre Kabel an den Management-Port 2 an und greifen Sie über die IP-Adresse 169.254.0 auf das Gerät zu.



Port-Bond-Modi (SG100 und SG1000)

Wenn Sie Netzwerkverbindungen für die SG100- und SG1000-Appliances konfigurieren, können Sie die Portbindung für die Ports verwenden, die mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk verbunden sind, sowie für die 1-GbE-Management-Ports, die eine Verbindung zum optionalen Admin-Netzwerk herstellen. Mit Port-Bonding sichern Sie Ihre Daten, indem Sie redundante Pfade zwischen StorageGRID-Netzwerken und der Appliance bereitstellen.

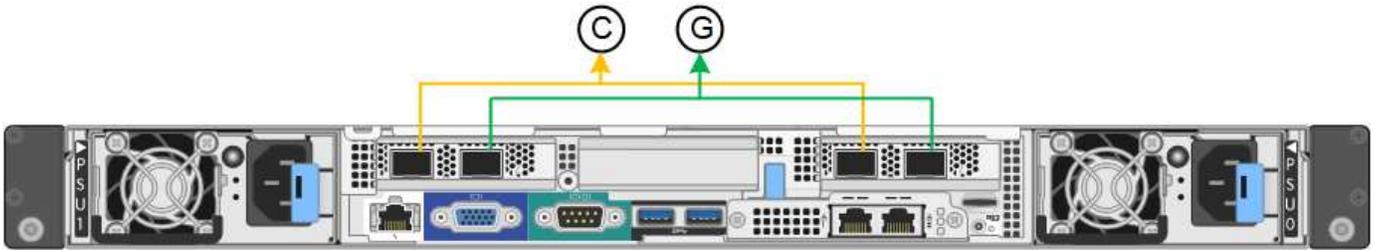
Netzwerk-Bond-Modi

Die Netzwerk-Ports auf der Services-Appliance unterstützen den Bond-Modus mit festen Ports oder den aggregierten Port-Bond-Modus für die Grid-Netzwerk- und Client-Netzwerkverbindungen.

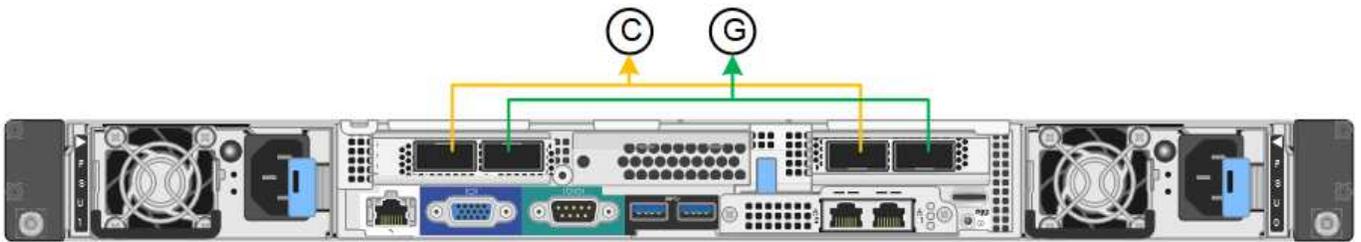
Bond-Modus mit festem Port

Der Fixed-Port-Bond-Modus ist die Standardkonfiguration für die Netzwerk-Ports. Die Abbildungen zeigen, wie die Netzwerk-Ports auf dem SG1000 oder SG100 im Fixed-Port-Bond-Modus gebunden sind.

SG100:



SG1000:



Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

Bei Verwendung des Bond-Modus mit festem Port können die Ports über den aktiv-Backup-Modus oder den Link Aggregation Control Protocol-Modus (LACP 802.3ad) verbunden werden.

- Im aktiv-Backup-Modus (Standard) ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Port 4 bietet einen Sicherungspfad für Port 2 (Grid Network), und Port 3 stellt einen Sicherungspfad für Port 1 (Client Network) bereit.
- Im LACP-Modus bildet jedes Port-Paar einen logischen Kanal zwischen der Services-Appliance und dem Netzwerk, wodurch ein höherer Durchsatz ermöglicht wird. Wenn ein Port ausfällt, stellt der andere Port den Kanal weiterhin bereit. Der Durchsatz wird verringert, die Konnektivität wird jedoch nicht beeinträchtigt.

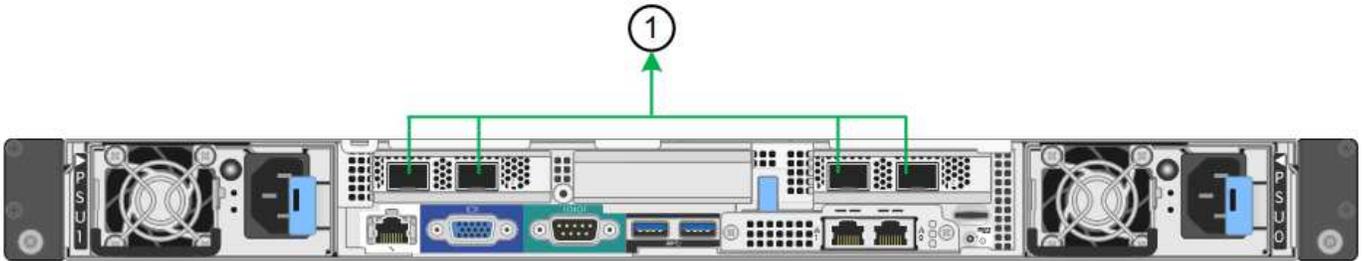


Wenn Sie keine redundanten Verbindungen benötigen, können Sie für jedes Netzwerk nur einen Port verwenden. Beachten Sie jedoch, dass die Meldung **Services Appliance Link Down** nach der Installation von StorageGRID im Grid Manager ausgelöst wird, was darauf hinweist, dass ein Kabel nicht angeschlossen ist. Sie können diese Warnungsregel sicher deaktivieren.

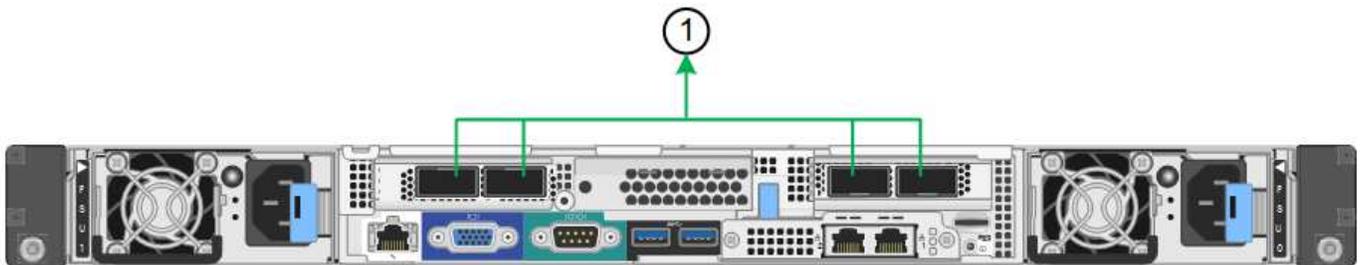
Bond-Modus für aggregierten Ports

Im Aggregat-Port-Bond-Modus wird der Durchsatz jedes StorageGRID-Netzwerks deutlich erhöht und zusätzliche Failover-Pfade bereitgestellt. Diese Abbildungen zeigen, wie die Netzwerk-Ports im aggregierten Port-Bond-Modus verbunden werden.

SG100:



SG1000:



Legende	Welche Ports sind verbunden
1	Alle verbundenen Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Datenverkehr verwendet werden können.

Wenn Sie planen, den aggregierten Port Bond-Modus zu verwenden:

- Sie müssen LACP Network Bond-Modus verwenden.
- Sie müssen für jedes Netzwerk ein eindeutiges VLAN-Tag angeben. Dieses VLAN-Tag wird zu jedem Netzwerkpaket hinzugefügt, um sicherzustellen, dass der Netzwerkverkehr an das richtige Netzwerk weitergeleitet wird.
- Die Ports müssen mit Switches verbunden sein, die VLAN und LACP unterstützen können. Wenn mehrere Switches an der LACP-Verbindung beteiligt sind, müssen die Switches MLAG (Multi-Chassis Link Aggregation Groups) oder eine vergleichbare Position unterstützen.
- Sie wissen, wie Sie die Switches für die Verwendung von VLAN, LACP und MLAG oder gleichwertig konfigurieren.

Wenn Sie nicht alle vier Ports verwenden möchten, können Sie einen, zwei oder drei Ports verwenden. Durch die Verwendung von mehr als einem Port wird die Wahrscheinlichkeit maximiert, dass einige Netzwerkverbindungen verfügbar bleiben, wenn einer der Ports ausfällt.



Wenn Sie weniger als vier Netzwerkanlüsse verwenden möchten, beachten Sie, dass nach der Installation des Appliance-Knotens im Grid Manager möglicherweise eine Warnmeldung für die **Services-Appliance-Verbindung aus** ausgelöst wird, was darauf hinweist, dass ein Kabel nicht angeschlossen ist. Sie können diese Warnungsregel für die ausgelöste Warnmeldung sicher deaktivieren.

Network Bond-Modi für Management-Ports

Für die beiden 1-GbE-Management-Ports auf der Services-Appliance können Sie den unabhängigen Netzwerk-Bond-Modus oder den aktiv-Backup-Netzwerk-Bond-Modus wählen, um eine Verbindung mit dem optionalen Admin-Netzwerk herzustellen. Diese Abbildungen zeigen, wie die Management-Ports auf den Appliances im Netzwerk-Bond-Modus für das Admin-Netzwerk verbunden sind.

SG100:



SG1000:



Legende	Netzwerk-Bond-Modus
A	Aktiv-Backup-Modus. Beide Management-Ports sind mit einem logischen Management-Port verbunden, der mit dem Admin-Netzwerk verbunden ist.
ICH	Unabhängiger Modus. Der Port auf der linken Seite ist mit dem Admin-Netzwerk verbunden. Der Anschluss rechts ist für temporäre lokale Verbindungen verfügbar (IP-Adresse 169.254.0.1).

Im Independent-Modus ist nur der Management-Port links mit dem Admin-Netzwerk verbunden. Dieser Modus stellt keinen redundanten Pfad bereit. Der Management Port auf der rechten Seite ist nicht verbunden und für temporäre lokale Verbindungen verfügbar (verwendet IP-Adresse 169.254.0.1)

Im Active-Backup-Modus sind beide Management-Ports mit dem Admin-Netzwerk verbunden. Es ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Die Verbindung dieser beiden physischen Ports zu einem logischen Management-Port bietet einen redundanten Pfad zum Admin-Netzwerk.



Wenn Sie eine temporäre lokale Verbindung zur Services-Appliance herstellen müssen, wenn die 1-GbE-Management-Ports für den aktiv-Backup-Modus konfiguriert sind, entfernen Sie die Kabel von beiden Management-Ports, schließen Sie das temporäre Kabel an den Verwaltungsport rechts an und greifen Sie über die IP-Adresse 169.254.0 auf das Gerät zu.

Sammeln Sie Installationsinformationen

Sammeln Sie Installationsinformationen: Übersicht

Während der Installation und Konfiguration einer StorageGRID Appliance treffen Sie Entscheidungen und sammeln Informationen über Ethernet Switch Ports, IP-Adressen sowie Port- und Network Bond-Modi.

Lesen Sie die Anweisungen für Ihr Gerät, um herauszufinden, welche Informationen Sie benötigen:

- "SGF6112"
- "SG6000"
- "SG5700"
- "SG100 und SG1000"

Alternativ können Sie mit Ihrem NetApp Professional Services Consultant zusammenarbeiten, um die Konfigurationsschritte mit dem NetApp ConfigBuilder Tool zu optimieren und zu automatisieren. Siehe ["Automatisierung der Appliance-Installation und -Konfiguration"](#).

Installationsdaten sammeln (SGF6112)

Notieren Sie anhand der folgenden Tabellen die erforderlichen Informationen für jedes Netzwerk, das Sie mit dem Gerät verbinden. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.



Verwenden Sie anstelle der Tabellen das mit ConfigBuilder bereitgestellte Arbeitsbuch. Mit der Arbeitsmappe „ConfigBuilder“ können Sie Ihre Systeminformationen hochladen und eine JSON-Datei erstellen, um einige Konfigurationsschritte im Installationsprogramm für StorageGRID-Appliances automatisch auszuführen. Siehe ["Automatisierung der Appliance-Installation und -Konfiguration"](#).

Überprüfen Sie die StorageGRID-Version

Vergewissern Sie sich vor der Installation einer SGF6112-Appliance, dass Ihr StorageGRID-System eine erforderliche Version der StorageGRID-Software verwendet.

Appliance	Erforderliche StorageGRID Version
SGF6112	11.7 oder höher (neuester Hotfix empfohlen)

Administrations- und Wartungs-Ports

Das Admin-Netzwerk für StorageGRID ist ein optionales Netzwerk, das zur Systemadministration und -Wartung verwendet wird. Die Appliance stellt über die folgenden Ports auf der Appliance eine Verbindung zum Admin-Netzwerk her.

Die folgende Abbildung zeigt die RJ-45-Ports am SG6112-Gerät.



Erforderliche Informationen	Ihr Wert
Admin-Netzwerk aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein • Ja (Standard)
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Unabhängig (Standard) • Aktiv/Backup
Switch-Port für den im Diagramm eingekreisten linken Port (Standard-aktiver Port für unabhängigen Netzwerk-Bond-Modus)	
Switch-Port für den rechten Port im Diagramm eingekreist (nur aktiv-Backup-Netzwerk-Bond-Modus)	
MAC-Adresse für den Netzwerkport Admin Hinweis: das MAC-Adressenetikett auf der Vorderseite des Geräts listet die MAC-Adresse für den BMC-Verwaltungspport auf. Um die MAC-Adresse für den Admin-Netzwerkanschluss zu ermitteln, müssen Sie der Hexadezimalzahl auf dem Etikett 2 hinzufügen. Wenn die MAC-Adresse auf dem Etikett beispielsweise mit 09 endet, endet die MAC-Adresse für den Admin-Port in 0B . Wenn die MAC-Adresse auf dem Etikett mit (y)FF endet, endet die MAC-Adresse für den Admin-Port in (y+1)01 . Sie können diese Berechnung einfach durchführen, indem Sie den Rechner unter Windows öffnen, ihn auf den Programmiermodus setzen, Hex auswählen, die MAC-Adresse eingeben und dann + 2 = eingeben.	
DHCP-zugewiesene IP-Adresse für den Admin-Netzwerkport, sofern nach dem Einschalten verfügbar Hinweis: Sie können die IP-Adresse ermitteln, die über DHCP zugewiesen wurde, indem Sie die MAC-Adresse verwenden, um die zugewiesene IP zu ermitteln.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den Appliance-Knoten im Admin-Netzwerk verwenden möchten Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:

Erforderliche Informationen	Ihr Wert
Admin-Netzwerk-Subnetze (CIDR)	

Netzwerkports

Die vier Netzwerkports auf der Appliance werden mit dem StorageGRID-Grid-Netzwerk und dem optionalen Client-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Verbindungsgeschwindigkeit	Wählen Sie für die SGF6112 eine der folgenden Optionen: <ul style="list-style-type: none"> • Auto (Standard) • 10 GBitE • 25 GBitE
Port Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Fest (Standard) • Aggregat
Switch-Port für Port 1 (Client-Netzwerk für festen Modus)	
Switch-Port für Port 2 (Grid-Netzwerk für Fixed-Modus)	
Switch-Port für Port 3 (Client-Netzwerk für festen Modus)	
Switch-Port für Port 4 (Grid-Netzwerk für Fixed-Modus)	

Grid-Netzwerkports

Das Grid-Netzwerk für StorageGRID ist ein erforderliches Netzwerk, das für den gesamten internen StorageGRID-Datenverkehr verwendet wird. Die Appliance wird über die vier Netzwerk-Ports mit dem Grid-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Aktiv/Backup (Standard) • LACP (802.3ad)

Erforderliche Informationen	Ihr Wert
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
VLAN Tag (wenn VLAN Tagging aktiviert ist)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Grid-Netzwerk, sofern nach dem Einschalten verfügbar	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den Appliance-Node im Grid-Netzwerk verwenden möchten Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Grid-Netzwerknetze (CIDRs)	
Einstellung für maximale Übertragungseinheit (MTU) (optional). Sie können den Standardwert 1500 verwenden oder die MTU auf einen für Jumbo Frames geeigneten Wert einstellen, z. B. 9000.	

Client-Netzwerkports

Das Client-Netzwerk für StorageGRID ist ein optionales Netzwerk, das in der Regel für den Zugriff auf das Grid auf das Clientprotokoll verwendet wird. Die Appliance wird über die vier Netzwerk-Ports mit dem Client-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Client-Netzwerk aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.

Erforderliche Informationen	Ihr Wert
VLAN-Tag (bei aktiviertem VLAN-Tagging)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Client-Netzwerk, falls nach dem Einschalten verfügbar	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:
Statische IP-Adresse, die Sie für den Appliance-Knoten im Client-Netzwerk verwenden möchten Hinweis: Wenn das Client-Netzwerk aktiviert ist, verwendet die Standardroute auf dem Gerät das hier angegebene Gateway.	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:

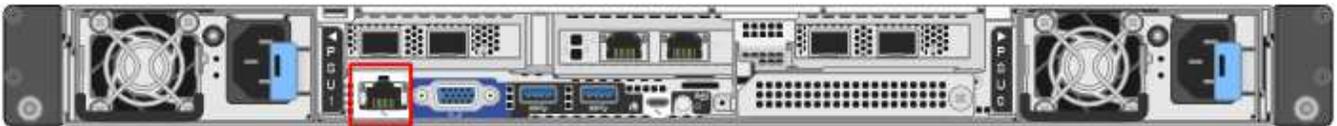
BMC-Management-Netzwerk-Ports

Sie können auf die BMC-Schnittstelle auf der Appliance über den in der Abbildung eingekreisten 1-GbE-Managementport zugreifen. Dieser Port unterstützt die Remote-Verwaltung der Controller-Hardware über Ethernet unter Verwendung des IPMI-Standards (Intelligent Platform Management Interface).



Sie können den Remote-IPMI-Zugriff für alle Appliances aktivieren oder deaktivieren, die einen BMC enthalten, indem Sie den privaten Endpunkt der Management-API VERWENDEN, PUT /private/bmc.

Die folgende Abbildung zeigt den BMC-Managementport auf der SG6112-Appliance.



Erforderliche Informationen	Ihr Wert
Ethernet-Switch-Port Sie stellen eine Verbindung zum BMC-Management-Port her (im Diagramm eingekreist).	
DHCP-zugewiesene IP-Adresse für das BMC-Managementnetzwerk, sofern nach dem Einschalten verfügbar	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:
Statische IP-Adresse, die Sie für den BMC-Verwaltungsport verwenden möchten	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:

Verwandte Informationen

- ["Kabelgerät \(SGF6112\)"](#)
- ["Konfigurieren Sie StorageGRID-IP-Adressen"](#)

Erfassen von Installationsinformationen (SG6000)

Notieren Sie die erforderlichen Informationen für jedes Netzwerk, das Sie mit dem Gerät verbinden, in den Tabellen. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.



Verwenden Sie anstelle der Tabellen das mit ConfigBuilder bereitgestellte Arbeitsbuch. Mit der Arbeitsmappe „ConfigBuilder“ können Sie Ihre Systeminformationen hochladen und eine JSON-Datei erstellen, um einige Konfigurationsschritte im Installationsprogramm für StorageGRID-Appliances automatisch auszuführen. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

Erforderliche Informationen für die Verbindung mit SANtricity System Manager auf Storage Controllern

Beide Storage-Controller in der Appliance (entweder die Controller der E2800 Serie oder die EF570 Controller) werden mit dem Managementnetzwerk verbunden, das Sie für SANtricity System Manager verwenden. Die Controller befinden sich in jeder Appliance wie folgt:

- SG6060 und SG6060X: Controller A befindet sich oben und Controller B befindet sich unten.
- SGF6024: Controller A befindet sich auf der linken Seite, und Controller B befindet sich auf der rechten Seite.

Erforderliche Informationen	Ihr Wert für Controller A	Ihr Wert für Controller B
Ethernet-Switch-Port Sie werden eine Verbindung zu Management-Port 1 herstellen (gekennzeichnet mit P1 auf dem Controller).		
MAC-Adresse für Management-Port 1 (auf einem Etikett in der Nähe von Port P1 gedruckt)		
Über DHCP zugewiesene IP-Adresse für Management-Port 1, sofern nach dem Einschalten verfügbar Hinweis: Wenn das Netzwerk, das Sie mit dem Speicher-Controller verbinden, einen DHCP-Server enthält, kann der Netzwerkadministrator die MAC-Adresse verwenden, um die vom DHCP-Server zugewiesene IP-Adresse zu ermitteln.		

Erforderliche Informationen	Ihr Wert für Controller A	Ihr Wert für Controller B
Statische IP-Adresse, die Sie für die Appliance im Managementnetzwerk verwenden möchten	Für IPv4: <ul style="list-style-type: none"> • IPv4-Adresse: • Subnetzmaske: • Gateway: Für IPv6: <ul style="list-style-type: none"> • IPv6-Adresse: • Routingfähige IP-Adresse: • IP-Adresse des Storage Controller-Routers: 	Für IPv4: <ul style="list-style-type: none"> • IPv4-Adresse: • Subnetzmaske: • Gateway: Für IPv6: <ul style="list-style-type: none"> • IPv6-Adresse: • Routingfähige IP-Adresse: • IP-Adresse des Storage Controller-Routers:
IP-Adressformat	Bitte auswählen: <ul style="list-style-type: none"> • IPv4 • IPv6 	Bitte auswählen: <ul style="list-style-type: none"> • IPv4 • IPv6
Geschwindigkeit und Duplexmodus Hinweis: Sie müssen sicherstellen, dass der Ethernet-Switch für das SANtricity-System-Manager-Managementnetzwerk auf Autonegotiation gesetzt ist.	Muss sein: <ul style="list-style-type: none"> • Autonegotiation (Standard) 	Muss sein: <ul style="list-style-type: none"> • Autonegotiation (Standard)

Zum Anschließen des SG6000-CN-Controllers an das Admin-Netzwerk erforderliche Informationen

Das Admin-Netzwerk für StorageGRID ist ein optionales Netzwerk, das zur Systemadministration und -Wartung verwendet wird. Die Appliance stellt über die folgenden 1-GbE-Management-Ports des SG6000-CN-Controllers eine Verbindung zum Admin-Netzwerk her.



Erforderliche Informationen	Ihr Wert
Admin-Netzwerk aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein • Ja (Standard)
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Unabhängig (Standard) • Aktiv/Backup

Erforderliche Informationen	Ihr Wert
Switch-Port für den linken Port im roten Kreis im Diagramm (Standard-aktiv-Port für unabhängigen Netzwerk-Bond-Modus)	
Switch-Port für den rechten Port im roten Kreis im Diagramm (nur aktiv-Backup Netzwerk-Bond-Modus)	
<p>MAC-Adresse für den Netzwerkport Admin</p> <p>Hinweis: das MAC-Adressenetikett auf der Vorderseite des SG6000-CN Controllers listet die MAC-Adresse für den BMC-Management-Port auf. Um die MAC-Adresse für den Admin-Netzwerkanschluss zu ermitteln, müssen Sie der Hexadezimalzahl auf dem Etikett 2 hinzufügen. Wenn die MAC-Adresse auf dem Etikett beispielsweise mit 09 endet, endet die MAC-Adresse für den Admin-Port in 0B. Wenn die MAC-Adresse auf dem Etikett mit (y)FF endet, endet die MAC-Adresse für den Admin-Port in (y+1)01. Sie können diese Berechnung einfach durchführen, indem Sie den Rechner unter Windows öffnen, ihn auf den Programmiermodus setzen, Hex auswählen, die MAC-Adresse eingeben und dann + 2 = eingeben.</p>	
<p>DHCP-zugewiesene IP-Adresse für den Admin-Netzwerkport, sofern nach dem Einschalten verfügbar</p> <p>Hinweis: Sie können die IP-Adresse ermitteln, die über DHCP zugewiesen wurde, indem Sie die MAC-Adresse verwenden, um die zugewiesene IP zu ermitteln.</p>	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
<p>Statische IP-Adresse, die Sie für den Appliance-Speicherknoten im Admin-Netzwerk verwenden möchten</p> <p>Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.</p>	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Admin-Netzwerk-Subnetze (CIDR)	

Erforderliche Informationen zum Verbinden und Konfigurieren von 10/25-GbE-Ports am SG6000-CN Controller

Die vier 10/25-GbE-Ports des SG6000-CN-Controllers stellen eine Verbindung zum StorageGRID-Grid-Netzwerk und dem optionalen Client-Netzwerk her.

Erforderliche Informationen	Ihr Wert
Verbindungsgeschwindigkeit	<p>Bitte auswählen:</p> <ul style="list-style-type: none"> • Auto (Standard) • 10 GBitE • 25 GBitE

Erforderliche Informationen	Ihr Wert
Port Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Fest (Standard) • Aggregat
Switch-Port für Port 1 (Client-Netzwerk für festen Modus)	
Switch-Port für Port 2 (Grid-Netzwerk für Fixed-Modus)	
Switch-Port für Port 3 (Client-Netzwerk für festen Modus)	
Switch-Port für Port 4 (Grid-Netzwerk für Fixed-Modus)	

Informationen zum Anschließen des SG6000-CN-Controllers an das Grid-Netzwerk erforderlich

Das Grid-Netzwerk für StorageGRID ist ein erforderliches Netzwerk, das für den gesamten internen StorageGRID-Datenverkehr verwendet wird. Die Appliance wird über die 10/25-GbE-Ports des SG6000-CN-Controllers mit dem Grid-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
VLAN-Tag (bei aktiviertem VLAN-Tagging)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Grid-Netzwerk, sofern nach dem Einschalten verfügbar	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den Appliance-Speicherknoten im Grid-Netzwerk verwenden möchten Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Grid-Netzwerknetze (CIDRs)	

Informationen zum Anschließen des SG6000-CN-Controllers an das Client-Netzwerk erforderlich

Das Client-Netzwerk für StorageGRID ist ein optionales Netzwerk, das in der Regel für den Zugriff auf das Grid auf das Clientprotokoll verwendet wird. Die Appliance wird über die 10/25-GbE-Ports des SG6000-CN-Controllers mit dem Client-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Client-Netzwerk aktiviert	Bitte auswählen: <ul style="list-style-type: none">• Nein (Standard)• Ja.
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none">• Aktiv/Backup (Standard)• LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none">• Nein (Standard)• Ja.
VLAN-Tag (bei aktiviertem VLAN-Tagging)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Client-Netzwerk, falls nach dem Einschalten verfügbar	<ul style="list-style-type: none">• IPv4-Adresse (CIDR):• Gateway:
Statische IP-Adresse, die Sie für den Appliance-Speicherknoten im Client-Netzwerk verwenden möchten	<ul style="list-style-type: none">• IPv4-Adresse (CIDR):• Gateway:
Hinweis: Wenn das Client-Netzwerk aktiviert ist, verwendet die Standardroute auf dem Controller das hier angegebene Gateway.	

Informationen zum Anschließen des SG6000-CN Controllers an das BMC-Managementnetzwerk erforderlich

Sie können über den folgenden 1-GbE-Management-Port auf die BMC-Schnittstelle des SG6000-CN Controllers zugreifen. Dieser Port unterstützt die Remote-Verwaltung der Controller-Hardware über Ethernet unter Verwendung des IPMI-Standards (Intelligent Platform Management Interface).



Sie können den Remote-IPMI-Zugriff für alle Appliances aktivieren oder deaktivieren, die einen BMC enthalten, indem Sie den privaten Endpunkt der Management-API VERWENDEN, PUT /private/bmc.

Erforderliche Informationen	Ihr Wert
Ethernet-Switch-Port Sie stellen eine Verbindung zum BMC-Management-Port her (im Diagramm eingekreist).	
DHCP-zugewiesene IP-Adresse für das BMC-Managementnetzwerk, sofern nach dem Einschalten verfügbar	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den BMC-Verwaltungsport verwenden möchten	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:

Verwandte Informationen

- ["SG6000 Controller"](#)
- ["Überprüfen Sie die Appliance-Netzwerkverbindungen"](#)
- ["Port-Bond-Modi \(SG6000-CN-Controller\)"](#)
- ["Kabelgerät \(SG6000\)"](#)
- ["Konfigurieren Sie StorageGRID-IP-Adressen"](#)

Installationsinformationen (SG5700) erfassen

Notieren Sie die erforderlichen Informationen für jedes Netzwerk, das Sie mit dem Gerät verbinden, in den Tabellen. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.



Verwenden Sie anstelle der Tabellen das mit ConfigBuilder bereitgestellte Arbeitsbuch. Mit der Arbeitsmappe „ConfigBuilder“ können Sie Ihre Systeminformationen hochladen und eine JSON-Datei erstellen, um einige Konfigurationsschritte im Installationsprogramm für StorageGRID-Appliances automatisch auszuführen. Siehe ["Automatisierung der Appliance-Installation und -Konfiguration"](#).

Für die Verbindung mit SANtricity System Manager auf dem E2800 Controller erforderliche Informationen

Sie verbinden den Controller der E2800 Serie mit dem Managementnetzwerk, das Sie für SANtricity System Manager verwenden.

Erforderliche Informationen	Ihr Wert
Ethernet-Switch-Port die Verbindung zum Management-Port 1 wird hergestellt	
MAC-Adresse für Management-Port 1 (auf einem Etikett in der Nähe von Port P1 gedruckt)	

Erforderliche Informationen	Ihr Wert
<p>Über DHCP zugewiesene IP-Adresse für Management-Port 1, sofern nach dem Einschalten verfügbar</p> <p>Hinweis: Wenn das Netzwerk, das Sie mit dem E2800-Controller verbinden, einen DHCP-Server enthält, kann der Netzwerkadministrator die MAC-Adresse verwenden, um die vom DHCP-Server zugewiesene IP-Adresse zu ermitteln.</p>	
<p>Geschwindigkeit und Duplexmodus</p> <p>Hinweis: Sie müssen sicherstellen, dass der Ethernet-Switch für das SANtricity-System-Manager-Managementnetzwerk auf Autonegotiation gesetzt ist.</p>	<p>Muss sein:</p> <ul style="list-style-type: none"> • Autonegotiation (Standard)
<p>IP-Adressformat</p>	<p>Bitte auswählen:</p> <ul style="list-style-type: none"> • IPv4 • IPv6
<p>Statische IP-Adresse, die Sie für die Appliance im Managementnetzwerk verwenden möchten</p>	<p>Für IPv4:</p> <ul style="list-style-type: none"> • IPv4-Adresse: • Subnetzmaske: • Gateway: <p>Für IPv6:</p> <ul style="list-style-type: none"> • IPv6-Adresse: • Routingfähige IP-Adresse: • E2800 Controller-Router-IP-Adresse:

Für die Verbindung des E5700SG-Controllers mit dem Admin-Netzwerk erforderliche Informationen

Das Admin-Netzwerk für StorageGRID ist ein optionales Netzwerk, das zur Systemadministration und -Wartung verwendet wird. Die Appliance wird über die 1-GbE-Management-Ports des E5700SG Controllers mit dem Admin-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
<p>Admin-Netzwerk aktiviert</p>	<p>Bitte auswählen:</p> <ul style="list-style-type: none"> • Nein • Ja (Standard)

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Unabhängig • Aktiv/Backup
Switch-Port für Port 1	
Switch-Port für Port 2 (nur aktiv-Backup-Netzwerk-Bond-Modus)	
Über DHCP zugewiesene IP-Adresse für Management-Port 1, sofern nach dem Einschalten verfügbar Hinweis: enthält das Admin-Netzwerk einen DHCP-Server, zeigt der E5700SG-Controller nach dem Start die DHCP-zugewiesene IP-Adresse auf seinem 7-Segment-Display an. Sie können auch die IP-Adresse bestimmen, die über DHCP zugewiesen wurde, indem Sie die MAC-Adresse verwenden, um die zugewiesene IP-Adresse zu ermitteln.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den Appliance-Speicherknoten im Admin-Netzwerk verwenden möchten Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Admin-Netzwerk-Subnetze (CIDR)	

Erforderliche Informationen zum Verbinden und Konfigurieren von 10/25-GbE-Ports auf dem E5700SG Controller

Die vier 10/25-GbE-Ports des E5700SG-Controllers stellen eine Verbindung zum StorageGRID-Grid-Netzwerk und dem Client-Netzwerk her.



Siehe "[Port-Bond-Modi \(E5700SG Controller\)](#)".

Erforderliche Informationen	Ihr Wert
Verbindungsgeschwindigkeit Hinweis: Wenn Sie 25 GbE wählen, installieren Sie SPF28 Transceiver. Autonegotiation wird nicht unterstützt, daher müssen Sie auch die Ports und die verbundenen Switches für 25 GbE konfigurieren.	Bitte auswählen: <ul style="list-style-type: none"> • 10 GbE (Standard) • 25 GbE
Port Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Fest (Standard) • Aggregat

Erforderliche Informationen	Ihr Wert
Switch-Port für Port 1 (Client-Netzwerk)	
Switch-Port für Port 2 (Grid-Netzwerk)	
Switch-Port für Port 3 (Client-Netzwerk)	
Switch-Port für Port 4 (Grid-Netzwerk)	

Zum Verbinden des E5700SG-Controllers mit dem Grid-Netzwerk erforderliche Informationen

Das Grid-Netzwerk für StorageGRID ist ein erforderliches Netzwerk, das für den gesamten internen StorageGRID-Datenverkehr verwendet wird. Die Appliance wird über die 10/25-GbE-Ports des E5700SG-Controllers mit dem Grid-Netzwerk verbunden.



Siehe "[Port-Bond-Modi \(E5700SG Controller\)](#)".

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
VLAN-Tag (bei aktiviertem VLAN-Tagging)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Grid-Netzwerk, sofern nach dem Einschalten verfügbar Hinweis: enthält das Grid-Netzwerk einen DHCP-Server, zeigt der E5700SG-Controller nach dem Start die DHCP-zugewiesene IP-Adresse für das Grid-Netzwerk auf seiner 7-Segment-Anzeige an.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den Appliance-Speicherknoten im Grid-Netzwerk verwenden möchten Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:

Erforderliche Informationen	Ihr Wert
Grid-Netzwerknetze (CIDR) Hinweis: Wenn das Client-Netzwerk nicht aktiviert ist, verwendet die Standardroute auf dem Controller das hier angegebene Gateway.	

Für die Verbindung des E5700SG-Controllers mit dem Client-Netzwerk erforderliche Informationen

Das Client-Netzwerk für StorageGRID ist ein optionales Netzwerk, das in der Regel für den Zugriff auf das Grid auf das Clientprotokoll verwendet wird. Die Appliance wird über die 10/25-GbE-Ports des E5700SG-Controllers mit dem Client-Netzwerk verbunden.



Siehe "[Port-Bond-Modi \(E5700SG Controller\)](#)".

Erforderliche Informationen	Ihr Wert
Client-Netzwerk aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
VLAN-Tag (Bei aktiviertem VLAN-Tagging)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Client-Netzwerk, falls nach dem Einschalten verfügbar	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den Appliance-Speicherknoten im Client-Netzwerk verwenden möchten Hinweis: Wenn das Client-Netzwerk aktiviert ist, verwendet die Standardroute auf dem Controller das hier angegebene Gateway.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:

Verwandte Informationen

- "[Netzwerkverbindungen \(SG5700\)](#)"
- "[Port-Bond-Modi \(E5700SG Controller\)](#)"

- ["Hardware konfigurieren \(SG5700\)"](#)

Erfassen von Installationsinformationen (SG100 und SG1000)

Notieren Sie die erforderlichen Informationen für jedes Netzwerk, das Sie mit dem Gerät verbinden, in den Tabellen. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.



Verwenden Sie anstelle der Tabellen das mit ConfigBuilder bereitgestellte Arbeitsbuch. Mit der Arbeitsmappe „ConfigBuilder“ können Sie Ihre Systeminformationen hochladen und eine JSON-Datei erstellen, um einige Konfigurationsschritte im Installationsprogramm für StorageGRID-Appliances automatisch auszuführen. Siehe ["Automatisierung der Appliance-Installation und -Konfiguration"](#).

Überprüfen Sie die StorageGRID-Version

Vergewissern Sie sich vor der Installation einer SG100- oder SG1000-Service-Appliance, dass Ihr StorageGRID-System eine erforderliche Version der StorageGRID-Software verwendet.

Appliance	Erforderliche StorageGRID Version
SG1000	11.3 oder höher (letzter Hotfix empfohlen)
SG100	11.4 oder höher (letzter Hotfix empfohlen)

Administrations- und Wartungs-Ports

Das Admin-Netzwerk für StorageGRID ist ein optionales Netzwerk, das zur Systemadministration und -Wartung verwendet wird. Die Appliance stellt über die folgenden 1-GbE-Management-Ports auf der Appliance eine Verbindung zum Admin-Netzwerk her.

SG100 RJ-45-Ports:



SG1000 RJ-45-Ports:



Erforderliche Informationen	Ihr Wert
Admin-Netzwerk aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein • Ja (Standard)

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Unabhängig (Standard) • Aktiv/Backup
Switch-Port für den im Diagramm eingekreisten linken Port (Standard-aktiver Port für unabhängigen Netzwerk-Bond-Modus)	
Switch-Port für den rechten Port im Diagramm eingekreist (nur aktiv-Backup-Netzwerk-Bond-Modus)	
<p>MAC-Adresse für den Netzwerkport Admin</p> <p>Hinweis: das MAC-Adressenetikett auf der Vorderseite des Geräts listet die MAC-Adresse für den BMC-Verwaltungsport auf. Um die MAC-Adresse für den Admin-Netzwerk-Port zu ermitteln, fügen Sie 2 zur Hexadezimalzahl auf dem Etikett hinzu. Wenn die MAC-Adresse auf dem Etikett beispielsweise mit 09 endet, endet die MAC-Adresse für den Admin-Port in 0B. Wenn die MAC-Adresse auf dem Etikett mit (y)FF endet, endet die MAC-Adresse für den Admin-Port in (y+1)01. Sie können diese Berechnung einfach durchführen, indem Sie den Rechner unter Windows öffnen, ihn auf den Programmiermodus setzen, Hex auswählen, die MAC-Adresse eingeben und dann + 2 = eingeben.</p>	
<p>DHCP-zugewiesene IP-Adresse für den Admin-Netzwerkport, sofern nach dem Einschalten verfügbar</p> <p>Hinweis: Sie können die IP-Adresse ermitteln, die über DHCP zugewiesen wurde, indem Sie die MAC-Adresse verwenden, um die zugewiesene IP zu ermitteln.</p>	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
<p>Statische IP-Adresse, die Sie für den Appliance-Knoten im Admin-Netzwerk verwenden möchten</p> <p>Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.</p>	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Admin-Netzwerk-Subnetze (CIDR)	

Netzwerkports

Die vier Netzwerkports auf der Appliance werden mit dem StorageGRID-Grid-Netzwerk und dem optionalen Client-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Verbindungsgeschwindigkeit	<p>Wählen Sie für das SG100 eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> • Auto (Standard) • 10 GBitE • 25 GBitE <p>Wählen Sie für den SG1000 eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> • Auto (Standard) • 10 GBitE • 25 GBitE • 40 GBitE • 100 GBitE <p>Hinweis: für die SG1000-, 10- und 25-GbE-Geschwindigkeiten sind QSA-Adapter erforderlich.</p>
Port Bond-Modus	<p>Bitte auswählen:</p> <ul style="list-style-type: none"> • Fest (Standard) • Aggregat
Switch-Port für Port 1 (Client-Netzwerk für festen Modus)	
Switch-Port für Port 2 (Grid-Netzwerk für Fixed-Modus)	
Switch-Port für Port 3 (Client-Netzwerk für festen Modus)	
Switch-Port für Port 4 (Grid-Netzwerk für Fixed-Modus)	

Grid-Netzwerkports

Das Grid-Netzwerk für StorageGRID ist ein erforderliches Netzwerk, das für den gesamten internen StorageGRID-Datenverkehr verwendet wird. Die Appliance wird über die vier Netzwerk-Ports mit dem Grid-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	<p>Bitte auswählen:</p> <ul style="list-style-type: none"> • Aktiv/Backup (Standard) • LACP (802.3ad)

Erforderliche Informationen	Ihr Wert
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
VLAN-Tag (bei aktiviertem VLAN-Tagging)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Grid-Netzwerk, sofern nach dem Einschalten verfügbar	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den Appliance-Node im Grid-Netzwerk verwenden möchten Hinweis: Wenn Ihr Netzwerk kein Gateway hat, geben Sie die gleiche statische IPv4-Adresse für das Gateway an.	<ul style="list-style-type: none"> • IPv4-Adresse (CIDR): • Gateway:
Grid-Netzwerknetze (CIDRs)	
Einstellung für maximale Übertragungseinheit (MTU) (optional) Sie können den Standardwert von 1500 verwenden oder die MTU auf einen Wert setzen, der für Jumbo-Frames geeignet ist, z. B. 9000.	

Client-Netzwerkports

Das Client-Netzwerk für StorageGRID ist ein optionales Netzwerk, das in der Regel für den Zugriff auf das Grid auf das Clientprotokoll verwendet wird. Die Appliance wird über die vier Netzwerk-Ports mit dem Client-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Client-Netzwerk aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.
Netzwerk-Bond-Modus	Bitte auswählen: <ul style="list-style-type: none"> • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: <ul style="list-style-type: none"> • Nein (Standard) • Ja.

Erforderliche Informationen	Ihr Wert
VLAN-Tag (wenn VLAN-Tagging aktiviert ist)	Geben Sie einen Wert zwischen 0 und 4095 ein:
DHCP-zugewiesene IP-Adresse für das Client-Netzwerk, falls nach dem Einschalten verfügbar	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:
Statische IP-Adresse, die Sie für den Appliance-Knoten im Client-Netzwerk verwenden möchten Hinweis: Wenn das Client-Netzwerk aktiviert ist, verwendet die Standardroute auf dem Gerät das hier angegebene Gateway.	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:

BMC-Management-Netzwerk-Ports

Sie können über den in der Abbildung eingekreisten 1-GbE-Managementport auf die BMC-Schnittstelle auf der Services-Appliance zugreifen. Dieser Port unterstützt die Remote-Verwaltung der Controller-Hardware über Ethernet unter Verwendung des IPMI-Standards (Intelligent Platform Management Interface).



Sie können den Remote-IPMI-Zugriff für alle Appliances aktivieren oder deaktivieren, die einen BMC enthalten, indem Sie den privaten Endpunkt der Management-API VERWENDEN, PUT /private/bmc.

BMC-Management-Port SG100:



SG1000 BMC-Management-Port:



Erforderliche Informationen	Ihr Wert
Ethernet-Switch-Port Sie stellen eine Verbindung zum BMC-Management-Port her (im Diagramm eingekreist).	
DHCP-zugewiesene IP-Adresse für das BMC-Managementnetzwerk, sofern nach dem Einschalten verfügbar	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:
Statische IP-Adresse, die Sie für den BMC-Verwaltungsport verwenden möchten	<ul style="list-style-type: none"> IPv4-Adresse (CIDR): Gateway:

Verwandte Informationen

- ["Kabelgerät \(SG100 und SG1000\)"](#)
- ["Konfigurieren Sie StorageGRID-IP-Adressen"](#)

Automatisierung der Appliance-Installation und -Konfiguration

Eine Automatisierung von Installation und Konfiguration kann sich bei der Implementierung mehrerer StorageGRID Instanzen oder einer großen, komplexen StorageGRID Instanz als nützlich erweisen.

Mithilfe der NetApp StorageGRID Tools können Sie die Installation und Konfiguration Ihrer StorageGRID Appliances automatisieren. Nach der Installation und Konfiguration der Appliances können Sie dies tun ["Automatisieren Sie die Konfiguration des gesamten StorageGRID Systems"](#).

Sie können die Konfiguration folgender Komponenten automatisieren:

- IP-Adressen für Grid-Netzwerk, Admin-Netzwerk und Client-Netzwerk
- BMC Schnittstelle
- Netzwerkverbindungen
 - Port Bond-Modus
 - Netzwerk-Bond-Modus
 - Verbindungsgeschwindigkeit

Automatisierungsoptionen

Um die Installation und Konfiguration der Appliance zu automatisieren, verwenden Sie eine oder mehrere der folgenden Optionen:

- Generieren Sie eine JSON-Datei mit Konfigurationsdetails. Verwenden Sie zusammen mit Ihrem NetApp Professional Services Berater das ["NetApp ConfigBuilder Tool"](#) Gehen Sie wie folgt vor:

Schritt	Beratung für NetApp Professional Services	Verwenden Sie ConfigBuilder
1	Auftragsnummer abrufen	
2		Arbeitsbuch erhalten
3	Das Arbeitsbuch ausfüllen	
4		Arbeitsmappe hochladen
5		JSON-Datei generieren
6	Laden Sie die JSON-Datei in die Appliance hoch	



Sie können mehrere Appliances mit derselben JSON-Datei konfigurieren.

Das Konfigurieren Ihrer Appliance mit einer hochgeladenen JSON-Datei ist häufig effizienter als das manuelle Durchführen der Konfiguration, insbesondere, wenn Sie viele Nodes konfigurieren müssen. Für

die manuelle Durchführung der Konfiguration müssen mehrere Seiten im Installationsprogramm der StorageGRID-Appliance verwendet und die Konfigurationsdatei nacheinander für jeden Knoten angewendet werden.

- Wenn Sie ein fortgeschrittener Benutzer sind, können Sie die folgenden StorageGRID Python-Skripte verwenden, um Ihr System zu installieren und zu konfigurieren:
 - `configure-sga.py`: Automatisieren Sie die Installation und Konfiguration Ihrer Geräte. Siehe [Automatisierung der Appliance-Installation und -Konfiguration mit dem Skript `configure-sga.py`](#).
 - `configure-storagegrid.py`: Konfigurieren Sie andere Komponenten des gesamten StorageGRID-Systems (das "Grid"). Siehe ["Automatisieren Sie die StorageGRID-Konfiguration"](#).



StorageGRID-Automatisierungs-Python-Skripte können direkt verwendet werden oder als Beispiele für die Verwendung der StorageGRID Installations-REST-API in Grid-Implementierungs- und Konfigurations-Tools, die Sie selbst entwickeln. Siehe Anweisungen für ["Herunterladen und Extrahieren der StorageGRID-Installationsdateien"](#).

Automatisieren Sie die Appliance-Konfiguration mit dem StorageGRID Appliance Installer

Nachdem Sie eine JSON-Datei generiert haben, können Sie die Konfiguration einer oder mehrerer Appliances automatisieren, indem Sie die JSON-Datei mit dem Installationsprogramm von StorageGRID Appliance hochladen.

Bevor Sie beginnen

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Das ist schon [Die JSON-Datei wurde generiert](#) Mithilfe Ihres NetApp Professional Services Beraters.
- Ihr Gerät enthält die neueste Firmware, die mit StorageGRID 11.5 oder höher kompatibel ist.
- Sie sind auf der Appliance, die Sie mit konfigurieren, mit dem Installationsprogramm für die StorageGRID-Appliance verbunden ["Unterstützter Webbrowser"](#).

Schritte

1. Wählen Sie im Installationsprogramm des StorageGRID-Geräts **Erweitert > Gerätekonfiguration aktualisieren** aus. Die Seite Gerätekonfiguration aktualisieren wird angezeigt.
2. Suchen Sie die JSON-Datei mit der Konfiguration, die Sie hochladen möchten, und wählen Sie sie aus.

Die Datei wird hochgeladen und validiert. Wenn der Validierungsprozess abgeschlossen ist, wird der Dateiname neben einem grünen Häkchen angezeigt.



Möglicherweise wird die Verbindung zur Appliance unterbrochen, wenn die Konfiguration aus der JSON-Datei Abschnitte für `link_config`, `networks` Oder beides. Wenn Sie innerhalb von 1 Minute keine Verbindung mehr hergestellt haben, geben Sie die Appliance-URL erneut ein, indem Sie eine der anderen IP-Adressen verwenden, die der Appliance zugewiesen wurden.

Upload JSON

JSON configuration	<input type="button" value="Browse"/>	<input checked="" type="checkbox"/> appliances.orig.json
Node name	<input type="text" value="-- Select a node"/>	
<input type="button" value="Apply JSON configuration"/>		

Das Dropdown-Menü **Node Name** enthält die in der JSON-Datei definierten Node-Namen auf oberster Ebene.



Wenn die Datei nicht gültig ist, wird der Dateiname rot angezeigt und eine Fehlermeldung in einem gelben Banner angezeigt. Die ungültige Datei wird nicht auf die Appliance angewendet. ConfigBuilder überprüft, ob Sie über eine gültige JSON-Datei verfügen.

3. Wählen Sie einen Knoten aus der Liste im Dropdown-Menü **Knotenname** aus.

Die Schaltfläche **Apply JSON Configuration** wird aktiviert.

4. Wählen Sie **JSON-Konfiguration anwenden**.

Die Konfiguration wird auf den ausgewählten Knoten angewendet.

Automatisierung der Appliance-Installation und -Konfiguration mit dem Skript `configure-sga.py`

Wenn Sie ein fortgeschrittener Benutzer sind, können Sie das verwenden `configure-sga.py` Skript zur Automatisierung vieler Installations- und Konfigurationsaufgaben für StorageGRID-Appliance-Nodes, einschließlich der Installation und Konfiguration eines primären Admin-Knotens. Dieses Skript kann nützlich sein, wenn Sie über eine große Anzahl von Geräten verfügen, die konfiguriert werden müssen.

Sie können das Skript auch zum Generieren einer JSON-Datei verwenden, die Informationen zur Appliance-Konfiguration enthält. Sie können die JSON-Datei in das Installationsprogramm von StorageGRID Appliance hochladen, um alle Appliance-Nodes gleichzeitig zu konfigurieren. Sie können die JSON-Datei auch bearbeiten und dann hochladen, um eine neue Konfiguration auf eine oder mehrere Appliances anzuwenden.



Dieses Verfahren richtet sich an fortgeschrittene Benutzer mit Erfahrung in der Verwendung von Befehlszeilenschnittstellen. Alternativ können Sie auch [Verwenden Sie das Installationsprogramm für StorageGRID-Appliances, um die Konfiguration zu automatisieren](#).

Bevor Sie beginnen

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Das ist schon [Die JSON-Datei wurde generiert](#) Mithilfe Ihres NetApp Professional Services Beraters.
- Ihr Gerät enthält die neueste Firmware, die mit StorageGRID 11.5 oder höher kompatibel ist.
- Sie haben die IP-Adresse des Admin-Netzwerks für die Appliance konfiguriert.
- Sie haben die heruntergeladen `configure-sga.py` Datei: Die Datei ist im Installationsarchiv enthalten, oder Sie können darauf zugreifen, indem Sie im StorageGRID-Appliance-Installationsprogramm auf **Hilfe** >

Installationsskript für Geräte klicken.

Schritte

1. Melden Sie sich an der Linux-Maschine an, die Sie verwenden, um das Python-Skript auszuführen.
2. Für allgemeine Hilfe bei der Skript-Syntax und um eine Liste der verfügbaren Parameter anzuzeigen, geben Sie Folgendes ein:

```
configure-sga.py --help
```

Der `configure-sga.py` Skript verwendet fünf Unterbefehle:

- `advanced` Für erweiterte Interaktionen von StorageGRID Appliances, einschließlich BMC-Konfiguration und Erstellen einer JSON-Datei, die die aktuelle Konfiguration der Appliance enthält
- `configure` Zum Konfigurieren des RAID-Modus, des Node-Namens und der Netzwerkparameter
- `install` Zum Starten einer StorageGRID Installation
- `monitor` Zur Überwachung einer StorageGRID Installation
- `reboot` Um das Gerät neu zu starten

Wenn Sie ein Unterbefehlsargument (erweitert, konfigurieren, installieren, überwachen oder neu booten), gefolgt vom eingeben `--help` Option Sie erhalten einen anderen Hilfetext mit mehr Details zu den Optionen, die in diesem Unterbefehl verfügbar sind:

```
configure-sga.py subcommand --help
```

Wenn möglich [Sichern Sie die Appliance-Konfiguration in einer JSON-Datei](#), Stellen Sie sicher, dass die Knotennamen folgende Anforderungen erfüllen:

- Jeder Node-Name ist eindeutig, wenn Sie alle Appliance-Nodes automatisch über eine JSON-Datei konfigurieren möchten.
 - Muss ein gültiger Hostname sein, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
 - Kann Buchstaben, Zahlen und Bindestriche verwenden.
 - Kann nicht mit einem Bindestrich beginnen oder enden.
 - Darf nicht nur Zahlen enthalten.
3. Um die Konfiguration aus der JSON-Datei auf die Appliance anzuwenden, geben Sie Folgendes ein, wobei `SGA-INSTALL-IP` Ist die Admin-Netzwerk-IP-Adresse für die Appliance, `json-file-name` Ist der Name der JSON-Datei, und `node-name-inside-json-file` Ist der Name des Knotens mit der anzuwendenden Konfiguration:

```
configure-sga.py advanced --restore-file json-file-name --restore-node node-name-inside-json-file SGA-INSTALL-IP
```
 4. Um die aktuelle Konfiguration des Appliance-Knotens zu bestätigen, geben Sie hier Folgendes ein `SGA-INSTALL-IP` Ist die Admin-Netzwerk-IP-Adresse für die Appliance:

```
configure-sga.py configure SGA-INSTALL-IP
```

Die Ergebnisse zeigen aktuelle IP-Informationen für die Appliance an, einschließlich der IP-Adresse des primären Admin-Knotens und Informationen über Admin-, Grid- und Client-Netzwerke.

```

Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

```

StorageGRID Appliance

```

Name:          LAB-SGA-2-30
Node type:     storage

```

StorageGRID primary Admin Node

```

IP:           172.16.1.170
State:        unknown
Message:      Initializing...
Version:      Unknown

```

Network Link Configuration

Link Status

Link	State	Speed (Gbps)
----	-----	-----
1	Up	10
2	Up	10
3	Up	10
4	Up	10
5	Up	1
6	Down	N/A

Link Settings

```

Port bond mode:    FIXED
Link speed:        10GBE

Grid Network:      ENABLED
  Bonding mode:    active-backup
  VLAN:            novlan
  MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

Admin Network:     ENABLED
  Bonding mode:    no-bond
  MAC Addresses:   00:80:e5:29:70:f4

```

```
Client Network:      ENABLED
    Bonding mode:    active-backup
    VLAN:            novlan
    MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:  172.17.0.0/21
             172.18.0.0/21
             192.168.0.0/21
  MTU:       1500

Admin Network
  CIDR:      10.224.2.30/21 (Static)
  MAC:       00:80:E5:29:70:F4
  Gateway:   10.224.0.1
  Subnets:  10.0.0.0/8
             172.19.0.0/16
             172.21.0.0/16
  MTU:       1500

Client Network
  CIDR:      47.47.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:89
  Gateway:   47.47.0.1
  MTU:       2000

#####
##### If you are satisfied with this configuration, #####
##### execute the script with the "install" sub-command. #####
#####
```

5. Wenn Sie einen der Werte in der aktuellen Konfiguration ändern müssen, verwenden Sie den `configure` Unterbefehl, um sie zu aktualisieren. Wenn Sie beispielsweise die IP-Adresse ändern möchten, die die Appliance für die Verbindung zum primären Admin-Node verwendet `172.16.2.99` Geben Sie Folgendes ein:

```
configure-sga.py configure --admin-ip 172.16.2.99 _SGA-INSTALL-IP_
```

6. Wenn Sie die Appliance-Konfiguration in einer JSON-Datei sichern möchten, verwenden Sie die erweiterten und `backup-file` Unterbefehle. Wenn Sie beispielsweise die Konfiguration einer Appliance mit IP-Adresse sichern möchten `SGA-INSTALL-IP` Zu einer Datei mit dem Namen `appliance-SG1000.json`, Geben Sie Folgendes ein:

```
configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP
```

Die JSON-Datei, die die Konfigurationsinformationen enthält, wird in das gleiche Verzeichnis geschrieben, aus dem Sie das Skript ausgeführt haben.



Überprüfen Sie, ob der Node-Name der generierten JSON-Datei der Name der Appliance entspricht. Nehmen Sie keine Änderungen an dieser Datei vor, es sei denn, Sie sind ein erfahrener Benutzer und haben ein gründliches Verständnis von StorageGRID APIs.

7. Wenn Sie mit der Gerätekonfiguration zufrieden sind, verwenden Sie das `install` Und `monitor` Unterbefehle zum Installieren des Geräts:

```
configure-sga.py install --monitor SGA-INSTALL-IP
```

8. Wenn Sie das Gerät neu starten möchten, geben Sie Folgendes ein:

```
configure-sga.py reboot SGA-INSTALL-IP
```

Automatisieren Sie die StorageGRID-Konfiguration

Nachdem Sie die Grid-Nodes installiert und konfiguriert haben, können Sie die Konfiguration des StorageGRID Systems automatisieren.

Bevor Sie beginnen

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

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

- Sie haben ein erstellt `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`).

Über diese Aufgabe

Sie können das verwenden `configure-storagegrid.py` Python-Skript und das `configure-storagegrid.json` Konfigurationsdatei zur automatischen Konfiguration des StorageGRID Systems



Sie können das System auch mit dem konfigurieren "[Grid Manager](#)" Oder im "[Installations-API](#)".

Schritte

1. Melden Sie sich an der Linux-Maschine an, die Sie verwenden, um das Python-Skript auszuführen.
2. Wechseln Sie in das Verzeichnis, in dem Sie das Installationsarchiv extrahiert haben.

Zum 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
```

Nachdem Sie fertig sind

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 Recovery-Paket-Datei sichern, damit Sie das StorageGRID-System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Zum Beispiel kopieren Sie den Text auf einen sicheren, gesicherten Netzwerkstandort und an einen sicheren Cloud-Storage-Standort.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

Wenn Sie angegeben haben, dass zufällige Passwörter generiert werden sollen, müssen Sie die extrahieren `Passwords.txt` Datei und suchen Sie nach den Kennwörtern, 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.           #####  
#####
```

Das StorageGRID System wird installiert und konfiguriert, wenn eine Bestätigungsmeldung angezeigt wird.

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

Überblick über die Installations-REST-APIs

StorageGRID bietet zwei REST-APIs zur Durchführung von Installationsaufgaben: Die StorageGRID Installations-API und die StorageGRID Appliance Installer-API.

Beide APIs verwenden die Swagger Open Source API-Plattform, um die API-Dokumentation bereitzustellen. Swagger ermöglicht Entwicklern und nicht-Entwicklern die Interaktion mit der API in einer Benutzeroberfläche, die zeigt, 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 mit der API Docs Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Jeder REST-API-Befehl umfasst die URL der API, eine HTTP-Aktion, alle erforderlichen oder optionalen URL-Parameter sowie eine erwartete API-Antwort.

StorageGRID Installations-API

Die StorageGRID Installations-API ist nur verfügbar, wenn Sie das StorageGRID-System zu Beginn konfigurieren und eine primäre Wiederherstellung des Admin-Knotens durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um auf die API-Dokumentation zuzugreifen, gehen Sie auf die Installations-Webseite des primären Admin-Knotens und wählen Sie in der Menüleiste **Hilfe > API-Dokumentation** aus.

Die StorageGRID Installations-API umfasst die folgenden Abschnitte:

- **Config:** Operationen im Zusammenhang mit der Produktfreigabe und den Versionen der API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Grid:** Konfigurationsvorgänge auf Grid-Ebene. Grid-Einstellungen erhalten und aktualisiert werden, einschließlich Grid-Details, Grid-Netzwerknetzen, Grid-Passwörter und NTP- und DNS-Server-IP-Adressen.
- **Nodes:** Konfigurationsvorgänge auf Node-Ebene. Sie können eine Liste der Grid-Nodes abrufen, einen Grid-Node löschen, einen Grid-Node konfigurieren, einen Grid-Node anzeigen und die Konfiguration eines Grid-Node zurücksetzen.
- **Provision:** Bereitstellungsvorgänge. Sie können den Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung:** Wiederherstellungsvorgänge für primären Admin-Knoten. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket:** Operationen zum Herunterladen des Wiederherstellungspakets.
- **Standorte:** Konfigurationsvorgänge auf Standort-Ebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.

StorageGRID Appliance Installer-API

Der Zugriff auf die Installer-API von StorageGRID Appliance ist über HTTPS möglich `Controller_IP:8443`.

Um auf die API-Dokumentation zuzugreifen, gehen Sie zum StorageGRID Appliance Installer auf dem Gerät und wählen Sie in der Menüleiste **Hilfe > API Docs** aus.

Die StorageGRID Appliance Installer-API umfasst die folgenden Abschnitte:

- **Clone:** Operationen zum Konfigurieren und Steuern des Node-Klonens.
- **Verschlüsselung:** Operationen zur Verwaltung der Verschlüsselung und Anzeige des Verschlüsselungsstatus.
- **Hardware config:** Operationen zur Konfiguration von Systemeinstellungen auf angeschlossener Hardware.
- **Installation:** Vorgänge zum Starten der Appliance-Installation und zur Überwachung des

Installationsstatus.

- **Netzwerk:** Vorgänge im Zusammenhang mit der Grid-, Admin- und Client-Netzwerkconfiguration für eine StorageGRID-Appliance und Appliance-Port-Einstellungen.
- **Setup:** Operationen zur Unterstützung bei der Erstinstallation der Appliance einschließlich Anfragen, Informationen über das System zu erhalten und die primäre Admin-Knoten-IP zu aktualisieren.
- **Support:** Operationen für den Neustart des Controllers und das Abrufen von Protokollen.
- **Update-config:** Vorgänge zum Aktualisieren der StorageGRID-Appliance-Konfiguration.
- **Upgrade:** Vorgänge im Zusammenhang mit der Aktualisierung der Appliance-Firmware.
- **Uploadsg:** Operationen zum Hochladen von StorageGRID-Installationsdateien.

Hardware installieren

Hardware registrieren

Die Registrierung der Appliance-Hardware bietet Support-Vorteile.

Schritte

1. Suchen Sie die Seriennummer des Gehäuses für das Gerät. Bei SG6000 Appliances befindet sich die Seriennummer des Chassis auf dem Storage Controller-Shelf.

Sie finden die Nummer auf dem Packzettel, in Ihrer Bestätigungs-E-Mail oder auf dem Gerät nach dem Auspacken.



Die SG6000 Storage Appliance enthält mehrere Seriennummern. Die Seriennummer auf dem Storage-Controller-Shelf muss registriert und verwendet werden, wenn Sie Service oder Support für die SG6000 Appliance anrufen.

2. Wechseln Sie zur NetApp Support Site unter "mysupport.netapp.com".
3. Bestimmen Sie, ob Sie die Hardware registrieren müssen:

Wenn Sie ein...	Führen Sie die folgenden Schritte aus...
Bestehender NetApp Kunde	<ol style="list-style-type: none">a. Melden Sie sich mit Ihrem Benutzernamen und Passwort an.b. Wählen Sie Produkte > Meine Produkte.c. Bestätigen Sie, dass die neue Seriennummer aufgeführt ist.d. Falls nicht, folgen Sie den Anweisungen für neue NetApp Kunden.

Wenn Sie ein...	Führen Sie die folgenden Schritte aus...
Neuer NetApp Kunde	<p>a. Klicken Sie auf Jetzt registrieren und erstellen Sie ein Konto.</p> <p>b. Wählen Sie Produkte > Produkte Registrieren.</p> <p>c. Geben Sie die Seriennummer des Produkts und die angeforderten Details ein.</p> <p>Nach der Registrierung können Sie die erforderliche Software herunterladen. Der Genehmigungsprozess kann bis zu 24 Stunden in Anspruch nehmen.</p>

In Schrank oder Rack installieren

In Schrank oder Rack einbauen (SGF6112)

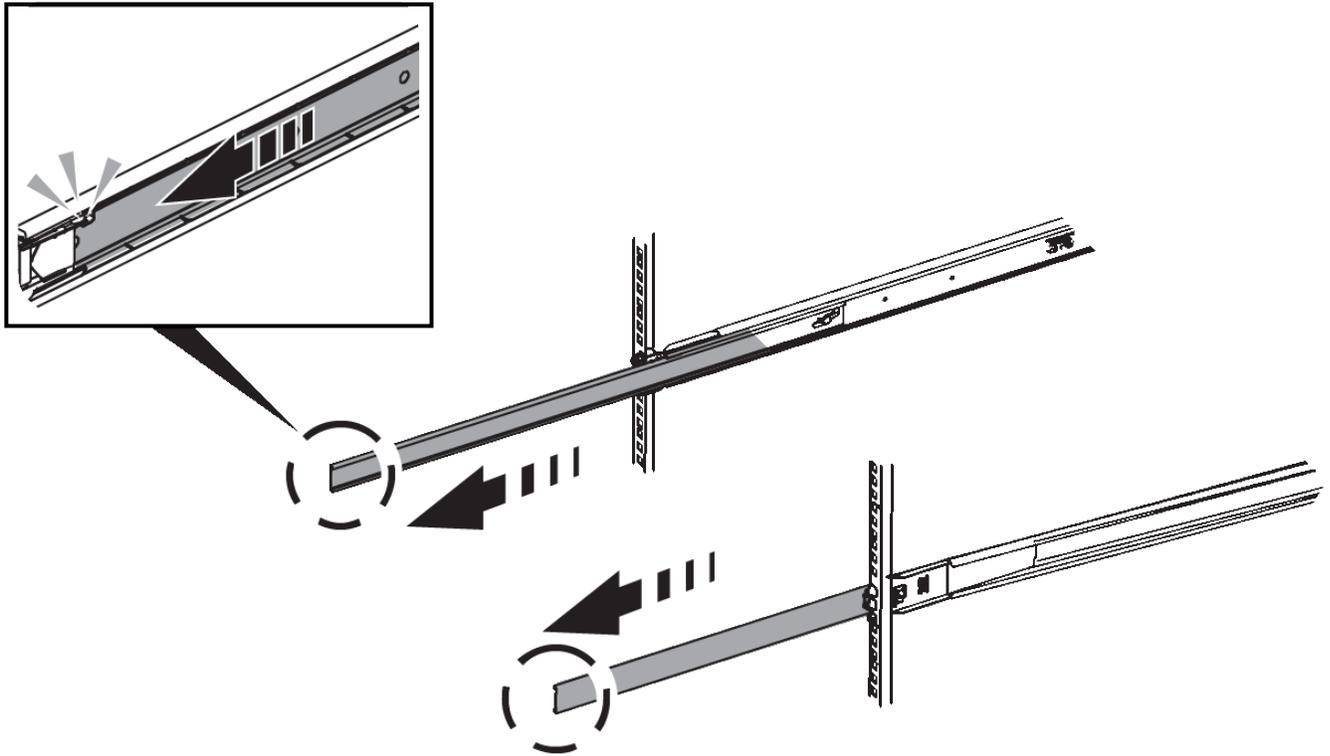
Sie installieren eine Reihe von Schienen für das Gerät in Ihrem Schrank oder Rack und schieben das Gerät dann auf die Schienen.

Bevor Sie beginnen

- Sie haben das im Lieferumfang enthaltene Sicherheitshinweisen geprüft und die Vorsichtsmaßnahmen für das Bewegen und Installieren von Hardware verstanden.
- Sie haben die Anweisungen im Lieferumfang des Schienensatzes erhalten.

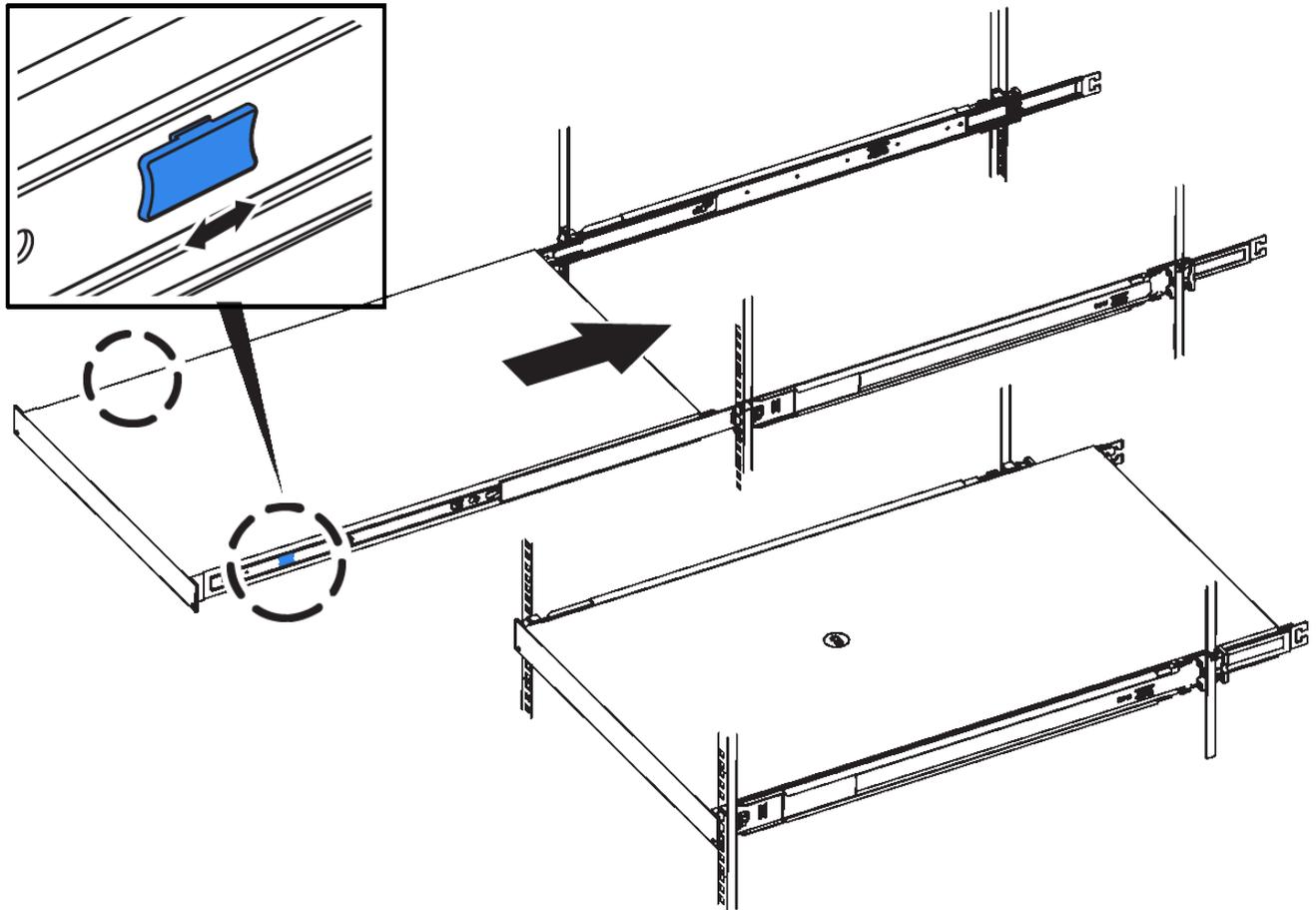
Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.
2. Verlängern Sie auf den beiden Schienen, die im Schrank oder Rack installiert sind, die beweglichen Teile der Schienen, bis Sie ein Klicken hören.



3. Setzen Sie das Gerät in die Schienen ein.
4. Schieben Sie das Gerät in das Gehäuse oder Rack.

Wenn Sie das Gerät nicht weiter bewegen können, ziehen Sie an den blauen Verriegelungen auf beiden Seiten des Gehäuses, um das Gerät vollständig einzuschieben.



5. Ziehen Sie die unverlierbaren Schrauben an der Gerätevorderseite fest, um das Gerät im Rack zu befestigen.



Befestigen Sie die Frontverkleidung erst, nachdem Sie das Gerät eingeschaltet haben.

SG6000

In Schrank oder Rack installieren (SG6000)

Beim SG6060 und SGF6024 installieren Sie Schienen in Ihrem Schrank oder Rack und schieben das Controller-Shelf, alle Erweiterungseinschübe und den Compute-Controller auf die Schienen. Installieren Sie beim SG6060 die Laufwerke erst in jedem Shelf, wenn die Shelves installiert sind.

Modell	Installieren	Zur Information
SG6060	Controller Shelf mit 60 Laufwerken und Erweiterung-Shelves mit 60 Laufwerken	"Installation von Shelves mit 60 Laufwerken"

Modell	Installieren	Zur Information
SG6060	60 Laufwerke in jedes Shelf	" Installieren Sie Laufwerke "
SGF6024	Controller Shelf mit 24 Laufwerken	" Installation von Shelves mit 24 Laufwerken "
SG6060 und SGF6024	SG6000-CN Computing-Controller	" Installieren Sie den SG6000-CN-Controller "

Installation von Shelves mit 60 Laufwerken (SG6060)

Sie installieren einen Satz Schienen für das E2860-Controller-Shelf in Ihrem Schrank oder Rack und schieben das Controller-Shelf dann auf die Schienen. Bei Installation der Erweiterungs-Shelves für 60 Laufwerke gilt dasselbe Verfahren.

Bevor Sie beginnen

- Sie haben das im Lieferumfang enthaltene Sicherheitshinweisen geprüft und die Vorsichtsmaßnahmen für das Bewegen und Installieren von Hardware verstanden.
- Sie haben die Anweisungen im Lieferumfang des Schienensatz erhalten.



Jedes Shelf mit 60 Laufwerken wiegt ohne installierte Laufwerke etwa 60 kg (132 lb). Vier Personen oder ein mechanisierter Lift sind erforderlich, um das Regal sicher zu bewegen.



Um eine Beschädigung der Hardware zu vermeiden, verschieben Sie niemals das Shelf, wenn Laufwerke installiert sind. Vor dem Verschieben des Shelves müssen alle Laufwerke entfernt werden.



Installieren Sie bei der Installation des E2860 Controller-Shelves oder optionaler Erweiterungs-Shelves die Hardware von unten nach oben im Rack oder Schrank, um zu vermeiden, dass das System umkippt. Installieren Sie den SG6000-CN Controller über dem E2860 Controller-Shelf und Erweiterungs-Shelves, um sicherzustellen, dass sich die schwersten Geräte unten im Rack oder Rack befinden.



Stellen Sie vor der Installation sicher, dass die im Lieferumfang des Geräts enthaltenen 0,5-m-Glasfaserkabel oder -Kabel lang genug für das geplante Layout sind.

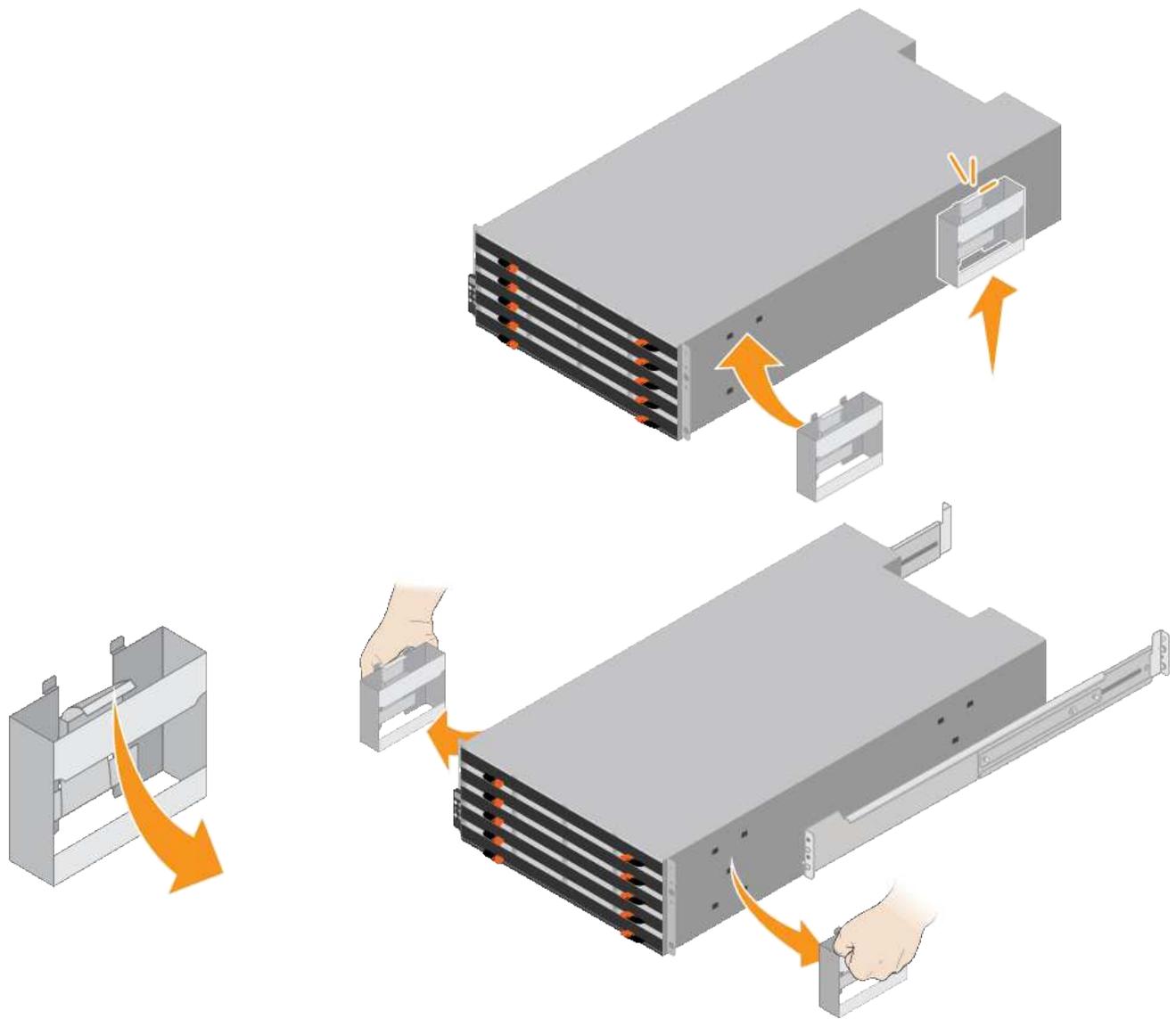
Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.

Bei Vierkantlochrack zuerst die mitgelieferten Käfigmuttern einbauen, um die Vorder- und Rückseite des Regals mit Schrauben zu sichern.

2. Entfernen Sie den äußeren Verpackungskasten für das Gerät. Falten Sie dann die Klappen auf dem inneren Kasten nach unten.
3. Wenn Sie das Gerät mit der Hand anheben, befestigen Sie die vier Griffe an den Seiten des Gehäuses.

Drücken Sie auf jeden Griff nach oben, bis er einrastet.



4. Setzen Sie die Rückseite des Regals (das Ende mit den Anschlüssen) auf die Schienen.
5. Das Regal von unten halten und in den Schrank schieben. Wenn Sie die Griffe verwenden, lösen Sie mit den Daumenverriegelungen jeweils einen Griff, während Sie das Regal einschieben.

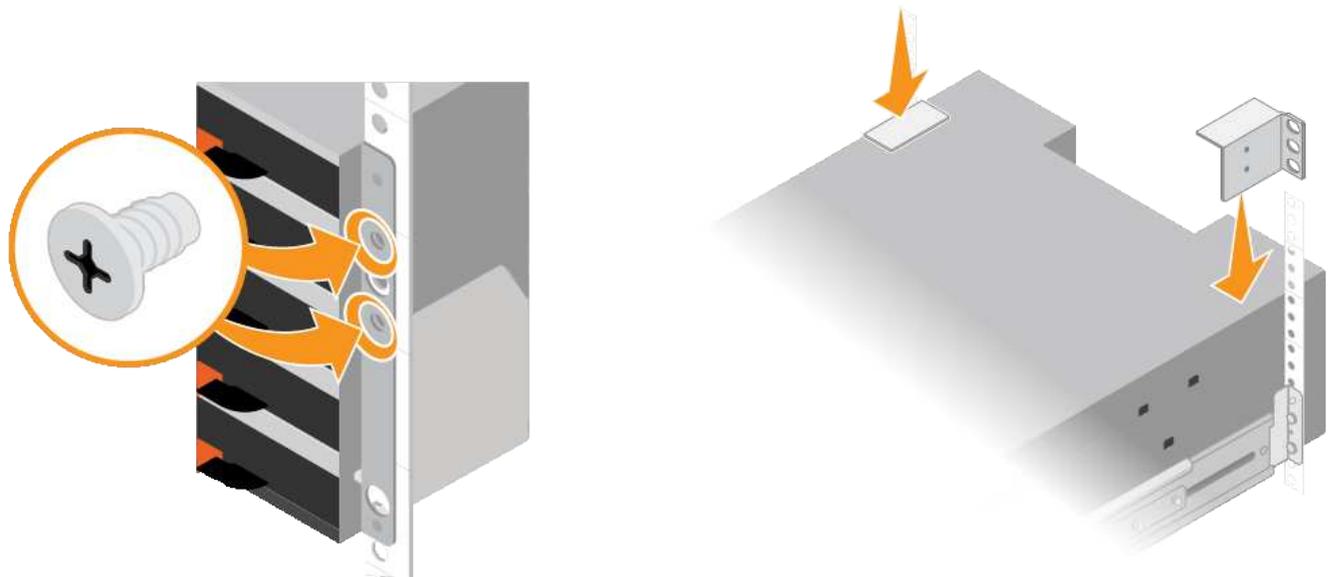
Um die Griffe zu entfernen, ziehen Sie den Entriegelungshebel nach unten und ziehen Sie dann aus dem Shelf heraus.

6. Befestigen Sie das Regal an der Vorderseite des Schrank.

Bringen Sie die Schrauben an beiden Seiten in die ersten und dritten Löcher von der Oberseite des Regals ein.

7. Befestigen Sie das Regal an der Rückseite des Gehäuses.

Legen Sie zwei hintere Halterungen an jeder Seite des oberen hinteren Bereichs des Regals an. Bringen Sie die Schrauben in die ersten und dritten Löcher jeder Halterung ein.



8. Wiederholen Sie diese Schritte für alle Erweiterungs-Shelfs.

Laufwerke installieren (SG6060)

Installieren Sie nach der Installation des Shelf für 60 Laufwerke in einem Schrank oder Rack alle 60 Laufwerke in das Shelf. Der Versand für das E2860 Controller-Shelf umfasst zwei SSD-Laufwerke, die Sie im oberen Einschub des Controller Shelf installieren sollten. Jedes optionale Erweiterungs-Shelf umfasst 60 HDD-Laufwerke und keine SSD-Laufwerke.

Bevor Sie beginnen

Sie haben das E2860 Controller-Shelf oder optionale Erweiterungs-Shelfs (ein oder zwei) im Rack oder Rack installiert.



Um eine Beschädigung der Hardware zu vermeiden, verschieben Sie niemals das Shelf, wenn Laufwerke installiert sind. Vor dem Verschieben des Shelves müssen alle Laufwerke entfernt werden.

Schritte

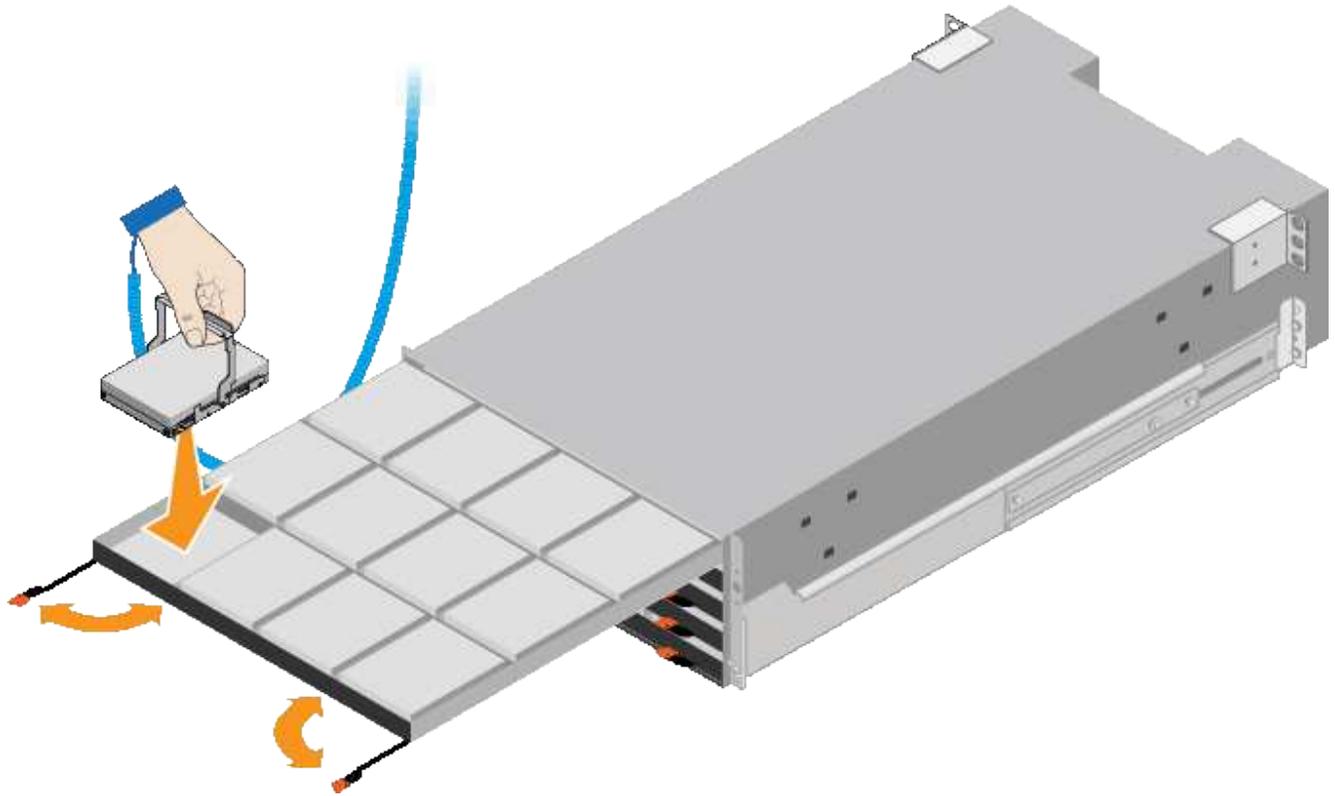
1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Nehmen Sie die Laufwerke aus der Verpackung.
3. Lösen Sie die Hebel an der oberen Antriebsschublade, und schieben Sie die Schublade mit den Hebeln heraus.
4. Suchen Sie die beiden SSD-Laufwerke.



Erweiterungs-Shelfs verwenden keine SSD-Laufwerke.

5. Heben Sie jeden Antriebsgriff in eine vertikale Position.
6. Installieren Sie die beiden SSD-Laufwerke in den Steckplätzen 0 und 1 (die ersten beiden Steckplätze entlang der linken Seite der Schublade).

7. Positionieren Sie jedes Laufwerk vorsichtig in seinen Steckplatz, und senken Sie den angehobenen Laufwerkgriff ab, bis er einrastet.



8. Setzen Sie 10 Festplattenlaufwerke in das obere Fach ein.
9. Schieben Sie die Schublade wieder nach innen, indem Sie die Mitte drücken und beide Hebel vorsichtig schließen.



Drücken Sie die Schublade nicht mehr, wenn Sie sich binden. Schieben Sie die Schublade mit den Freigabehebel an der Vorderseite der Schublade nach außen. Setzen Sie dann die Schublade vorsichtig wieder in den Schlitz ein.

10. Wiederholen Sie diese Schritte, um Festplattenlaufwerke in die anderen vier Schubladen zu installieren.



Sie müssen alle 60 Laufwerke installieren, um den korrekten Betrieb zu gewährleisten.

11. Befestigen Sie die Frontverkleidung am Shelf.
12. Wenn Sie Erweiterungs-Shelfs haben, wiederholen Sie diese Schritte, um 12 Festplattenlaufwerke in jede Schublade jedes Erweiterungs-Shelfs zu installieren.
13. Befolgen Sie die Anweisungen zur Installation des SG6000-CN in einem Schrank oder Rack.

Shelfs mit 24 Laufwerken installieren (SGF6024)

Sie installieren einen Satz Schienen für das EF570 Controller-Shelf in Ihrem Schrank oder Rack und schieben das Array dann auf die Schienen.

Bevor Sie beginnen

- Sie haben das im Lieferumfang enthaltene Sicherheitshinweisen geprüft und die Vorsichtsmaßnahmen für

das Bewegen und Installieren von Hardware verstanden.

- Sie haben die Anweisungen im Lieferumfang des Schienensatz enthalten.

Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.

Bei Vierkantlochschränken zuerst die mitgelieferten Käfigmuttern einbauen, um die Vorder- und Rückseite des Regals mit Schrauben zu sichern.

2. Entfernen Sie den äußeren Verpackungskasten für das Gerät. Falten Sie dann die Klappen auf dem inneren Kasten nach unten.
3. Setzen Sie die Rückseite des Regals (das Ende mit den Anschlüssen) auf die Schienen.



Ein voll beladenes Regal wiegt etwa 24 kg (52 lb). Zum sicheren Bewegen des Gehäuses sind zwei Personen erforderlich.

4. Schieben Sie das Gehäuse vorsichtig ganz auf die Schienen.



Möglicherweise müssen Sie die Schienen anpassen, um sicherzustellen, dass das Gehäuse den ganzen Weg auf die Schienen führt.

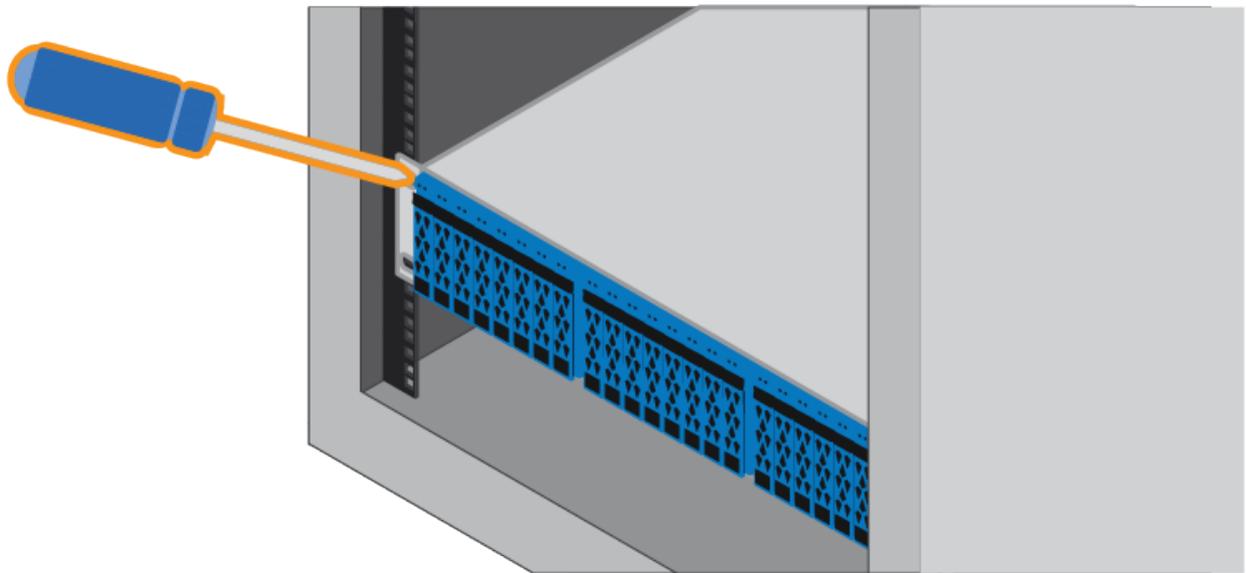


Stellen Sie keine zusätzlichen Geräte auf die Schienen, nachdem Sie die Installation des Gehäuses abgeschlossen haben. Die Schienen sind nicht für zusätzliches Gewicht ausgelegt.

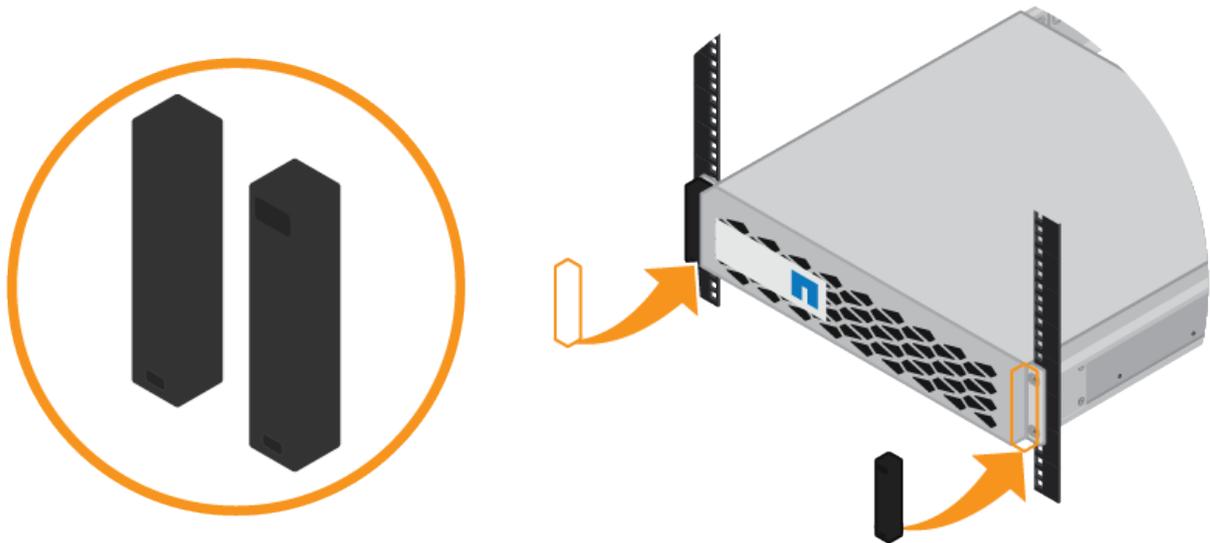


Falls zutreffend, müssen Sie die Shelf-Endkappen oder die Systemverkleidung entfernen, um das Gehäuse am Rack-Beitrag zu befestigen. In diesem Fall müssen Sie die Endkappen oder die Blende austauschen, wenn Sie fertig sind.

5. Befestigen Sie das Gehäuse an der Vorderseite des Schranks oder Racks und Schienen, indem Sie zwei M5-Schrauben durch die Befestigungshalterungen (vorinstalliert auf beiden Seiten des Gehäuses), die Löcher am Rack oder am Systemschrank und die Löcher auf der Vorderseite der Schienen einsetzen.



6. Befestigen Sie das Gehäuse an der Rückseite der Schienen, indem Sie zwei M5-Schrauben durch die Halterungen am Gehäuse und an der Halterung des Schienensatz einsetzen.
7. Ersetzen Sie gegebenenfalls die Shelf-Abschlusskappen oder die Systemblende.



Installieren des SG6000-CN Controllers (SG6060 und SG6024)

Sie installieren einen Satz Schienen für den SG6000-CN Controller in Ihrem Schrank oder Rack und schieben den Controller dann auf die Schienen.

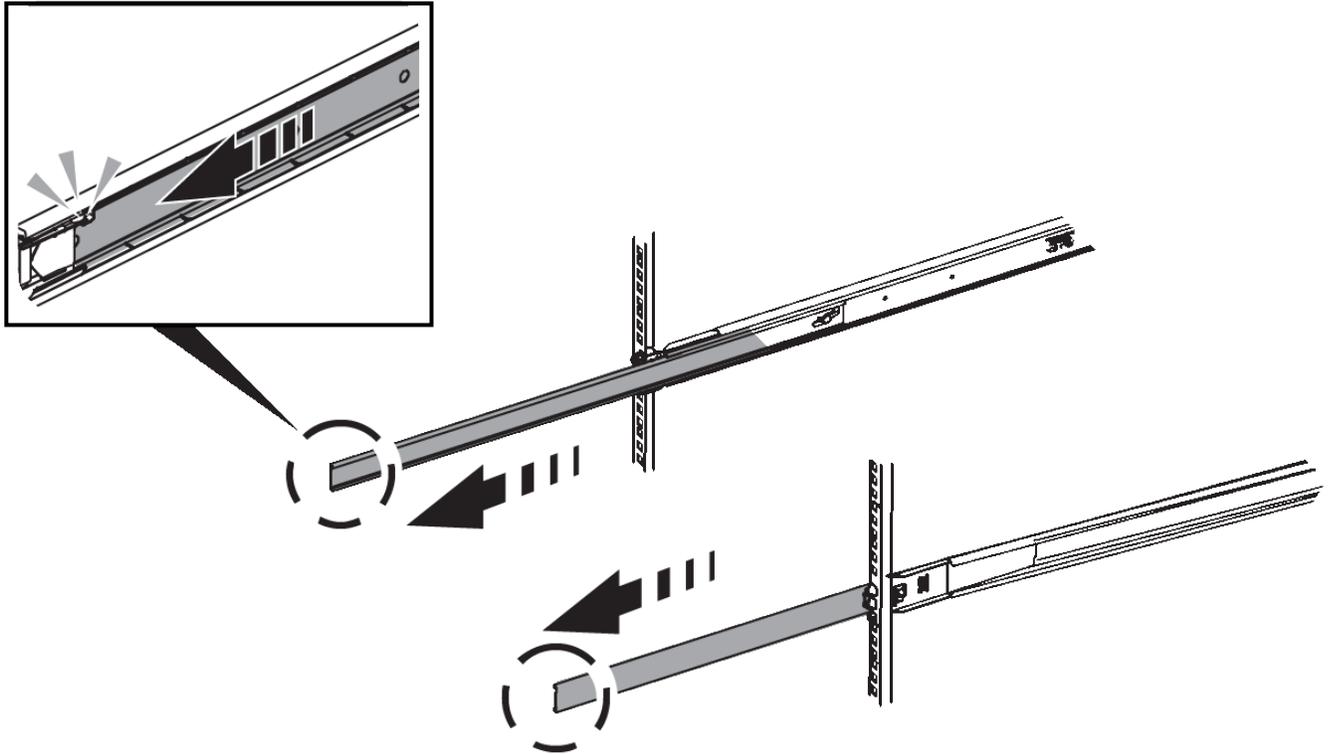
Bevor Sie beginnen

- Sie haben das im Lieferumfang enthaltene Sicherheitshinweisen geprüft und die Vorsichtsmaßnahmen für das Bewegen und Installieren von Hardware verstanden.

- Sie haben die Anweisungen im Lieferumfang des Schienensatz enthalten.
- Sie haben das E2860 Controller-Shelf und -Laufwerke oder das EF570 Controller-Shelf installiert.

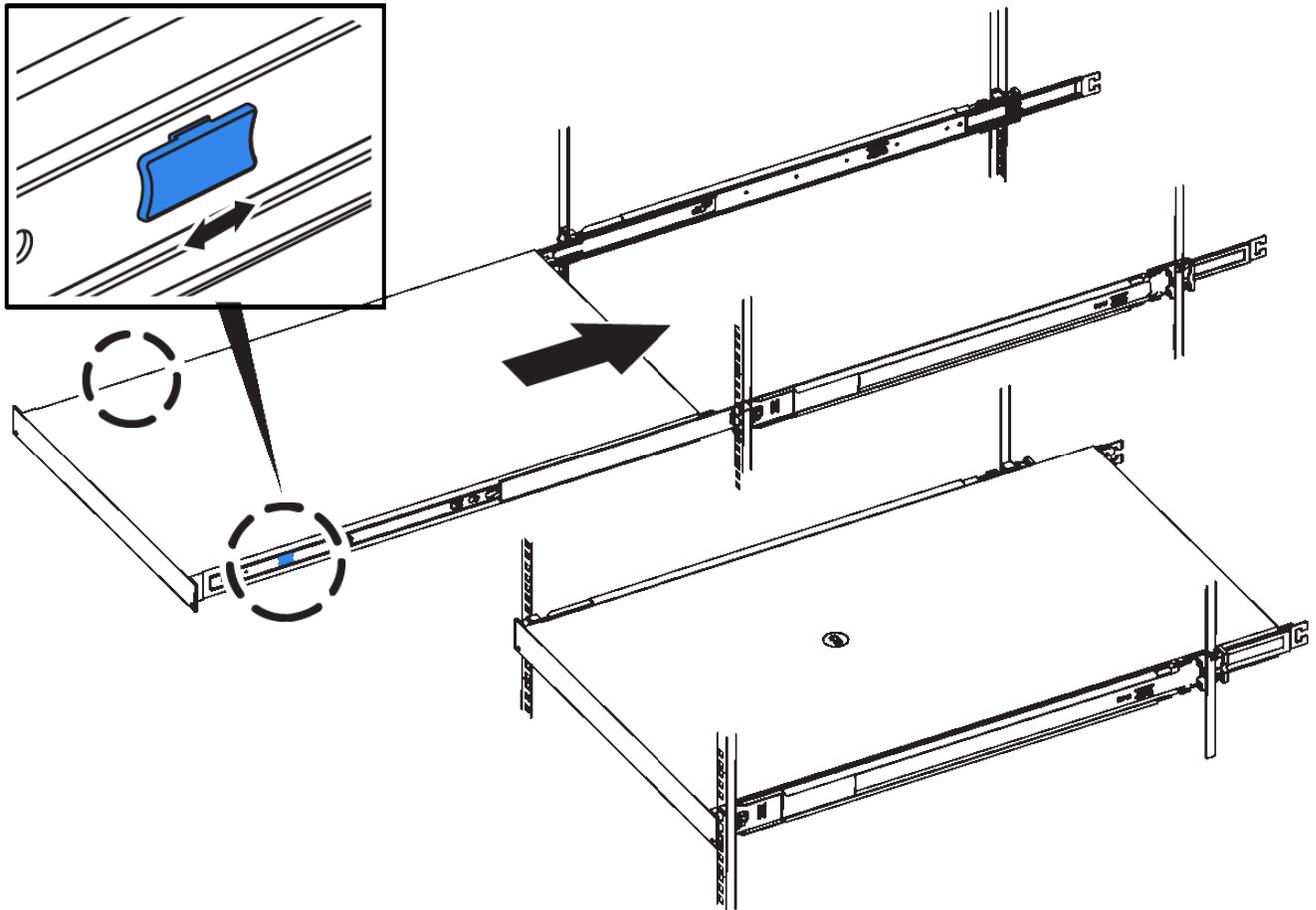
Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.
2. Verlängern Sie auf den beiden Schienen, die im Schrank oder Rack installiert sind, die beweglichen Teile der Schienen, bis Sie ein Klicken hören.



3. Setzen Sie den SG6000-CN-Controller in die Schienen ein.
4. Schieben Sie den Controller in den Schrank oder Rack.

Wenn Sie den Controller nicht weiter bewegen können, ziehen Sie die blauen Laschen auf beiden Seiten des Chassis, um den Controller vollständig einzuschieben.



Bringen Sie die Frontverkleidung erst an, nachdem Sie den Controller eingeschaltet haben.

5. Ziehen Sie die unverlierbaren Schrauben an der Vorderseite des Controllers fest, um den Controller im Rack zu befestigen.



In Schrank oder Rack installieren (SG5700)

Sie installieren eine Reihe von Schienen in Ihrem Schrank oder Rack und schieben das Gerät dann auf die Schienen. Wenn Sie ein SG5760 besitzen, installieren Sie die Laufwerke nach der Installation des Geräts.

Bevor Sie beginnen

- Sie haben das im Lieferumfang enthaltene Sicherheitshinweisen geprüft und die Vorsichtsmaßnahmen für das Bewegen und Installieren von Hardware verstanden.
- Sie haben die Anweisungen im Lieferumfang des Schienensatz enthalten.

Installieren Sie SG5712

Führen Sie die folgenden Schritte aus, um eine SG5712-Appliance in einem Rack oder Schrank zu installieren.



Die SG5712 wiegt bei voller Beladung mit Laufwerken ca. 64 lb (29 kg). Um den SG5712 sicher zu bewegen, sind zwei Personen oder ein mechanisierter Lift erforderlich.



Installieren Sie die Hardware von der Unterseite des Racks oder Racks bis zu, um ein Umkippen des Geräts zu verhindern.

Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen zu installieren.
2. Setzen Sie die Rückseite des Geräts (das Ende mit den Anschlüssen) auf die Schienen.
3. Schieben Sie das Gerät vorsichtig bis zum Ende in den Schrank oder das Rack.
4. Befestigen Sie das Gerät gemäß den Anweisungen im Schienensatz am Schrank oder Rack.
5. Befestigen Sie die Blende an der Vorderseite.

SG5760 installieren

Führen Sie die folgenden Schritte aus, um eine SG5760-Appliance und alle Erweiterungs-Shelfs in einem Rack oder Schrank zu installieren.



Installieren Sie die Hardware von der Unterseite des Racks oder Racks bis zu, um ein Umkippen des Geräts zu verhindern.



Die SG5760 wiegt ca. 60 kg (132 lb), ohne dass Laufwerke installiert sind. Vier Personen oder ein mechanisierter Lift sind erforderlich, um eine leere SG5760 sicher zu bewegen.



Um eine Beschädigung der Hardware zu vermeiden, verschieben Sie niemals eine SG5760, wenn Laufwerke installiert sind. Vor dem Verschieben des Shelfs müssen alle Laufwerke entfernt werden.

Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.
2. Bereiten Sie das Gerät vor:
 - a. Entfernen Sie den äußeren Verpackungskasten.
 - b. Klappen Sie die Klappen auf dem inneren Kasten nach unten.
 - c. Wenn Sie die SG5760 von Hand anheben, befestigen Sie die vier Griffe an den Seiten des Chassis.

Sie entfernen diese Griffe, während Sie das Gerät auf die Schienen schieben.

3. Wenn Ihr Schrank über ein quadratisches Loch verfügt, bringen Sie die Käfigmuttern an, damit Sie die Vorder- und Rückseite des Regals mit Schrauben sichern können.
4. Setzen Sie die Rückseite des Geräts (das Ende mit den Anschlüssen) auf die Schienen.
5. Halten Sie das Gerät von unten ab, und schieben Sie es in das Rack oder den Schrank.

Verwenden Sie die Daumenverriegelungen, um die Griffe zu lösen, während Sie das Gerät einschieben.

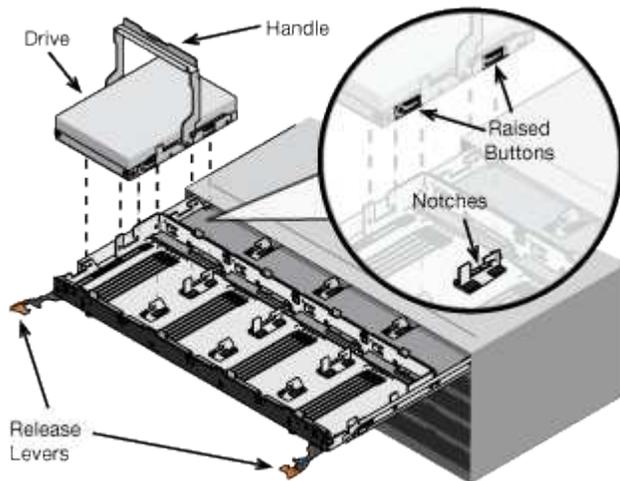
6. Befestigen Sie das Gerät an der Vorderseite des Racks, indem Sie auf jeder Seite zwei Schrauben in die erste und dritte Bohrung (von oben nach unten) einsetzen.

7. Befestigen Sie das Gerät mit den Halterungen an der Rückseite des Racks oder Schrankes.

8. Installieren Sie 12 Laufwerke in jedem der fünf Laufwerkseinschübe.

Sie müssen alle 60 Laufwerke installieren, um den korrekten Betrieb zu gewährleisten.

- a. Setzen Sie das ESD-Armband auf, und entfernen Sie die Antriebe aus der Verpackung.
- b. Lösen Sie die Hebel an der oberen Antriebsschublade, und schieben Sie die Schublade mit den Hebeln heraus.
- c. Heben Sie den Laufwerkgriff senkrecht an, und richten Sie die Tasten am Laufwerk an den Kerben in der Schublade aus.



- d. Drücken Sie vorsichtig auf die Oberseite des Laufwerks, und drehen Sie den Laufwerkgriff nach unten, bis das Laufwerk einrastet.
- e. Schieben Sie nach dem Einbau der ersten 12 Laufwerke die Schublade wieder nach innen, indem Sie die Mitte drücken und beide Hebel vorsichtig schließen.
- f. Wiederholen Sie diese Schritte für die anderen vier Schubläden.

9. Befestigen Sie die Frontverkleidung.

In Schrank oder Rack installieren (SG100 und SG1000)

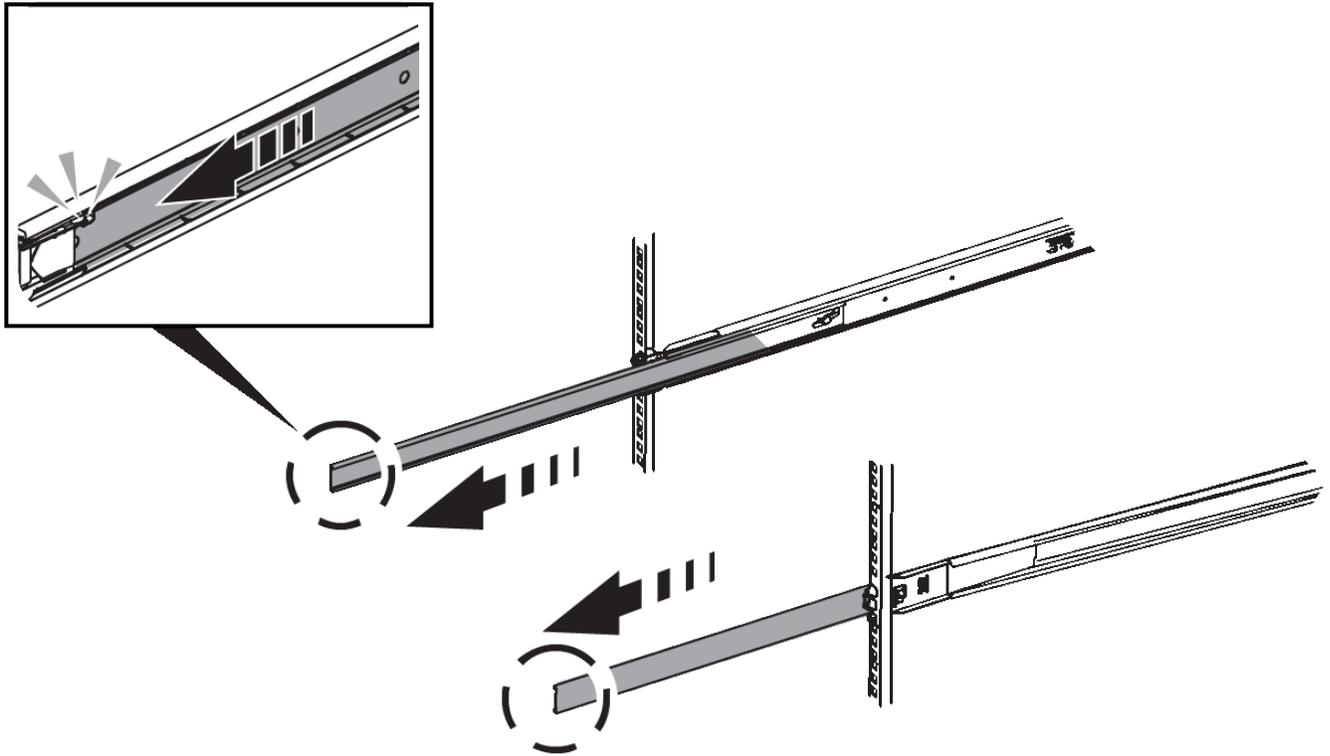
Sie installieren eine Reihe von Schienen für das Gerät in Ihrem Schrank oder Rack und schieben das Gerät dann auf die Schienen.

Bevor Sie beginnen

- Sie haben das im Lieferumfang enthaltene Sicherheitshinweisen geprüft und die Vorsichtsmaßnahmen für das Bewegen und Installieren von Hardware verstanden.
- Sie haben die Anweisungen im Lieferumfang des Schienensatzes erhalten.

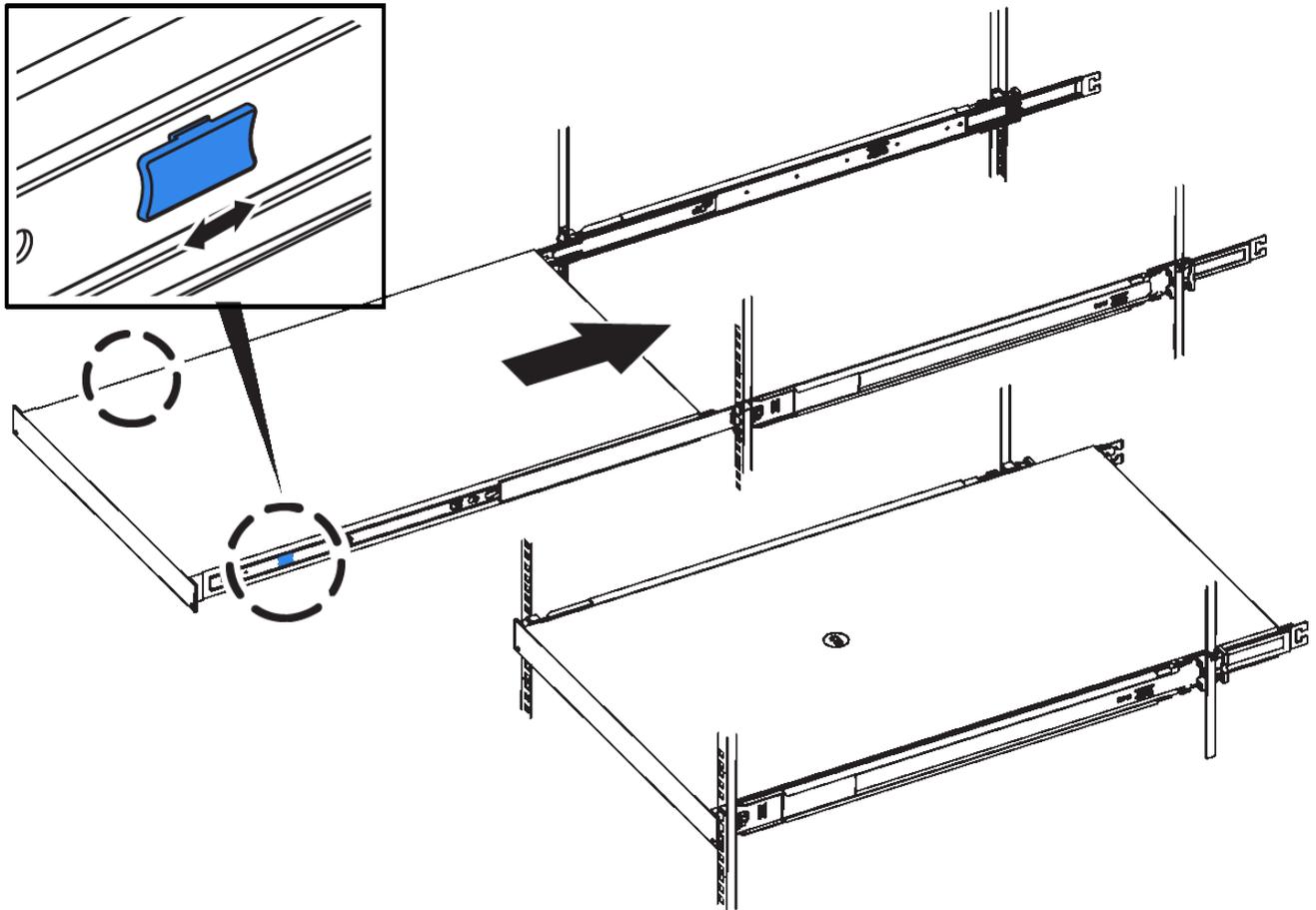
Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.
2. Verlängern Sie auf den beiden Schienen, die im Schrank oder Rack installiert sind, die beweglichen Teile der Schienen, bis Sie ein Klicken hören.



3. Setzen Sie das Gerät in die Schienen ein.
4. Schieben Sie das Gerät in das Gehäuse oder Rack.

Wenn Sie das Gerät nicht weiter bewegen können, ziehen Sie an den blauen Verriegelungen auf beiden Seiten des Gehäuses, um das Gerät vollständig einzuschieben.



Befestigen Sie die Frontverkleidung erst, nachdem Sie das Gerät eingeschaltet haben.

Kabelgerät

Kabelgerät (SGF6112)

Sie verbinden den Management-Port der Appliance mit dem Service-Laptop und verbinden die Netzwerkports der Appliance mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk für StorageGRID.

Bevor Sie beginnen

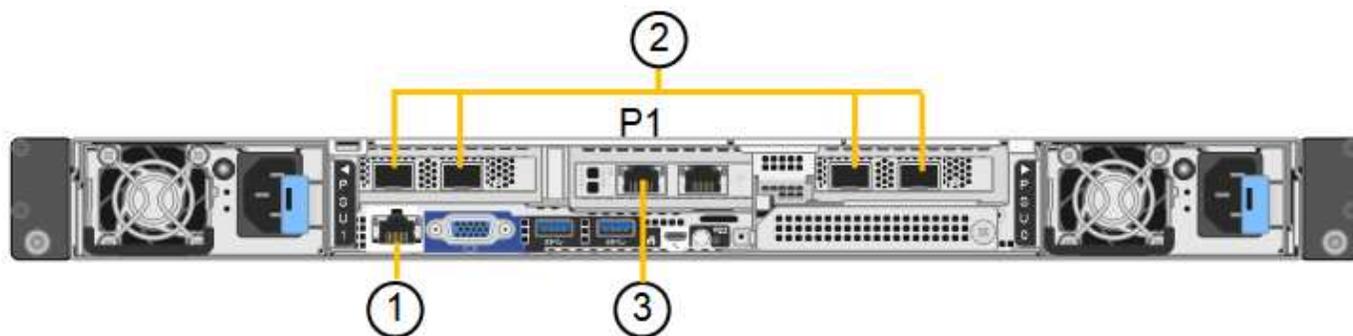
- Sie verfügen über ein RJ-45-Ethernet-Kabel zum Anschließen des Management-Ports.
- Sie haben eine der folgenden Optionen für die Netzwerkanschlüsse. Diese Gegenstände sind nicht im Lieferumfang des Geräts enthalten.
 - Ein bis vier Twinax-Kabel zum Anschließen der vier Netzwerk-Ports.
 - Ein bis vier SFP+ oder SFP28 Transceiver, wenn Sie optische Kabel für die Ports verwenden möchten.



Gefahr der Laserstrahlung — keinen Teil eines SFP-Transceivers zerlegen oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

Über diese Aufgabe

Die folgenden Abbildungen zeigen die Ports auf der Rückseite des SGF6112.



Legende	Port	Typ des Ports	Nutzung
1	BMC-Management-Port auf der Appliance	1 GbE (RJ-45)	Stellt eine Verbindung zum Netzwerk her, in dem Sie auf die BMC-Schnittstelle zugreifen.
2	Vier 10/25-GbE-Netzwerkports auf der Appliance		Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.
3	Admin-Netzwerk-Port auf der Appliance (in der Abbildung mit „P1“ gekennzeichnet)	1 GbE (RJ-45) Wichtig: dieser Port arbeitet nur mit 1/10-GbE (RJ-45) und unterstützt keine 100-Megabit-Geschwindigkeiten.	Verbindet die Appliance mit dem Admin-Netzwerk für StorageGRID.
	Rechtmäßiger RJ-45-Anschluss am Gerät	1 GbE (RJ-45) Wichtig: dieser Port arbeitet nur mit 1/10-GbE (RJ-45) und unterstützt keine 100-Megabit-Geschwindigkeiten.	<ul style="list-style-type: none"> • Kann mit Verwaltungsport 1 verbunden werden, wenn Sie eine redundante Verbindung zum Admin-Netzwerk wünschen. • Kann getrennt bleiben und für einen temporären lokalen Zugang verfügbar sein (IP 169.254.0.1). • Während der Installation kann verwendet werden, um das Gerät an einen Service-Laptop anzuschließen, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

Schritte

1. Schließen Sie den BMC-Managementport der Appliance über ein Ethernet-Kabel an das Managementnetzwerk an.

Obwohl diese Verbindung optional ist, wird empfohlen, den Support zu erleichtern.

2. Verbinden Sie die Netzwerk-Ports des Geräts mit den entsprechenden Netzwerk-Switches über Twinax-Kabel oder optische Kabel und Transceiver.

Alle vier Netzwerkports müssen dieselbe Verbindungsgeschwindigkeit verwenden.



SGF6112-Verbindungsgeschwindigkeit (GbE)	Erforderliche Ausrüstung
10	SFP+-Transceiver
25	SFP28-Transceiver

- Wenn Sie den Modus Fixed Port Bond verwenden möchten (Standard), verbinden Sie die Ports mit dem StorageGRID-Grid und den Client-Netzwerken, wie in der Tabelle dargestellt.

Port	Verbindung wird hergestellt mit...
Port 1	Client-Netzwerk (optional)
Port 2	Grid-Netzwerk
Port 3	Client-Netzwerk (optional)
Port 4	Grid-Netzwerk

- Wenn Sie den aggregierten Port Bond-Modus verwenden möchten, verbinden Sie einen oder mehrere Netzwerkports mit einem oder mehreren Switches. Sie sollten mindestens zwei der vier Ports verbinden, um einen Single Point of Failure zu vermeiden. Wenn Sie mehrere Switches für eine einzelne LACP-Verbindung verwenden, müssen die Switches MLAG oder Äquivalent unterstützen.

3. Wenn Sie das Admin-Netzwerk für StorageGRID verwenden möchten, schließen Sie den Admin-Netzwerkport des Geräts über ein Ethernet-Kabel an das Admin-Netzwerk an.

Kabelgerät (SG6000)

Sie verbinden die Speicher-Controller mit dem SG6000-CN-Controller, verbinden die Management-Ports aller drei Controller und verbinden die Netzwerk-Ports des SG6000-CN-Controllers mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk für StorageGRID.

Bevor Sie beginnen

- Das Gerät verfügt über die vier optischen Kabel zum Anschließen der beiden Speicher-Controller an den SG6000-CN-Controller.
- Sie verfügen über RJ-45-Ethernet-Kabel (mindestens vier) für den Anschluss der Management-Ports.
- Sie haben eine der folgenden Optionen für die Netzwerkanschlüsse. Diese Gegenstände sind nicht im Lieferumfang des Geräts enthalten.
 - Ein bis vier Twinax-Kabel zum Anschließen der vier Netzwerk-Ports.
 - Ein bis vier SFP+ oder SFP28 Transceiver, wenn Sie optische Kabel für die Ports verwenden möchten.



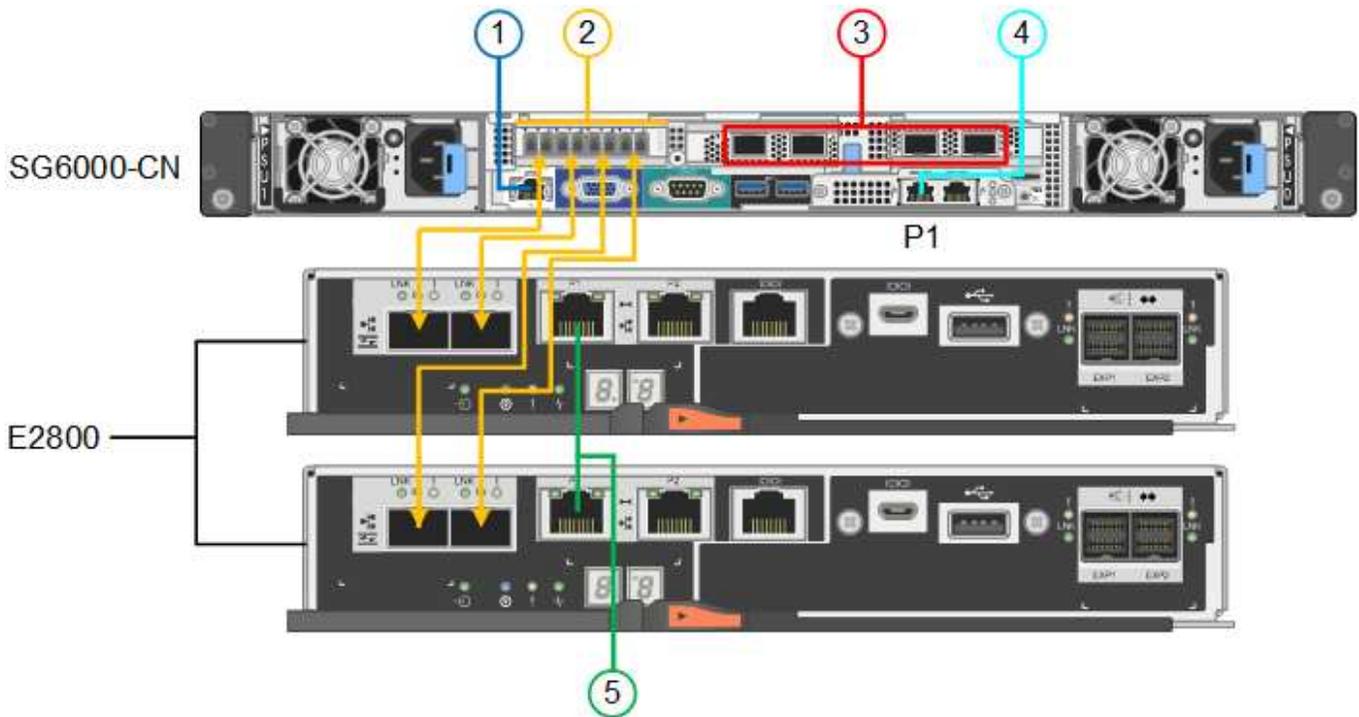
Gefahr der Laserstrahlung — keinen Teil eines SFP-Transceivers zerlegen oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

Über diese Aufgabe

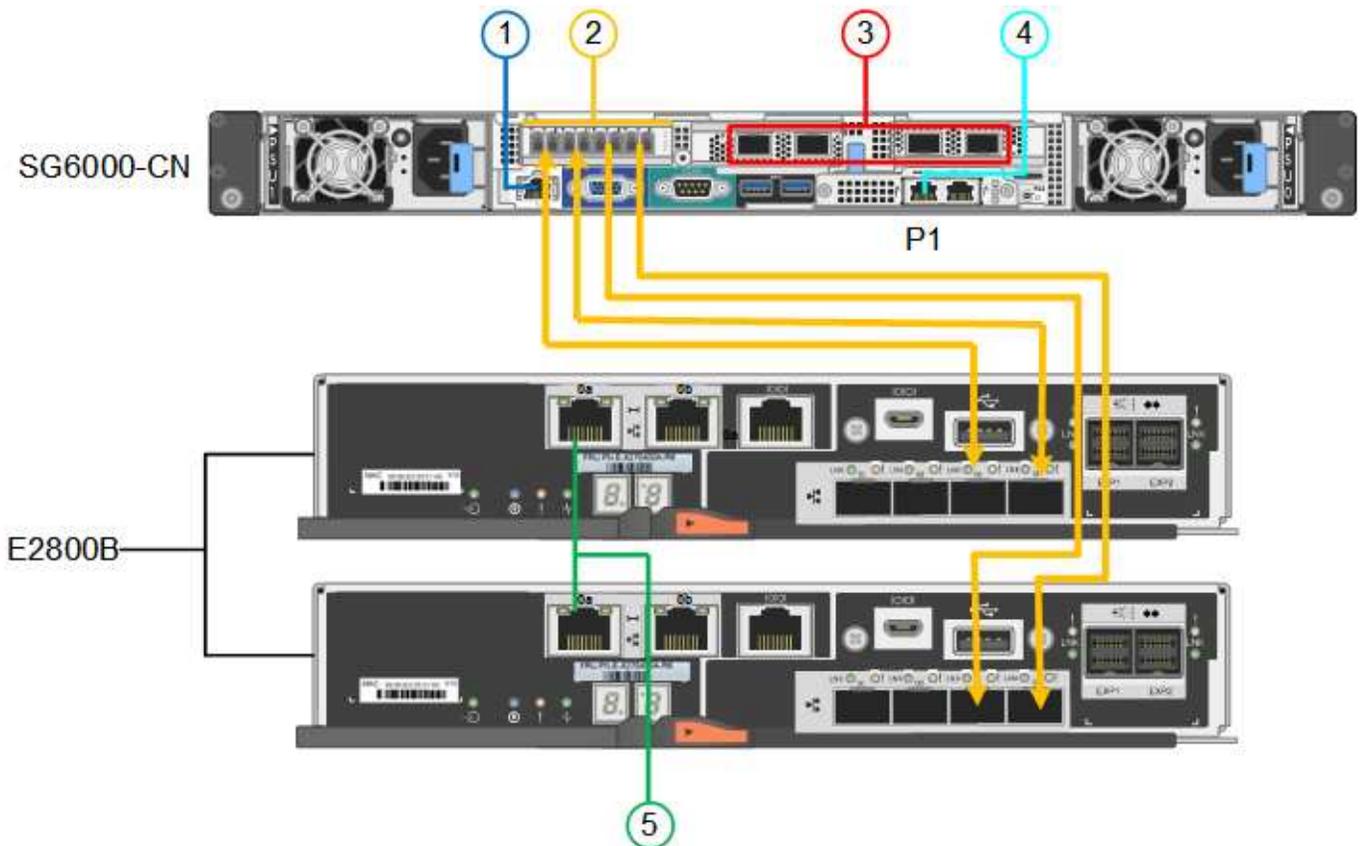
Die nachfolgende Abbildung zeigt die drei Controller in den SG6060 und SG6060X Appliances, wobei der SG6000-CN Computing-Controller oben und die beiden E2800 Storage-Controller unten dargestellt sind. Das SG6060 verwendet E2800A-Controller und das SG6060X verwendet E2800B-Controller.

-  Beide Versionen des E2800 Controllers haben die gleichen Spezifikationen und funktionieren mit Ausnahme der Lage der Interconnect-Ports.
-  Verwenden Sie keinen E2800A- und E2800B-Controller in derselben Appliance.

SG6060-Verbindungen:

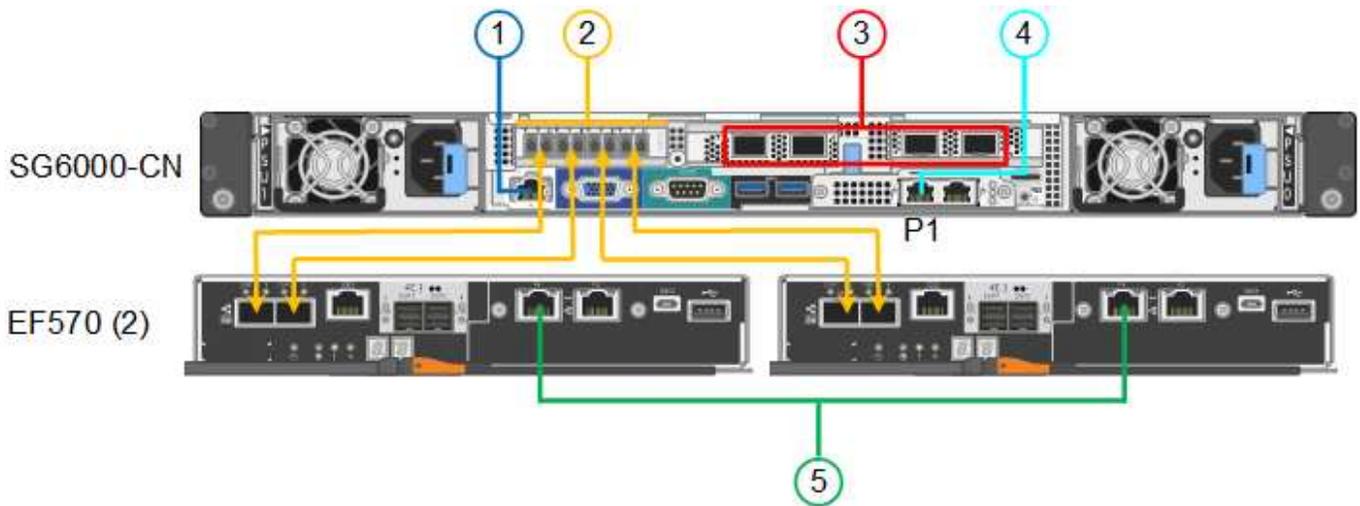


SG6060X-Verbindungen:



Die folgende Abbildung zeigt die drei Controller in der SGF6024 Appliance mit dem SG6000-CN Compute-Controller oben und den beiden EF570 Storage-Controllern nebeneinander unter dem Computing-Controller.

SGF6024-Verbindungen:



Legende	Port	Typ des Ports	Nutzung
1	BMC-Management-Port am SG6000-CN Controller	1 GbE (RJ-45)	Stellt eine Verbindung zum Netzwerk her, in dem Sie auf die BMC-Schnittstelle zugreifen.

Legende	Port	Typ des Ports	Nutzung
2	FC-Verbindungs-Ports: <ul style="list-style-type: none"> • 4 auf dem SG6000-CN-Controller • 2 auf jedem Storage Controller 	Optisches 16-Gbit/s FC SFP+	Verbinden Sie jeden Speicher-Controller mit dem SG6000-CN-Controller.
3	Vier Netzwerk-Ports auf dem SG6000-CN Controller	10/25-GbE	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.
4	Admin-Netzwerk-Port am SG6000-CN Controller (in der Abbildung mit P1 gekennzeichnet)	1 GbE (RJ-45) Wichtig: dieser Port arbeitet nur mit 1000 BaseT/Full und unterstützt keine Geschwindigkeiten von 10 oder 100 Megabit.	Verbindet den SG6000-CN-Controller mit dem Admin-Netzwerk für StorageGRID.
	Rechtmäßiger RJ-45-Anschluss am SG6000-CN-Controller	1 GbE (RJ-45) Wichtig: dieser Port arbeitet nur mit 1000 BaseT/Full und unterstützt keine Geschwindigkeiten von 10 oder 100 Megabit.	<ul style="list-style-type: none"> • Kann mit Verwaltungsport 1 verbunden werden, wenn Sie eine redundante Verbindung zum Admin-Netzwerk wünschen. • Kann unverkabelt und für temporären lokalen Zugang verfügbar sein (IP 169.254.0.1). • Kann während der Installation verwendet werden, um den SG6000-CN-Controller mit einem Service-Laptop zu verbinden, wenn keine DHCP-zugewiesenen IP-Adressen verfügbar sind.
5	Management-Port 1 auf jedem Storage Controller	1 GbE (RJ-45)	Stellt eine Verbindung mit dem Netzwerk her, in dem Sie auf SANtricity System Manager zugreifen.
	Management-Port 2 auf jedem Storage Controller	1 GbE (RJ-45)	Reserviert für technischen Support.

Schritte

1. Schließen Sie den BMC-Management-Port des SG6000-CN Controllers über ein Ethernet-Kabel an das Managementnetzwerk an.

Obwohl diese Verbindung optional ist, wird empfohlen, den Support zu erleichtern.

2. Verbinden Sie die beiden FC-Ports an jedem Speicher-Controller mit den FC-Ports des SG6000-CN Controllers. Verwenden Sie dazu vier optische Kabel und vier SFP+-Transceiver für die Speicher-

Controller.

3. Verbinden Sie die Netzwerk-Ports des SG6000-CN Controllers mit den entsprechenden Netzwerk-Switches über Twinax-Kabel oder optische Kabel und SFP+ oder SFP28 Transceiver.



Die vier Netzwerkanschlüsse müssen dieselbe Verbindungsgeschwindigkeit verwenden. Installieren Sie SFP+-Transceiver, wenn Sie 10-GbE-Verbindungsgeschwindigkeiten verwenden möchten. Installieren Sie SFP28 Transceiver, wenn Sie 25-GbE-Linkgeschwindigkeiten verwenden möchten.

- Wenn Sie den Modus Fixed Port Bond verwenden möchten (Standard), verbinden Sie die Ports mit dem StorageGRID-Grid und den Client-Netzwerken, wie in der Tabelle dargestellt.

Port	Verbindung wird hergestellt mit...
Port 1	Client-Netzwerk (optional)
Port 2	Grid-Netzwerk
Port 3	Client-Netzwerk (optional)
Port 4	Grid-Netzwerk

- Wenn Sie den aggregierten Port Bond-Modus verwenden möchten, verbinden Sie einen oder mehrere Netzwerkports mit einem oder mehreren Switches. Sie sollten mindestens zwei der vier Ports verbinden, um einen Single Point of Failure zu vermeiden. Wenn Sie mehrere Switches für eine einzelne LACP-Verbindung verwenden, müssen die Switches MLAG oder Äquivalent unterstützen.
4. Wenn Sie das Admin-Netzwerk für StorageGRID verwenden möchten, verbinden Sie den Admin-Netzwerkanschluss des SG6000-CN-Controllers über ein Ethernet-Kabel mit dem Admin-Netzwerk.
 5. Wenn Sie das Managementnetzwerk für SANtricity System Manager verwenden möchten, verbinden Sie Managementport 1 (P1) an jedem Storage Controller (der RJ-45-Port auf der linken Seite) mit einem Netzwerkmanagement für SANtricity System Manager.

Verwenden Sie den Management-Port 2 (P2) nicht auf den Speichercontrollern (der RJ-45-Port auf der rechten Seite). Dieser Port ist für technischen Support reserviert.

Verwandte Informationen

["Port-Bond-Modi \(SG6000-CN-Controller\)"](#)

Kabel-Appliance (SG5700)

Sie verbinden die beiden Controller miteinander, verbinden die Management-Ports auf jedem Controller und verbinden die 10/25-GbE-Ports des E5700SG Controllers mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk für StorageGRID.

Bevor Sie beginnen

- Sie haben die folgenden Artikel ausgepackt, die im Lieferumfang des Geräts enthalten sind:
 - Zwei Netzkabel.
 - Zwei optische Kabel für die FC Interconnect-Ports an den Controllern.

- Acht SFP+-Transceiver, die entweder 10 GbE oder 16 Gbit/s FC unterstützen. Die Transceiver können mit den beiden Interconnect Ports auf beiden Controllern und mit den vier 10/25-GbE-Netzwerkports auf dem E5700SG Controller verwendet werden, vorausgesetzt, die Netzwerk-Ports benötigen eine 10-GbE-Verbindungsgeschwindigkeit.
- Sie haben folgende Produkte erhalten, die nicht im Lieferumfang des Geräts enthalten sind:
 - Ein bis vier optische Kabel für die 10/25-GbE-Ports, die Sie verwenden möchten.
 - Ein bis vier SFP28-Transceiver, wenn Sie 25-GbE-Verbindungsgeschwindigkeit verwenden möchten.
 - Ethernet-Kabel für die Verbindung der Management-Ports.

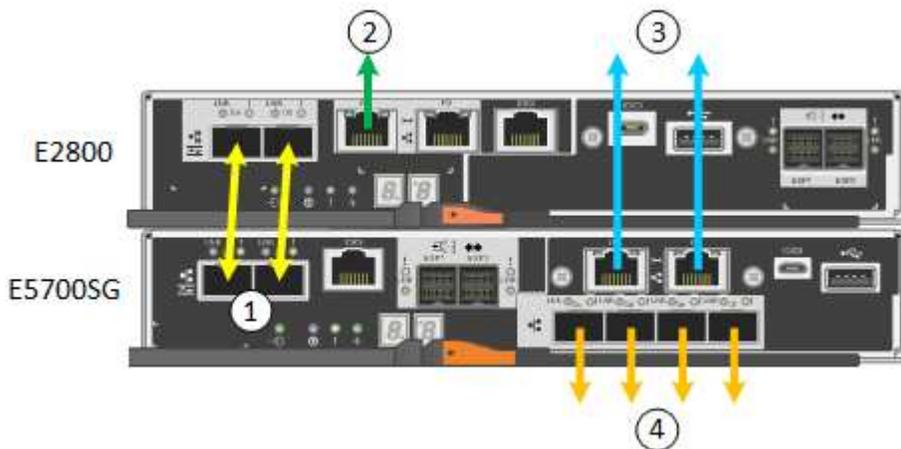


Gefahr der Laserstrahlung — keinen Teil eines SFP-Transceivers zerlegen oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

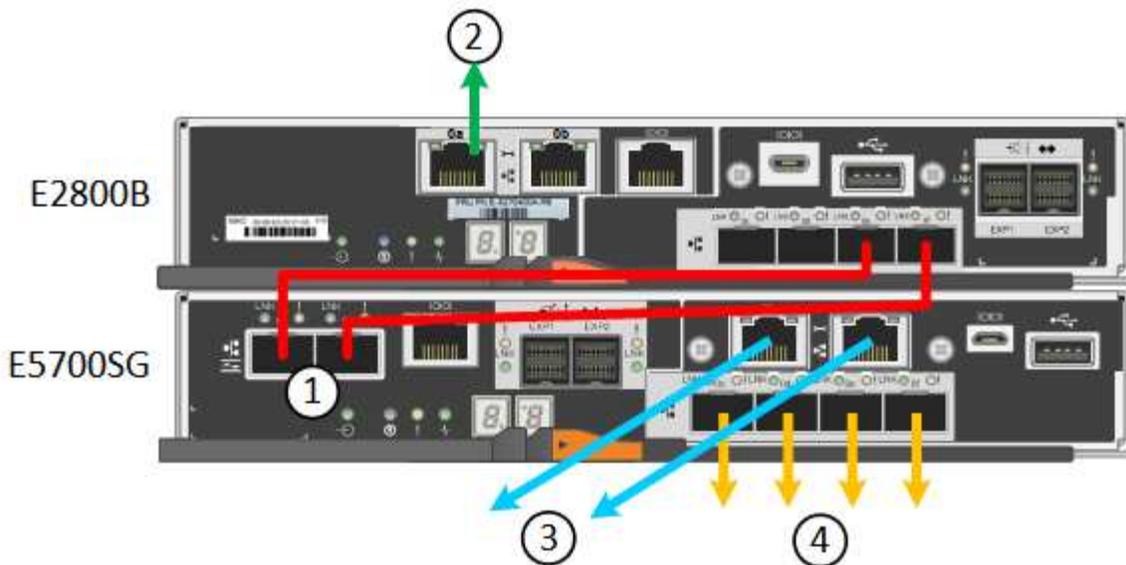
Über diese Aufgabe

Die Zahlen zeigen die beiden Controller der SG5760 und SG5760X, wobei der Storage Controller der E2800 Serie oben und der E5700SG Controller unten gezeigt werden. In den SG5712 und SG5712X befindet sich der Speicher-Controller der E2800 Serie links vom E5700SG-Controller, wenn er von hinten betrachtet wird.

SG5760-Verbindungen:



SG5760X-Verbindungen:



Legende	Port	Typ des Ports	Nutzung
1	Zwei Interconnect-Ports an jedem Controller	16 Gbit/s FC optisch SFP+	Verbinden Sie die beiden Controller miteinander.
2	Management-Port 1 auf dem Controller der E2800 Serie	1 GbE (RJ-45)	Stellt eine Verbindung mit dem Netzwerk her, in dem Sie auf SANtricity System Manager zugreifen. Sie können das Admin-Netzwerk für StorageGRID oder ein unabhängiges Managementnetzwerk verwenden.
2	Management-Port 2 auf dem Controller der E2800 Serie	1 GbE (RJ-45)	Reserviert für technischen Support.
3	Management-Port 1 am E5700SG Controller	1 GbE (RJ-45)	Verbindet den E5700SG-Controller mit dem Admin-Netzwerk für StorageGRID.

Legende	Port	Typ des Ports	Nutzung
3	Management-Port 2 am E5700SG Controller	1 GbE (RJ-45)	<ul style="list-style-type: none"> • Kann mit Verwaltungsport 1 verbunden werden, wenn Sie eine redundante Verbindung zum Admin-Netzwerk wünschen. • Kann unverkabelt und für temporären lokalen Zugang verfügbar sein (IP 169.254.0.1). • Kann während der Installation verwendet werden, um den E5700SG-Controller mit einem Service-Laptop zu verbinden, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.
4	10/25-GbE-Ports 1-4 auf dem E5700SG Controller	10-GbE oder 25-GbE Hinweis: die im Lieferumfang des Geräts enthaltenen SFP+ Transceiver unterstützen 10-GbE-Verbindungsgeschwindigkeiten. Wenn Sie für die vier Netzwerk-Ports 25-GbE-Verbindungsgeschwindigkeiten verwenden möchten, müssen Sie SFP28-Transceiver bereitstellen.	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her. Siehe "Port-Bond-Modi (E5700SG Controller)" .

Schritte

1. Verbinden Sie den E2800 Controller mit dem E5700SG Controller mithilfe von zwei optischen Kabeln und vier der acht SFP+ Transceiver.

Diesen Port verbinden...	Zu diesem Port...
Interconnect-Port 1 auf dem E2800 Controller	Interconnect-Port 1 am E5700SG Controller
Interconnect-Port 2 auf dem E2800 Controller	Interconnect-Port 2 am E5700SG Controller

2. Wenn Sie planen, SANtricity System Manager zu verwenden, verbinden Sie Managementport 1 (P1) am E2800 Controller (der RJ-45 Port auf der linken Seite) mit dem Managementnetzwerk für SANtricity System Manager. Verwenden Sie dazu ein Ethernetkabel.

Verwenden Sie den Management-Port 2 (P2) nicht auf dem E2800 Controller (der RJ-45-Port auf der rechten Seite). Dieser Port ist für technischen Support reserviert.

3. Wenn Sie das Admin-Netzwerk für StorageGRID verwenden möchten, verbinden Sie den Verwaltungsport 1 des E5700SG-Controllers (der RJ-45-Port links) über ein Ethernet-Kabel mit dem Admin-Netzwerk.

Wenn Sie den Active-Backup-Netzwerk-Bond-Modus für das Admin-Netzwerk verwenden möchten, verbinden Sie den Management-Port 2 des E5700SG-Controllers (der RJ-45-Port rechts) über ein Ethernet-Kabel mit dem Admin-Netzwerk.

4. Verbinden Sie die 10/25-GbE-Ports des E5700SG Controllers mit den entsprechenden Netzwerk-Switches über optische Kabel und SFP+ oder SFP28-Transceiver.



Alle Ports müssen dieselbe Verbindungsgeschwindigkeit verwenden. Installieren Sie SFP+-Transceiver, wenn Sie 10-GbE-Verbindungsgeschwindigkeiten verwenden möchten. Installieren Sie SFP28 Transceiver, wenn Sie 25-GbE-Linkgeschwindigkeiten verwenden möchten.

- Wenn Sie den Modus Fixed Port Bond verwenden möchten (Standard), verbinden Sie die Ports mit dem StorageGRID-Grid und den Client-Netzwerken, wie in der Tabelle dargestellt.

Port	Verbindung wird hergestellt mit...
Port 1	Client-Netzwerk (optional)
Port 2	Grid-Netzwerk
Port 3	Client-Netzwerk (optional)
Port 4	Grid-Netzwerk

- Wenn Sie den aggregierten Port Bond-Modus verwenden möchten, verbinden Sie einen oder mehrere Netzwerkports mit einem oder mehreren Switches. Sie sollten mindestens zwei der vier Ports verbinden, um einen Single Point of Failure zu vermeiden. Wenn Sie mehrere Switches für eine einzelne LACP-Verbindung verwenden, müssen die Switches MLAG oder Äquivalent unterstützen.

Verwandte Informationen

["Rufen Sie das Installationsprogramm für StorageGRID-Appliances auf"](#)

Kabelgerät (SG100 und SG1000)

Sie müssen den Management-Port der Appliance mit dem Service-Laptop verbinden und die Netzwerkanschlüsse der Appliance mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk für StorageGRID verbinden.

Bevor Sie beginnen

- Sie verfügen über ein RJ-45-Ethernet-Kabel zum Anschließen des Management-Ports.
- Sie haben eine der folgenden Optionen für die Netzwerkanschlüsse. Diese Gegenstände sind nicht im Lieferumfang des Geräts enthalten.
 - Ein bis vier Twinax-Kabel zum Anschließen der vier Netzwerk-Ports.
 - Für das SG100 sind ein bis vier SFP+ oder SFP28 Transceiver, wenn Sie optische Kabel für die Ports verwenden möchten.

- Für den SG1000, ein bis vier QSFP+ oder QSFP28 Transceiver, wenn Sie optische Kabel für die Ports verwenden möchten.

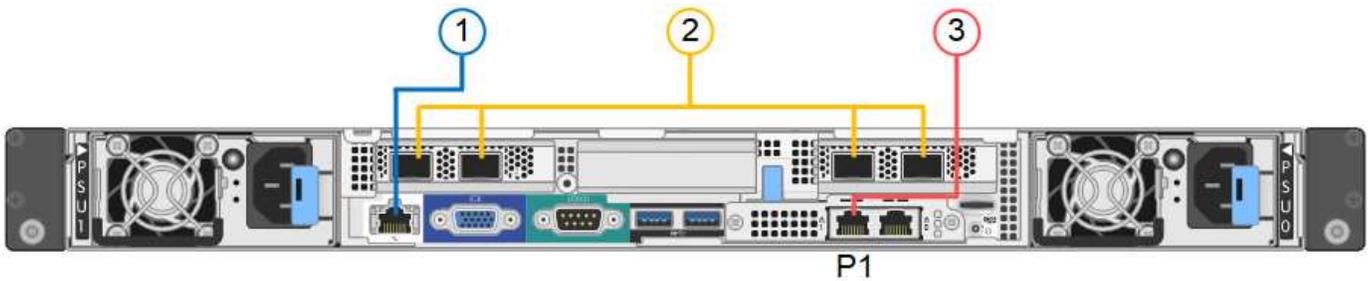


Gefahr der Laserstrahlung — kein Teil eines SFP- oder QSFP-Transceivers demontieren oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

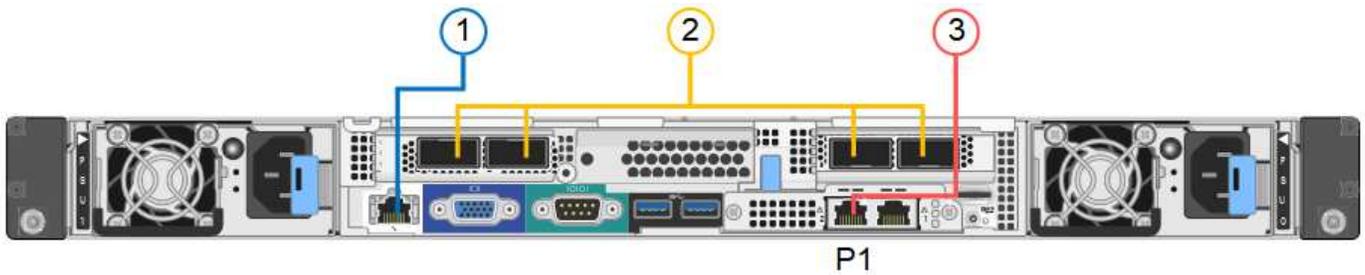
Über diese Aufgabe

Die folgenden Abbildungen zeigen die Anschlüsse auf der Rückseite des Geräts.

SG100-Port-Verbindungen:



SG1000-Port-Verbindungen:



Legende	Port	Typ des Ports	Nutzung
1	BMC-Management-Port auf der Appliance	1 GbE (RJ-45)	Stellt eine Verbindung zum Netzwerk her, in dem Sie auf die BMC-Schnittstelle zugreifen.
2	Vier Netzwerkports auf der Appliance	<ul style="list-style-type: none"> • Für das SG100: 10/25-GbE • Für den SG1000: 10/25/40/100-GbE 	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.
3	Admin-Netzwerk-Port auf der Appliance (in den Abbildungen mit „P1“ gekennzeichnet)	1 GbE (RJ-45) Wichtig: dieser Port arbeitet nur mit 1000 BaseT/Full und unterstützt keine Geschwindigkeiten von 10 oder 100 Megabit.	Verbindet die Appliance mit dem Admin-Netzwerk für StorageGRID.

Legende	Port	Typ des Ports	Nutzung
	Rechtmäßiger RJ-45-Anschluss am Gerät	1 GbE (RJ-45) Wichtig: dieser Port arbeitet nur mit 1000 BaseT/Full und unterstützt keine Geschwindigkeiten von 10 oder 100 Megabit.	<ul style="list-style-type: none"> • Kann mit Verwaltungsport 1 verbunden werden, wenn Sie eine redundante Verbindung zum Admin-Netzwerk wünschen. • Kann getrennt bleiben und für einen temporären lokalen Zugang verfügbar sein (IP 169.254.0.1). • Während der Installation kann verwendet werden, um das Gerät an einen Service-Laptop anzuschließen, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

Schritte

1. Schließen Sie den BMC-Managementport der Appliance über ein Ethernet-Kabel an das Managementnetzwerk an.

Obwohl diese Verbindung optional ist, wird empfohlen, den Support zu erleichtern.

2. Verbinden Sie die Netzwerk-Ports des Geräts mit den entsprechenden Netzwerk-Switches über Twinax-Kabel oder optische Kabel und Transceiver.

Alle vier Netzwerkports müssen dieselbe Verbindungsgeschwindigkeit verwenden. In der folgenden Tabelle finden Sie die für Ihre Hardware und Verbindungsgeschwindigkeit erforderlichen Geräte.



SG100 Verbindungsgeschwindigkeit (GbE)	Erforderliche Ausrüstung
10	SFP+-Transceiver
25	SFP28-Transceiver
SG1000 Link-Geschwindigkeit (GbE)	Erforderliche Ausrüstung
10	QSA- und SFP+-Transceiver
25	QSA und SFP28 Transceiver
40	QSFP+-Transceiver
100	QFSP28-Transceiver

- Wenn Sie den Modus Fixed Port Bond verwenden möchten (Standard), verbinden Sie die Ports mit dem StorageGRID-Grid und den Client-Netzwerken, wie in der Tabelle dargestellt.

Port	Verbindung wird hergestellt mit...
Port 1	Client-Netzwerk (optional)
Port 2	Grid-Netzwerk
Port 3	Client-Netzwerk (optional)
Port 4	Grid-Netzwerk

- Wenn Sie den aggregierten Port Bond-Modus verwenden möchten, verbinden Sie einen oder mehrere Netzwerkports mit einem oder mehreren Switches. Sie sollten mindestens zwei der vier Ports verbinden, um einen Single Point of Failure zu vermeiden. Wenn Sie mehrere Switches für eine einzelne LACP-Verbindung verwenden, müssen die Switches MLAG oder Äquivalent unterstützen.
3. Wenn Sie das Admin-Netzwerk für StorageGRID verwenden möchten, schließen Sie den Admin-Netzwerkport des Geräts über ein Ethernet-Kabel an das Admin-Netzwerk an.

Stromkabel anschließen und Strom anschließen

Stromkabel anschließen und Strom anschließen (SGF6112)

Nach dem Anschließen der Netzkabel können Sie das Gerät mit Strom versorgen.

Schritte

1. Schließen Sie ein Netzkabel an jede der beiden Netzteile im Gerät an.
2. Schließen Sie diese beiden Netzkabel an zwei verschiedene Stromverteiler (Power Distribution Units, PDUs) im Schrank oder Rack an.
3. Wenn der Netzschalter auf der Vorderseite des Geräts derzeit nicht blau leuchtet, drücken Sie die Taste, um das Gerät einzuschalten.

Drücken Sie den Netzschalter während des Einschaltens nicht erneut.

Die LED am Netzteil sollte grün leuchten, ohne zu blinken.

4. Wenn Fehler auftreten, beheben Sie alle Probleme.
5. Befestigen Sie die Frontverkleidung am Gerät, falls sie entfernt wurde.

Verwandte Informationen

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

Anschließen des Netzes und Anwenden der Stromversorgung (SG6000)

Nach dem Anschließen der Netzkabel können Sie den SG6000-CN Controller und die beiden Storage Controller oder optionale Erweiterungs-Shelfs mit Strom versorgen.

Schritte

1. Vergewissern Sie sich, dass beide Controller im Storage-Controller-Shelf deaktiviert sind.



Gefahr eines elektrischen Schlags — vor dem Anschließen der Netzkabel sicherstellen, dass die Netzschalter für jeden der beiden Speicher-Controller ausgeschaltet sind.

2. Wenn Sie über Erweiterungs-Shelfs verfügen, bestätigen Sie, dass beide IOM-Netzschalter aus sind.



Gefahr eines elektrischen Schlags — bevor Sie die Netzkabel anschließen, stellen Sie sicher, dass die beiden Netzschalter für jedes Erweiterungs-Regal ausgeschaltet sind.

3. Schließen Sie ein Netzkabel an jedes der beiden Netzteile im SG6000-CN-Controller an.
4. Schließen Sie diese beiden Netzkabel an zwei verschiedene Stromverteiler (Power Distribution Units, PDUs) im Schrank oder Rack an.
5. Schließen Sie ein Netzkabel an jede der beiden Netzteile im Storage Controller Shelf an.
6. Wenn Sie über Erweiterungs-Shelfs verfügen, schließen Sie ein Netzkabel an jede der beiden Netzteile in jedem Erweiterungs-Shelf an.
7. Verbinden Sie die beiden Netzkabel jedes Storage Shelf (einschließlich der optionalen Erweiterungs-Shelfs) mit zwei verschiedenen PDUs im Rack oder Rack.
8. Wenn der Netzschalter an der Vorderseite des SG6000-CN Controllers derzeit nicht blau leuchtet, drücken Sie die Taste, um den Controller einzuschalten.

Drücken Sie den Netzschalter während des Einschaltens nicht erneut.

9. Schalten Sie die beiden Netzschalter auf der Rückseite des Storage Controller Shelf ein. Wenn Sie über Erweiterungs-Shelfs verfügen, schalten Sie die beiden Netzschalter für jedes Shelf ein.
 - Schalten Sie die Netzschalter während des Einschaltens nicht aus.
 - Die Lüfter im Storage Controller Shelf und optionale Erweiterungs-Shelfs sind beim ersten Starten möglicherweise sehr laut. Das laute Geräusch beim Anfahren ist normal.
10. Überprüfen Sie nach dem Starten der Komponenten den Status.
 - Überprüfen Sie die sieben-Segment-Anzeige auf der Rückseite jedes Storage Controllers. Weitere Informationen finden Sie im Artikel über die Anzeige von Boot-Statuscodes.
 - Stellen Sie sicher, dass der Netzschalter an der Vorderseite des SG6000-CN-Controllers leuchtet.
11. Wenn Fehler auftreten, beheben Sie alle Probleme.
12. Befestigen Sie die Frontverkleidung bei Entfernung am SG6000-CN Controller.

Verwandte Informationen

- ["Statusanzeigen anzeigen anzeigen anzeigen"](#)
- ["Installieren Sie den SG6000-CN Controller wieder in den Schrank oder Rack"](#)

Stromkabel anschließen und Strom (SG5700) einschalten

Wenn Sie das Gerät mit Strom versorgen, werden beide Controller gestartet.

Bevor Sie beginnen

Vor dem Anschließen an die Stromversorgung müssen beide Netzschalter des Geräts ausgeschaltet sein.



Gefahr eines elektrischen Schlags — bevor Sie die Netzkabel anschließen, stellen Sie sicher, dass die beiden Netzschalter am Gerät ausgeschaltet sind.

Schritte

1. Stellen Sie sicher, dass die beiden Netzschalter am Gerät aus sind.
2. Schließen Sie die beiden Netzkabel an das Gerät an.
3. Verbinden Sie die beiden Netzkabel mit verschiedenen Stromverteilereinheiten (Power Distribution Units, PDUs) im Schrank oder Rack.
4. Schalten Sie die beiden Netzschalter am Gerät ein.
 - Schalten Sie die Netzschalter während des Einschalters nicht aus.
 - Die Fans sind beim ersten Start sehr laut. Das laute Geräusch beim Anfahren ist normal.
5. Prüfen Sie nach dem Starten der Controller ihre sieben Segmente.

Stromkabel anschließen und Strom einstecken (SG100 und SG1000)

Nach dem Anschließen der Netzkabel können Sie das Gerät mit Strom versorgen.

Schritte

1. Schließen Sie ein Netzkabel an jede der beiden Netzteile im Gerät an.
2. Schließen Sie diese beiden Netzkabel an zwei verschiedene Stromverteiler (Power Distribution Units, PDUs) im Schrank oder Rack an.
3. Wenn der Netzschalter auf der Vorderseite des Geräts derzeit nicht blau leuchtet, drücken Sie die Taste, um das Gerät einzuschalten.

Drücken Sie den Netzschalter während des Einschalters nicht erneut.

4. Wenn Fehler auftreten, beheben Sie alle Probleme.
5. Befestigen Sie die Frontverkleidung am Gerät, falls sie entfernt wurde.

Verwandte Informationen

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

Statusanzeigen und -Codes anzeigen

Die Geräte und Controller enthalten Anzeigen, mit denen Sie den Status der Gerätekomponenten ermitteln können.

SGF6112

Die Appliance enthält Anzeigen, mit denen Sie den Status des Appliance-Controllers und der SSDs ermitteln können:

- [Geräteteuchten und -Tasten](#)
- [Allgemeine Startcodes](#)
- [SSD-LEDs](#)

Verwenden Sie diese Informationen, um zu helfen ["Fehlerbehebung bei der Installation der SGF6112-Hardware"](#).

Geräteteuchten und -Tasten

Die folgende Abbildung zeigt Anzeigen und Tasten am SG6112-Gerät.



Legende	Anzeige	Status
1	Ein-/aus-Schalter	<ul style="list-style-type: none">• Blau: Das Gerät ist eingeschaltet.• Aus: Das Gerät ist ausgeschaltet.
2	Reset-Taste	Mit dieser Taste können Sie den Controller auf einen harten Reset zurücksetzen.
3	Schaltfläche „Identifizierung“	Mit dem BMC kann diese Taste auf Blinken, ein (Vollton) oder aus eingestellt werden. <ul style="list-style-type: none">• Blau, blinkend: Identifiziert das Gerät im Schrank oder Rack.• Blau, fest: Identifiziert das Gerät im Schrank oder Rack.• Aus: Das Gerät ist im Schrank oder Rack nicht visuell erkennbar.
4	Status-LED	<ul style="list-style-type: none">• Gelb, konstant: Ein Fehler ist aufgetreten. <p>Hinweis: um die Boot-up- und Fehlercodes anzuzeigen, "Rufen Sie die BMC-Schnittstelle auf".</p> <ul style="list-style-type: none">• Aus: Es sind keine Fehler vorhanden.
5	PFR	Diese Leuchte wird vom SGF6112-Gerät nicht verwendet und bleibt ausgeschaltet.

Allgemeine Startcodes

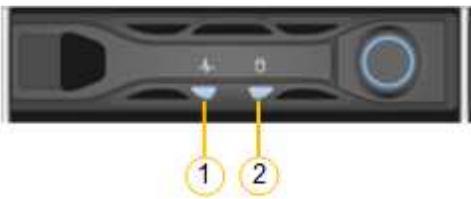
Beim Hochfahren oder nach einem harten Reset des Geräts treten folgende Aktionen auf:

1. Der BMC (Baseboard Management Controller) protokolliert Codes für die Boot-Sequenz, einschließlich etwaiger Fehler.
2. Der Betriebsschalter leuchtet auf.
3. Wenn während des Startvorgangs Fehler auftreten, leuchtet die Alarm-LED auf.

So zeigen Sie die Starts- und Fehlercodes an: ["Rufen Sie die BMC-Schnittstelle auf"](#).

SSD-LEDs

Die folgende Abbildung zeigt die SSD-Anzeigen auf der SG6112-Appliance.



LED	Anzeige	Status
1	Laufwerksstatus/-Fehler	<ul style="list-style-type: none">• Blau (fest): Laufwerk ist online• Gelb (konstant): Laufwerksausfall• Aus: Steckplatz ist leer <p>Hinweis: Wenn eine neue funktionierende SSD in einen funktionierenden SG6112 StorageGRID-Knoten eingesteckt wird, sollten die LEDs auf der SSD zunächst blinken, aber aufhören zu blinken, sobald das System feststellt, dass das Laufwerk über genügend Kapazität verfügt und funktionsfähig ist.</p>
2	Laufwerk aktiv	Blau (blinkend): Auf das Laufwerk wird zugegriffen

SG6000

Die SG6000 Appliance-Controller enthalten Anzeigen, die Ihnen helfen, den Status des Appliance-Controllers zu bestimmen:

- [Statusanzeigen und -Tasten am SG6000-CN-Controller](#)
- [Allgemeine Startcodes](#)
- [Statuscodes für das Booten der SG6000-Speicher-Controller](#)

Verwenden Sie diese Informationen, um zu helfen ["Fehlerbehebung bei der SG6000 Installation"](#).

Statusanzeigen und -Tasten am SG6000-CN-Controller

Der SG6000-CN-Controller enthält Anzeigen, mit denen Sie den Status des Controllers bestimmen können, einschließlich der folgenden Anzeigen und Schaltflächen.

Die folgende Abbildung zeigt Statusanzeigen und -Tasten am SG6000-CN-Controller.



Legende	Anzeige	Beschreibung
1	Ein-/aus-Schalter	<ul style="list-style-type: none">• Blau: Der Controller ist eingeschaltet.• Aus: Der Controller ist ausgeschaltet.
2	Reset-Taste	<i>Kein Indikator</i> Mit dieser Taste können Sie den Controller auf einen harten Reset zurücksetzen.
3	Schaltfläche „Identifizierung“	<ul style="list-style-type: none">• Blinkt oder leuchtet blau: Identifiziert den Controller im Schrank oder Rack.• Aus: Die Steuerung ist im Schrank oder Rack nicht visuell erkennbar. Diese Taste kann auf „Blinken“, „ein“ (Festkörper) oder „aus“ eingestellt werden.
4	Alarm-LED	<ul style="list-style-type: none">• Gelb: Ein Fehler ist aufgetreten. Hinweis: um die Boot-up- und Fehlercodes anzuzeigen, " Rufen Sie die BMC-Schnittstelle auf ". <ul style="list-style-type: none">• Aus: Es sind keine Fehler vorhanden.

Allgemeine Startcodes

Beim Hochfahren oder nach einem harten Reset des SG6000-CN-Controllers treten folgende Aktionen auf:

1. Der BMC (Baseboard Management Controller) protokolliert Codes für die Boot-Sequenz, einschließlich etwaiger Fehler.
2. Der Betriebsschalter leuchtet auf.
3. Wenn während des Startvorgangs Fehler auftreten, leuchtet die Alarm-LED auf.

So zeigen Sie die Starts- und Fehlercodes an: "[Rufen Sie die BMC-Schnittstelle auf](#)".

Statuscodes für das Booten der SG6000-Speicher-Controller

Jeder Storage Controller verfügt über eine Anzeige in sieben Segmenten, die Statuscodes bereitstellt, wenn der Controller heruntergefahren wird. Die Statuscodes sind sowohl für den E2800 Controller als auch für den EF570 Controller identisch.

Beschreibungen dieser Codes finden Sie in den Informationen zur Systemüberwachung der E-Series für Ihren Storage Controller-Typ.

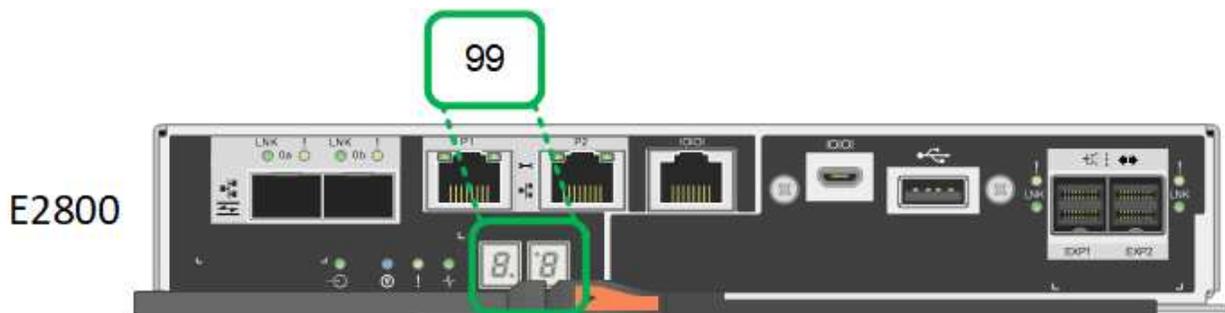
Schritte

1. Überwachen Sie während des Startvorgangs den Fortschritt, indem Sie die auf der siebensegmentreichen Anzeige angezeigten Codes für jeden Storage-Controller anzeigen.

Die sieben-Segment-Anzeige auf jedem Speicher-Controller zeigt die sich wiederholende Sequenz **OS**, **SD**, **blank** Um anzugeben, dass der Controller die Tagesbeginn-Verarbeitung durchführt.

2. Vergewissern Sie sich, dass nach dem Booten der Controller 99 angezeigt wird. Diese ist die Standard-ID für ein E-Series Controller-Shelf.

Vergewissern Sie sich, dass dieser Wert auf beiden Storage-Controllern angezeigt wird. Diese Abbildung zeigt in diesem Beispiel den E2800 Controller.



3. Wenn ein Controller oder beide andere Werte anzeigen, lesen Sie "[Fehlerbehebung bei der Hardwareinstallation \(SG6000 oder SG5700\)](#)" Und bestätigen Sie, dass Sie die Installationsschritte korrekt ausgeführt haben. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Verwandte Informationen

- "[NetApp Support](#)"
- "[Schalten Sie den SG6000-CN Controller ein, und überprüfen Sie den Betrieb](#)"

SG5700

Die Gerätesteuerung enthält Anzeigen, die Ihnen helfen, den Status der Gerätesteuerung zu bestimmen:

- [SG5700-Startstatuscodes](#)
- [Statusanzeigen am E5700SG Controller](#)
- [Allgemeine Startcodes](#)
- [Boot-Codes des E5700SG-Controllers](#)
- [E5700SG-Controller-Fehlercodes](#)

Verwenden Sie diese Informationen, um zu helfen "[Fehler bei der Installation der SG5700-Hardware beheben](#)".

SG5700-Startstatuscodes

Die sieben-Segment-Anzeigen auf jedem Controller zeigen Status- und Fehlercodes an, wenn das Gerät eingeschaltet wird.

Der E2800 Controller und der E5700SG Controller zeigen verschiedene Status und Fehlercodes an.

Um zu verstehen, was diese Codes bedeuten, lesen Sie die folgenden Ressourcen:

Controller	Referenz
E2800 Controller	<i>E5700 and E2800 System Monitoring Guide</i> Hinweis: die für den E5700 Controller der E-Series aufgeführten Codes gelten nicht für den E5700SG Controller in der Appliance.
E5700SG Controller	„status-Indikatoren am E5700SG-Controller“

Schritte

- Überwachen Sie während des Startvorgangs den Fortschritt, indem Sie die Codes auf den sieben Segmentanzeigen anzeigen.
 - Das 7-Segment-Display auf dem E2800-Controller zeigt die sich wiederholende Sequenz **OS**, **SD**, **blank** Um anzugeben, dass es die Tagesbeginn-Verarbeitung durchführt.
 - Das 7-Segment-Display des E5700SG-Reglers zeigt eine Sequenz von Codes an, die mit **AA** und **FF** enden.
- Bestätigen Sie, dass die sieben-Segment-Anzeigen nach dem Booten der Controller Folgendes anzeigen:

Controller	Sieben-Segment-Anzeige
E2800 Controller	Zeigt 99. Dies ist die Standard-ID für ein E-Series Controller-Shelf.
E5700SG Controller	<p>Zeigt HO, gefolgt von einer sich wiederholenden Sequenz von zwei Zahlen.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"><pre>HO -- IP address for Admin Network -- IP address for Grid Network HO</pre></div> <p>In der Sequenz ist der erste Zahlensatz die IP-Adresse, die vom DHCP für den Management-Port 1 des Controllers zugewiesen wird. Diese Adresse wird verwendet, um den Controller mit dem Admin-Netzwerk für StorageGRID zu verbinden. Die zweite Zahlengruppe ist die durch DHCP zugewiesene IP-Adresse, die zur Verbindung des Geräts mit dem Grid Network for StorageGRID verwendet wird.</p> <p>Hinweis: konnte eine IP-Adresse nicht über DHCP zugewiesen werden, wird 0.0.0.0 angezeigt.</p>

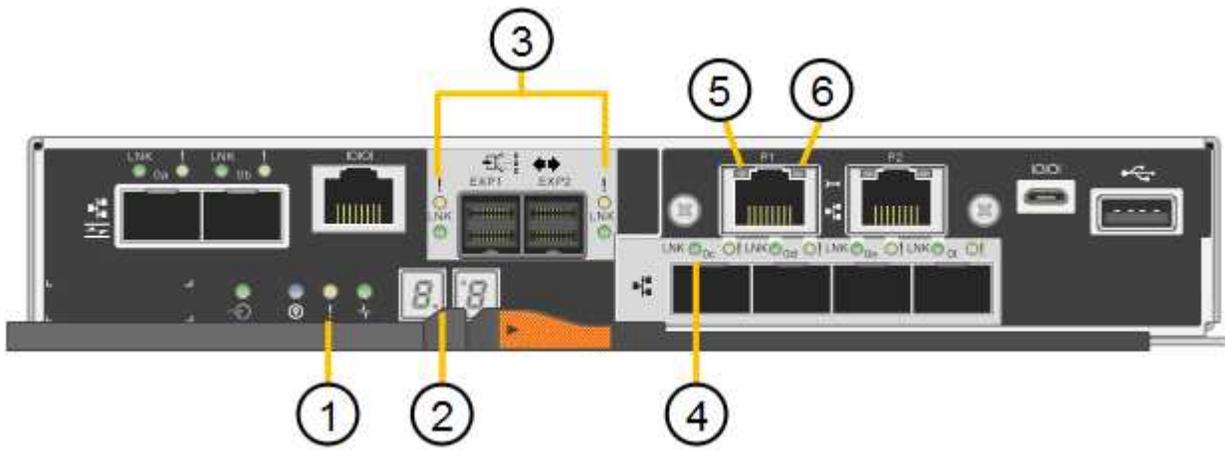
3. Wenn die sieben Segmente andere Werte anzeigen, siehe "[Fehlerbehebung bei der Hardwareinstallation \(SG6000 oder SG5700\)](#)" Und bestätigen Sie, dass Sie die Installationsschritte korrekt ausgeführt haben. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Statusanzeigen am E5700SG Controller

Die sieben-Segment-Anzeige und die LEDs auf dem E5700SG-Controller zeigen Status- und Fehlercodes an, während das Gerät eingeschaltet wird und die Hardware initialisiert wird. Sie können diese Anzeigen verwenden, um den Status zu bestimmen und Fehler zu beheben.

Nach dem Starten des Installationsprogramms für StorageGRID-Appliances sollten Sie die Statusanzeigen auf dem E5700SG-Controller regelmäßig überprüfen.

Die folgende Abbildung zeigt Statusanzeigen auf dem E5700SG Controller.



Legende	Anzeige	Beschreibung
1	Warnungs-LED	Gelb: Der Controller ist fehlerhaft und erfordert eine Bedienerwarnung, oder das Installationskript wurde nicht gefunden. Aus: Der Controller funktioniert ordnungsgemäß.
2	Sieben-Segment-Anzeige	Zeigt einen Diagnosecode an Sieben-Segment-Anzeigesequenzen ermöglichen es Ihnen, Fehler und den Betriebszustand der Appliance zu verstehen.
3	Warn-LEDs für den Erweiterungsport	Gelb: Diese LEDs sind immer gelb (keine Verbindung hergestellt), da das Gerät die Erweiterungs-Ports nicht nutzt.

Legende	Anzeige	Beschreibung
4	Status-LEDs für Host-Port-Link	Grün: Die Verbindung ist aktiviert. Aus: Die Verbindung ist ausgefallen.
5	Status-LEDs für Ethernet Link	Grün: Es wird eine Verbindung hergestellt. Aus: Keine Verbindung hergestellt.
6	LEDs für Ethernet-Aktivität	Grün: Die Verbindung zwischen dem Management-Port und dem Gerät, mit dem er verbunden ist (z. B. ein Ethernet-Switch) ist aktiviert. Aus: Es besteht keine Verbindung zwischen dem Controller und dem angeschlossenen Gerät. Blinkt grün: Es gibt Ethernet-Aktivität.

Allgemeine Startcodes

Beim Hochfahren oder nach einem harten Reset des Geräts treten folgende Aktionen auf:

1. Die sieben-Segment-Anzeige auf dem E5700SG-Controller zeigt eine allgemeine Sequenz von Codes, die nicht spezifisch für die Steuerung ist. Die allgemeine Sequenz endet mit den Codes AA und FF.
2. Startcodes, die speziell für den E5700SG-Controller gelten, werden angezeigt.

Boot-Codes des E5700SG-Controllers

Beim normalen Hochfahren des Geräts zeigt das siebenSegment-Display des E5700SG-Controllers die folgenden Codes in der angegebenen Reihenfolge an:

Codieren	Zeigt An
HI	Das Master-Boot-Skript wurde gestartet.
PP	Das System prüft, ob das FPGA aktualisiert werden muss.
HP	Das System überprüft, ob die 10/25-GbE-Controller-Firmware aktualisiert werden muss.
RB	Das System wird nach dem Anwenden von Firmware-Updates neu gebootet.
FP	Die Update-Prüfungen der Hardware-Subsystem-Firmware wurden abgeschlossen. Die Kommunikationsdienste zwischen den Controllern werden gestartet.

Codieren	Zeigt An
ER	Das System wartet auf die Konnektivität mit dem E2800 Controller und synchronisiert mit dem Betriebssystem SANtricity. Hinweis: Wenn dieser Bootvorgang nicht über diese Phase hinaus läuft, überprüfen Sie die Verbindungen zwischen den beiden Controllern.
HZ	Das System prüft gerade auf vorhandene StorageGRID Installationsdaten.
HO	Das Installationsprogramm für StorageGRID-Appliance wird ausgeführt.
HOCHVERFÜGBARKEIT	StorageGRID wird ausgeführt.

E5700SG-Controller-Fehlercodes

Diese Codes stellen Fehlerbedingungen dar, die auf dem E5700SG-Controller angezeigt werden können, wenn das Gerät hochfährt. Weitere zweistellige Hexadezimalcodes werden angezeigt, wenn bestimmte Hardware-Fehler auf niedriger Ebene auftreten. Wenn einer dieser Codes länger als ein oder zwei Sekunden andauert oder wenn Sie den Fehler nicht beheben können, indem Sie einem der vorgeschriebenen Fehlerbehebungsverfahren folgen, wenden Sie sich an den technischen Support.

Codieren	Zeigt An
22	Kein Master-Boot-Datensatz auf einem Boot-Gerät gefunden.
23	Das interne Flash-Laufwerk ist nicht verbunden.
2 A, 2 B	Stuck-Bus, DIMM-SPD-Daten können nicht gelesen werden.
40	Ungültige DIMMs.
41	Ungültige DIMMs.
42	Speichertest fehlgeschlagen.
51	Fehler beim SPD-Lesen.
92 bis 96	PCI-Bus-Initialisierung
A0 bis A3	SATA-Laufwerk-Initialisierung
AB	Alternativer Startcode:
AE	Booten von OS:
EA	DDR4-Schulung fehlgeschlagen.

Codieren	Zeigt An
E8	Kein Speicher installiert.
EU	Das Installationskript wurde nicht gefunden.
EP	Installation oder Kommunikation mit dem E2800-Controller ist fehlgeschlagen.

Verwandte Informationen

- ["NetApp Support"](#)
- ["E5700 und E2800 – System Monitoring Guide"](#)

SG100 und SG1000

Die Appliance enthält Anzeigen, die Ihnen beim Bestimmen des Status des Appliance-Controllers und der beiden SSDs helfen:

- [Geräteteuchten und -Tasten](#)
- [Allgemeine Startcodes](#)
- [SSD-LEDs](#)

Verwenden Sie diese Informationen, um zu helfen ["Fehlerbehebung bei der Hardwareinstallation von SG100 und SG1000"](#).

Geräteteuchten und -Tasten

Die folgende Abbildung zeigt Statusanzeigen und -Tasten des SG100 und SG1000.



Legende	Anzeige	Status
1	Ein-/aus-Schalter	<ul style="list-style-type: none"> • Blau: Das Gerät ist eingeschaltet. • Aus: Das Gerät ist ausgeschaltet.
2	Reset-Taste	Mit dieser Taste können Sie den Controller auf einen harten Reset zurücksetzen.

Legende	Anzeige	Status
3	Schaltfläche „Identifizierung“	<p>Diese Taste kann auf „Blinken“, „ein“ (Festkörper) oder „aus“ eingestellt werden.</p> <ul style="list-style-type: none"> • Blau, blinkend: Identifiziert das Gerät im Schrank oder Rack. • Blau, fest: Identifiziert das Gerät im Schrank oder Rack. • Aus: Das Gerät ist im Schrank oder Rack nicht visuell erkennbar.
4	Alarm-LED	<ul style="list-style-type: none"> • Gelb, konstant: Ein Fehler ist aufgetreten. <p>Hinweis: um die Boot-up- und Fehlercodes anzuzeigen, "Rufen Sie die BMC-Schnittstelle auf".</p> <ul style="list-style-type: none"> • Aus: Es sind keine Fehler vorhanden.

Allgemeine Startcodes

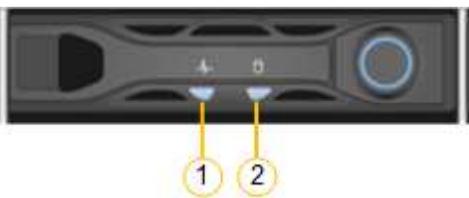
Beim Hochfahren oder nach einem harten Reset des Geräts treten folgende Aktionen auf:

1. Der BMC (Baseboard Management Controller) protokolliert Codes für die Boot-Sequenz, einschließlich etwaiger Fehler.
2. Der Betriebsschalter leuchtet auf.
3. Wenn während des Startvorgangs Fehler auftreten, leuchtet die Alarm-LED auf.

So zeigen Sie die Starts- und Fehlercodes an: "[Rufen Sie die BMC-Schnittstelle auf](#)".

SSD-LEDs

Die folgende Abbildung zeigt die SSD-Anzeigen auf dem SG100 und SG1000.



LED	Anzeige	Status
1	Laufwerksstatus/-Fehler	<ul style="list-style-type: none"> • Blau (fest): Laufwerk ist online • Gelb (blinkend): Laufwerksausfall • Aus: Steckplatz ist leer

LED	Anzeige	Status
2	Laufwerk aktiv	Blau (blinkend): Auf das Laufwerk wird zugegriffen

Richten Sie die Hardware ein

Hardware einrichten: Übersicht

Nachdem Sie die Appliance mit Strom versorgt haben, konfigurieren Sie die Netzwerkverbindungen, die von StorageGRID verwendet werden.

Konfigurieren Sie die erforderlichen Netzwerkverbindungen

Bei allen Appliances führen Sie mehrere Aufgaben zur Konfiguration erforderlicher Netzwerkverbindungen aus, z. B.:

- Greifen Sie auf den Appliance Installer zu
- Netzwerkverbindungen konfigurieren
- Überprüfen Sie Netzwerkverbindungen auf Portebene

Zusätzliche Konfiguration, die möglicherweise erforderlich ist

Je nachdem, welche Gerätetypen Sie konfigurieren, ist möglicherweise eine zusätzliche Hardwarekonfiguration erforderlich.

SANtricity System Manager

Für SG6000 und SG5700 konfigurieren Sie SANtricity System Manager. Die SANtricity-Software wird verwendet, um die Hardware für diese Appliances zu überwachen.

BMC Schnittstelle

Die folgenden Geräte verfügen über eine BMC-Schnittstelle, die konfiguriert werden muss:

- SGF6112
- SG6000
- SG1000
- SG100

Optionale Konfiguration

- Storage Appliances
 - Konfigurieren Sie SANtricity System Manager (SG6000 und SG5700) für die Hardware-Überwachung
 - Ändern Sie den RAID-Modus
- Service-Appliances
 - Greifen Sie auf die BMC-Schnittstelle für den SG100 und SG1000 sowie den SG6000-CN-Controller zu

Konfigurieren Sie StorageGRID-Verbindungen

Rufen Sie das Installationsprogramm für StorageGRID-Appliances auf

Sie müssen auf das Installationsprogramm der StorageGRID Appliance zugreifen, um die Installationsversion zu überprüfen und die Verbindungen zwischen der Appliance und den drei StorageGRID-Netzwerken zu konfigurieren: Das Grid-Netzwerk, das Admin-Netzwerk (optional) und das Client-Netzwerk (optional).

Bevor Sie beginnen

- Sie verwenden einen beliebigen Management-Client, der eine Verbindung zum StorageGRID-Admin-Netzwerk herstellen kann, oder Sie haben einen Service-Laptop.
- Der Client- oder Service-Laptop verfügt über einen "[Unterstützter Webbrowser](#)".
- Der Service Appliance oder Storage Appliance Controller ist mit allen geplanten StorageGRID-Netzwerken verbunden.
- Sie kennen die IP-Adresse, das Gateway und das Subnetz für die Service-Appliance oder den Storage-Appliance-Controller in diesen Netzwerken.
- Sie haben die geplanten Netzwerk-Switches konfiguriert.

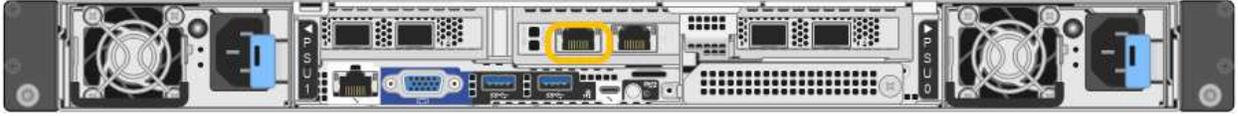
Über diese Aufgabe

Für den ersten Zugriff auf das Installationsprogramm der StorageGRID-Appliance können Sie die DHCP-zugewiesene IP-Adresse für den Port des Admin-Netzwerks auf der Services-Appliance oder dem Controller der Storage-Appliance verwenden (vorausgesetzt, es ist mit dem Admin-Netzwerk verbunden). Alternativ können Sie einen Service-Laptop direkt an die Service-Appliance oder den Controller der Storage-Appliance anschließen.

Schritte

1. Verwenden Sie, falls möglich, die DHCP-Adresse für den Admin-Netzwerk-Port auf der Service-Appliance oder dem Controller der Storage-Appliance. Der Admin-Netzwerkanschluss ist in der folgenden Abbildung hervorgehoben. (Verwenden Sie die IP-Adresse im Grid-Netzwerk, wenn das Admin-Netzwerk nicht verbunden ist.)

SGF6112



SG6000-CN



E5700SG

Beim E5700SG haben Sie folgende Möglichkeiten:

- Sehen Sie sich das Sieben-Segment-Display auf dem E5700SG-Controller an. Wenn Management-Port 1 und 10/25-GbE-Ports 2 und 4 auf dem E5700SG-Controller mit Netzwerken mit DHCP-Servern verbunden sind, versucht der Controller, beim Einschalten des Gehäuses dynamisch zugewiesene IP-Adressen zu erhalten. Nachdem der Controller den Einschaltvorgang abgeschlossen hat, zeigt sein 7-Segment-Display **HO** an, gefolgt von einer sich wiederholenden Sequenz von zwei Zahlen.

```
HO -- IP address for Admin Network -- IP address for Grid Network  
HO
```

In der Reihenfolge:

- Der erste Zahlensatz ist die DHCP-Adresse für den Appliance-Speicherknoten im Admin-Netzwerk, sofern er verbunden ist. Diese IP-Adresse ist dem Management-Port 1 des E5700SG-Controllers zugewiesen.
- Der zweite Zahlensatz ist die DHCP-Adresse für den Appliance-Speicherknoten im Grid-Netzwerk. Diese IP-Adresse wird 10/25-GbE-Ports 2 und 4 zugewiesen, wenn Sie das Gerät zum ersten Mal mit Strom versorgen.



Wenn eine IP-Adresse nicht über DHCP zugewiesen werden konnte, wird 0.0.0.0 angezeigt.

SG100



SG1000



a. Suchen Sie das MAC-Adressenetikett auf der Vorderseite der Service Appliance oder Speicher-

Appliance, und bestimmen Sie die MAC-Adresse für den Admin-Netzwerk-Port.

Auf dem MAC-Adressenetikett wird die MAC-Adresse für den BMC-Verwaltungsport aufgelistet.

Um die MAC-Adresse für den Admin-Netzwerk-Port zu ermitteln, fügen Sie **2** zur Hexadezimalzahl auf dem Etikett hinzu. Wenn die MAC-Adresse auf dem Etikett beispielsweise mit **09** endet, endet die MAC-Adresse für den Admin-Port in **0B**. Wenn die MAC-Adresse auf dem Etikett mit **(y)FF** endet, endet die MAC-Adresse für den Admin-Port in **(y+1)01**. Sie können diese Berechnung einfach durchführen, indem Sie den Rechner unter Windows öffnen, ihn auf den Programmiermodus setzen, Hex auswählen, die MAC-Adresse eingeben und dann **+ 2 =** eingeben.

b. Geben Sie die MAC-Adresse an Ihren Netzwerkadministrator an, damit er die DHCP-Adresse für die Appliance im Admin-Netzwerk nachsuchen kann.

c. Geben Sie auf dem Client diese URL für den StorageGRID-Appliance-Installer ein:

`https://Appliance_IP:8443`

Für ``Appliance_IP`` Verwenden Sie die DHCP-Adresse (verwenden Sie die IP-Adresse für das Admin-Netzwerk, wenn Sie diese haben).

d. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, zeigen Sie das Zertifikat mithilfe des Browser-Installationsassistenten an und installieren Sie es.

Die Meldung wird beim nächsten Zugriff auf diese URL nicht angezeigt.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt. Die Informationen und Meldungen, die beim ersten Zugriff auf diese Seite angezeigt werden, hängen davon ab, wie Ihr Gerät derzeit mit StorageGRID-Netzwerken verbunden ist. Möglicherweise werden Fehlermeldungen angezeigt, die in späteren Schritten gelöst werden.

[Home](#)[Configure Networking ▾](#)[Configure Hardware ▾](#)[Monitor Installation](#)[Advanced ▾](#)

Home

i The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type

Storage ▾

Node name

MM-2-108-SGA-lab25

Cancel

Save

Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

172.16.1.178

Connection state

Connection to 172.16.1.178 ready

Cancel

Save

Installation

Current state

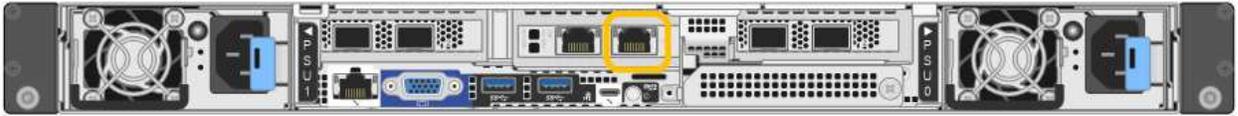
Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

[Start Installation](#)

2. Wenn Sie keine IP-Adresse über DHCP erhalten können, können Sie eine Link-Local-Verbindung verwenden.

SGF6112

Schließen Sie einen Service-Laptop mithilfe eines Ethernet-Kabels direkt an den ganz rechts am RJ-45-Port der Appliance an.



SG6000-CN

Schließen Sie einen Service-Laptop mithilfe eines Ethernet-Kabels direkt an den rechtesten RJ-45-Anschluss des SG6000-CN Controllers an.



E5700SG

Verbinden Sie den Service-Laptop über ein Ethernet-Kabel mit dem Management-Port 2 des E5700SG Controllers.



SG100

Schließen Sie einen Service-Laptop mithilfe eines Ethernet-Kabels direkt an den rechtesten RJ-45-Port des Services-Geräts an.



SG1000

Schließen Sie einen Service-Laptop mithilfe eines Ethernet-Kabels direkt an den rechtesten RJ-45-Port des Services-Geräts an.



- a. Öffnen Sie einen Webbrowser auf dem Service-Laptop.
- b. Geben Sie diese URL für das StorageGRID-Appliance-Installationsprogramm ein:
https://169.254.0.1:8443

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt. Die Informationen und Meldungen, die beim ersten Zugriff auf diese Seite angezeigt werden, hängen davon ab, wie Ihr Gerät derzeit mit StorageGRID-Netzwerken verbunden ist. Möglicherweise werden Fehlermeldungen

angezeigt, die in späteren Schritten gelöst werden.



Wenn Sie über eine Link-Local-Verbindung nicht auf die Startseite zugreifen können, konfigurieren Sie die Service-Laptop-IP-Adresse als 169.254.0.2, Und versuchen Sie es erneut.

Nachdem Sie fertig sind

Nach dem Zugriff auf das Installationsprogramm der StorageGRID-Appliance:

- Überprüfen Sie, ob die Installationsversion der StorageGRID Appliance auf der Appliance mit der auf dem StorageGRID-System installierten Softwareversion übereinstimmt. Aktualisieren Sie gegebenenfalls das Installationsprogramm für StorageGRID-Appliances.

["Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance"](#)

- Überprüfen Sie alle Meldungen, die auf der Startseite des StorageGRID-Appliance-Installationsprogramms angezeigt werden, und konfigurieren Sie die Linkkonfiguration und die IP-Konfiguration nach Bedarf.

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking | Configure Hardware | Monitor Installation | Advanced

Home

This Node

Node type: Gateway

Node name: xlr-10

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery:

Primary Admin Node IP: 192.168.7.44

Connection state: Connection to 192.168.7.44 ready

Cancel Save

Installation

Current state: Ready to start installation of xlr-10 into grid with Admin Node 192.168.7.44 running StorageGRID 11.6.0, using StorageGRID software downloaded from the Admin Node.

Start installation

Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance

Die Installationsversion der StorageGRID Appliance auf der Appliance muss mit der auf dem StorageGRID-System installierten Softwareversion übereinstimmen, um sicherzustellen, dass alle StorageGRID-Funktionen unterstützt werden.

Bevor Sie beginnen

Sie haben auf das Installationsprogramm für StorageGRID-Geräte zugegriffen.

Über diese Aufgabe

StorageGRID-Appliances werden ab Werk mit dem StorageGRID-Appliance-Installationsprogramm vorinstalliert. Wenn Sie einem kürzlich aktualisierten StorageGRID-System eine Appliance hinzufügen, müssen Sie möglicherweise das Installationsprogramm für StorageGRID-Appliances manuell aktualisieren, bevor Sie die Appliance als neuen Node installieren.

Das Installationsprogramm von StorageGRID Appliance wird automatisch aktualisiert, wenn Sie auf eine neue StorageGRID-Version aktualisieren. Sie müssen den StorageGRID-Appliance-Installer nicht auf installierten Appliance-Knoten aktualisieren. Diese Vorgehensweise ist nur erforderlich, wenn Sie eine Appliance installieren, die eine frühere Version des Installationsprogramms für StorageGRID-Geräte enthält.

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Firmware aktualisieren** aus.
2. Vergleichen Sie die aktuelle Firmware-Version mit der auf Ihrem StorageGRID System installierten Softwareversion. (Wählen Sie oben im Grid Manager das Hilfesymbol aus, und wählen Sie **über**.)

Die zweite Ziffer in den beiden Versionen sollte übereinstimmen. Wenn auf Ihrem StorageGRID-System beispielsweise die Version 11.6.x.y ausgeführt wird, sollte die StorageGRID Appliance Installer-Version 3.6.z sein.

3. Wenn die Appliance über eine heruntergeebene Version des Installationsprogramms für StorageGRID-Geräte verfügt, fahren Sie mit fort "[NetApp Downloads mit StorageGRID Appliance](#)".

Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.

4. Laden Sie die entsprechende Version der **Support-Datei für StorageGRID-Geräte** und der entsprechenden Prüfsummendatei herunter.

Die Support-Datei für StorageGRID Appliances ist eine .zip Archiv, das die aktuellen und früheren Firmware-Versionen für alle StorageGRID Appliance-Modelle enthält.

Nachdem Sie die Support-Datei für StorageGRID Appliances heruntergeladen haben, extrahieren Sie die .zip Archivieren Sie die README-Datei, und lesen Sie sie, um wichtige Informationen zur Installation des StorageGRID-Appliance-Installationsprogramms zu erhalten.

5. Befolgen Sie die Anweisungen auf der Seite Firmware aktualisieren Ihres StorageGRID-Appliance-Installationsprogramms, um die folgenden Schritte auszuführen:
 - a. Laden Sie die entsprechende Support-Datei (Firmware-Image) für Ihren Controller-Typ hoch. Einige Firmware-Versionen erfordern auch das Hochladen einer Prüfsummendatei. Wenn Sie zur Eingabe einer Prüfsummendatei aufgefordert werden, finden Sie diese auch in der Support-Datei für StorageGRID-Appliances.
 - b. Aktualisieren Sie die inaktive Partition.

- c. Starten Sie neu und tauschen Sie die Partitionen aus.
- d. Laden Sie die entsprechende Support-Datei (Firmware-Image) erneut für Ihren Controller-Typ hoch. Einige Firmware-Versionen erfordern auch das Hochladen einer Prüfsummendatei. Wenn Sie zur Eingabe einer Prüfsummendatei aufgefordert werden, finden Sie diese auch in der Support-Datei für StorageGRID-Appliances.
- e. Aktualisieren Sie die zweite (inaktive) Partition.

Verwandte Informationen

["Zugriff auf das Installationsprogramm der StorageGRID Appliance"](#)

Netzwerkverbindungen konfigurieren

Sie können Netzwerkverbindungen für die Ports konfigurieren, die zum Verbinden der Appliance mit dem Grid-Netzwerk, dem Client-Netzwerk und dem Admin-Netzwerk verwendet werden. Sie können die Verbindungsgeschwindigkeit sowie den Port- und Netzwerk-Bond-Modus einstellen.



Wenn Sie ConfigBuilder zum Generieren einer JSON-Datei verwenden, können Sie die Netzwerkverbindungen automatisch konfigurieren. Siehe ["Automatisierung der Appliance-Installation und -Konfiguration"](#).

Bevor Sie beginnen

- Das ist schon ["Zusätzliche Ausrüstung erhalten"](#) Erforderlich für Ihren Kabeltyp und die Verbindungsgeschwindigkeit.
- Sie haben die richtigen Transceiver in den Ports installiert, basierend auf der Verbindungsgeschwindigkeit, die Sie verwenden möchten.
- Sie haben die Netzwerk-Ports mit Switches verbunden, die Ihre gewählte Geschwindigkeit unterstützen.

Wenn Sie den aggregierten Port Bond-Modus, den LACP Network Bond-Modus oder VLAN-Tagging verwenden möchten:

- Sie haben die Netzwerk-Ports an der Appliance mit Switches verbunden, die VLAN und LACP unterstützen.
- Wenn mehrere Switches an der LACP-Verbindung beteiligt sind, unterstützen die Switches MLAG (Multi-Chassis Link Aggregation Groups) oder eine vergleichbare Position.
- Sie wissen, wie Sie die Switches für die Verwendung von VLAN, LACP und MLAG oder Ähnliches konfigurieren.
- Sie kennen das eindeutige VLAN-Tag, das für jedes Netzwerk verwendet werden soll. Dieses VLAN-Tag wird zu jedem Netzwerkpaket hinzugefügt, um sicherzustellen, dass der Netzwerkverkehr an das richtige Netzwerk weitergeleitet wird.

Über diese Aufgabe

Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-StandardEinstellung verwenden möchten.



Die LACP Übertragungs-Hash-Richtlinie ist layer2+3.

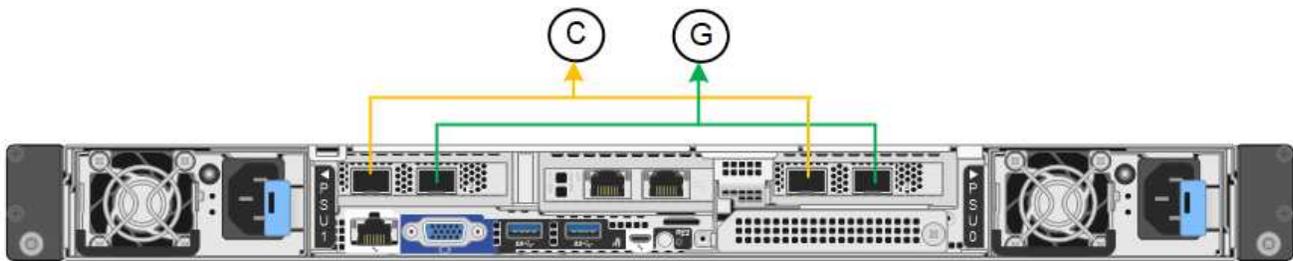
Die Abbildungen und Tabellen fassen die Optionen für den Port Bond-Modus und den Network Bond-Modus für jede Appliance zusammen. Weitere Informationen finden Sie im Folgenden:

- "Port-Bond-Modi (SGF6112)"
- "Port-Bond-Modi (SG6000-CN)"
- "Port-Bond-Modi (E5700SG)"
- "Port-Bond-Modi (SG1000 und SG100)"

SGF6112

Bond-Modus mit festem Port (Standard)

Die Abbildung zeigt, wie die vier Netzwerk-Ports im Bond-Modus mit festen Ports verbunden sind (Standardkonfiguration).



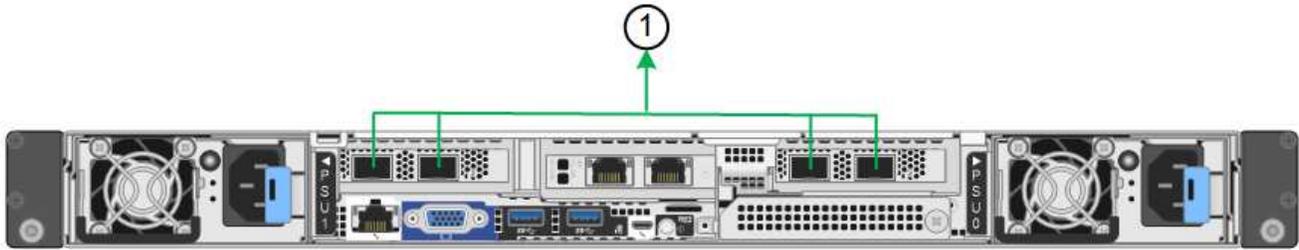
Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

In der Tabelle sind die Optionen für die Konfiguration der Netzwerkports zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Aktiv/Backup (Standard)	<ul style="list-style-type: none"> Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. Die Ports 1 und 3 werden nicht verwendet. Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. Die Ports 1 und 3 verwenden eine aktiv-Backup-Verbindung für das Client-Netzwerk. VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.
LACP (802.3ad)	<ul style="list-style-type: none"> Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. Die Ports 1 und 3 werden nicht verwendet. Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. Die Ports 1 und 3 verwenden eine LACP Bond für das Client-Netzwerk. VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.

Bond-Modus für aggregierten Ports

Die Abbildung zeigt, wie die vier Netzwerk-Ports im aggregierten Port-Bond-Modus verbunden sind.



Legende	Welche Ports sind verbunden
1	Alle vier Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Traffic verwendet werden können.

In der Tabelle sind die Optionen für die Konfiguration der Netzwerkports zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad)	<ul style="list-style-type: none"> Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete. 	<ul style="list-style-type: none"> Die Ports 1-4 verwenden eine einzelne LACP-Verbindung für das Grid-Netzwerk und das Client-Netzwerk. Zwei VLAN-Tags ermöglichen die Trennung von Grid-Netzwerkpaketen von Client-Netzwerkpaketen.

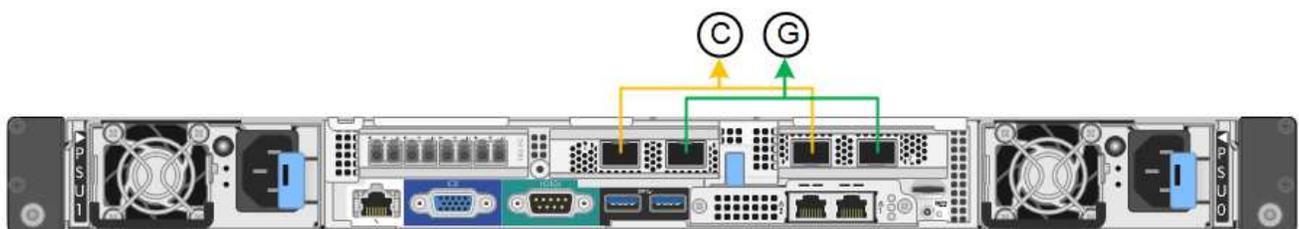
Active-Backup Netzwerk-Bond-Modus für Management-Ports

Diese Abbildung zeigt, wie die beiden 1-GbE-Management-Ports auf dem SGF6112 im Active-Backup-Netzwerk-Bond-Modus für das Admin-Netzwerk verbunden sind.

SG6000

Bond-Modus mit festem Port (Standard)

Diese Abbildung zeigt, wie die vier Netzwerk-Ports im Bond-Modus mit festen Ports verbunden sind (Standardkonfiguration).



Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

In der Tabelle sind die Optionen für die Konfiguration der Netzwerkports zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Aktiv/Backup (Standard)	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. • Die Ports 1 und 3 werden nicht verwendet. • Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. • Die Ports 1 und 3 verwenden eine aktiv-Backup-Verbindung für das Client-Netzwerk. • VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.
LACP (802.3ad)	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. • Die Ports 1 und 3 werden nicht verwendet. • Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. • Die Ports 1 und 3 verwenden eine LACP Bond für das Client-Netzwerk. • VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.

Bond-Modus für aggregierten Ports

Die Abbildung zeigt, wie die vier Netzwerk-Ports im Bond-Modus für aggregierte Ports verbunden sind.

Legende	Welche Ports sind verbunden
1	Alle vier Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Traffic verwendet werden können.

In der Tabelle sind die Optionen für die Konfiguration der Netzwerkports zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad)	<ul style="list-style-type: none"> Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete. 	<ul style="list-style-type: none"> Die Ports 1-4 verwenden eine einzelne LACP-Verbindung für das Grid-Netzwerk und das Client-Netzwerk. Zwei VLAN-Tags ermöglichen die Trennung von Grid-Netzwerkpaketen von Client-Netzwerkpaketen.

Active-Backup Netzwerk-Bond-Modus für Management-Ports

Diese Abbildung zeigt, wie die beiden 1-GbE-Management-Ports des SG6000-CN-Controllers im Active-Backup-Netzwerk-Bond-Modus des Admin-Netzwerks verbunden sind.



SG5700

Bond-Modus mit festem Port (Standard)

Die Abbildung zeigt, wie die vier 10/25-GbE-Ports im Bond-Modus mit festen Ports (Standardkonfiguration) verbunden sind.

Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

In der Tabelle sind die Optionen für die Konfiguration der vier 10/25-GbE-Ports zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Aktiv/Backup (Standard)	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. • Die Ports 1 und 3 werden nicht verwendet. • Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. • Die Ports 1 und 3 verwenden eine aktiv-Backup-Verbindung für das Client-Netzwerk. • VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.
LACP (802.3ad)	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. • Die Ports 1 und 3 werden nicht verwendet. • Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. • Die Ports 1 und 3 verwenden eine LACP Bond für das Client-Netzwerk. • VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.

Bond-Modus für aggregierten Ports

Diese Abbildung zeigt, wie die vier 10/25-GbE-Ports im Bond-Modus für aggregierte Ports verbunden sind.

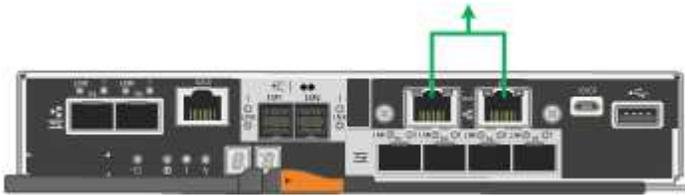
Legende	Welche Ports sind verbunden
1	Alle vier Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Traffic verwendet werden können.

In der Tabelle sind die Optionen für die Konfiguration der vier 10/25-GbE-Ports zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad)	<ul style="list-style-type: none"> • Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. • Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete. 	<ul style="list-style-type: none"> • Die Ports 1-4 verwenden eine einzelne LACP-Verbindung für das Grid-Netzwerk und das Client-Netzwerk. • Zwei VLAN-Tags ermöglichen die Trennung von Grid-Netzwerkpaketen von Client-Netzwerkpaketen.

Active-Backup Netzwerk-Bond-Modus für Management-Ports

Diese Abbildung zeigt, wie die zwei 1-GbE-Management-Ports auf dem E5700SG Controller im Active-Backup-Netzwerk-Bond-Modus für das Admin-Netzwerk verbunden sind.

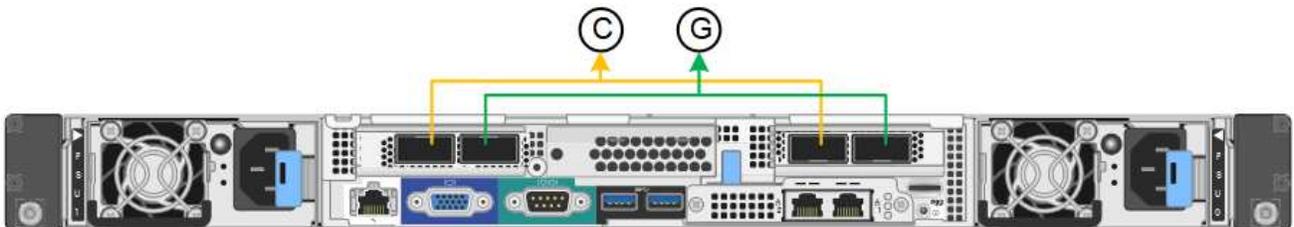


SG100 und SG1000

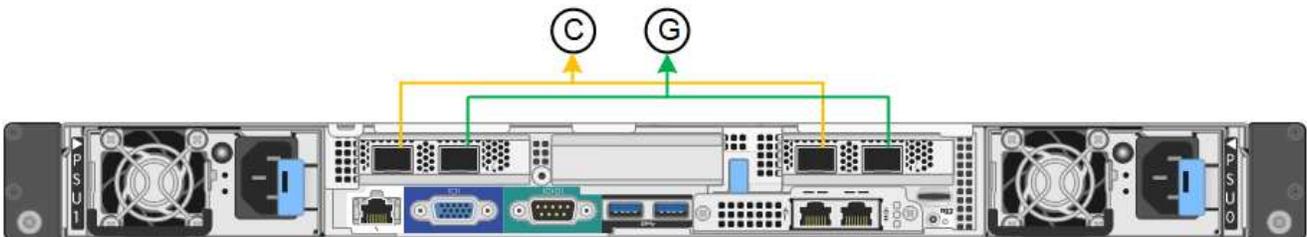
Bond-Modus mit festem Port (Standard)

Die Abbildungen zeigen, wie die vier Netzwerk-Ports des SG1000 oder SG100 im Fixed Port Bond-Modus (Standardkonfiguration) verbunden sind.

SG1000:



SG100:



Legende	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

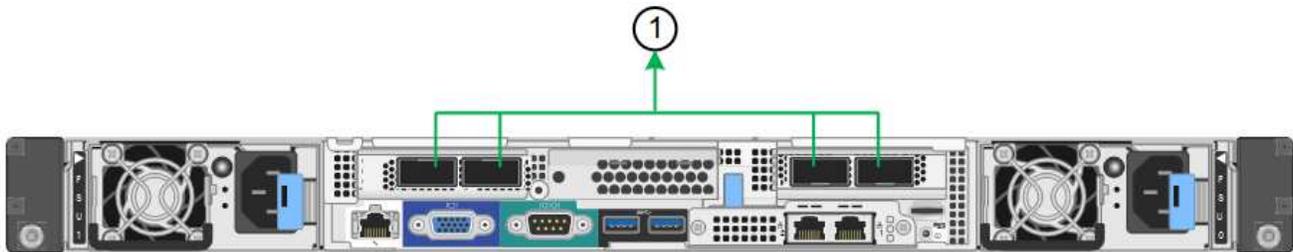
In der Tabelle sind die Optionen für die Konfiguration der vier Netzwerkanschlüsse zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Aktiv/Backup (Standard)	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. • Die Ports 1 und 3 werden nicht verwendet. • Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine aktiv-Backup-Verbindung für das Grid Network. • Die Ports 1 und 3 verwenden eine aktiv-Backup-Verbindung für das Client-Netzwerk. • VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.
LACP (802.3ad)	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. • Die Ports 1 und 3 werden nicht verwendet. • Ein VLAN-Tag ist optional. 	<ul style="list-style-type: none"> • Die Ports 2 und 4 verwenden eine LACP-Verbindung für das Grid-Netzwerk. • Die Ports 1 und 3 verwenden eine LACP Bond für das Client-Netzwerk. • VLAN-Tags können für beide Netzwerke festgelegt werden, damit der Netzwerkadministrator dies tun kann.

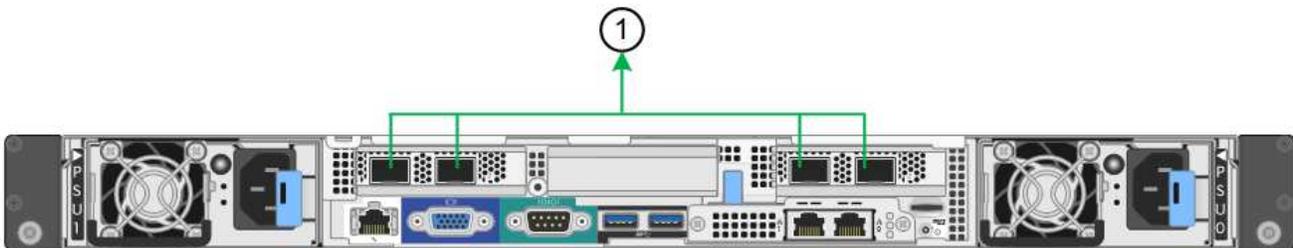
Bond-Modus für aggregierten Ports

Diese Abbildungen zeigen, wie die vier Netzwerk-Ports im aggregierten Port Bond-Modus verbunden sind.

SG1000:



SG100:



Legende	Welche Ports sind verbunden
1	Alle vier Ports werden in einer einzelnen LACP Bond gruppiert, sodass alle Ports für den Grid-Netzwerk- und Client-Netzwerk-Traffic verwendet werden können.

In der Tabelle sind die Optionen für die Konfiguration der vier Netzwerkanschlüsse zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standard-einstellung verwenden möchten.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad)	<ul style="list-style-type: none"> Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete. 	<ul style="list-style-type: none"> Die Ports 1-4 verwenden eine einzelne LACP-Verbindung für das Grid-Netzwerk und das Client-Netzwerk. Zwei VLAN-Tags ermöglichen die Trennung von Grid-Netzwerkpaketen von Client-Netzwerkpaketen.

Active-Backup Netzwerk-Bond-Modus für Management-Ports

Diese Abbildungen zeigen, wie die beiden 1-GbE-Management-Ports auf den Appliances im Active-Backup-Netzwerk-Bond-Modus für das Admin-Netzwerk verbunden sind.

SG1000:



SG100:



Schritte

1. Klicken Sie in der Menüleiste des StorageGRID-Appliance-Installationsprogramms auf **Netzwerke konfigurieren > Link-Konfiguration**.

Auf der Seite Network Link Configuration wird ein Diagramm der Appliance angezeigt, in dem die Netzwerk- und Verwaltungsports nummeriert sind.

In der Tabelle Verbindungsstatus werden der Verbindungsstatus, die Verbindungsgeschwindigkeit und andere Statistiken der nummerierten Ports aufgeführt.

Das erste Mal, wenn Sie diese Seite aufrufen:

- **Verbindungsgeschwindigkeit** ist auf **Auto** eingestellt.
- **Port Bond Modus** ist auf **fest** eingestellt.
- **Network Bond Mode** ist für das Grid Network auf **Active-Backup** eingestellt.
- Das **Admin-Netzwerk** ist aktiviert, und der Netzwerk-Bond-Modus ist auf **unabhängig** eingestellt.
- Das **Client-Netzwerk** ist deaktiviert.

2. Wählen Sie die Verbindungsgeschwindigkeit für die Netzwerkanschlüsse aus der Dropdown-Liste **Link Speed** aus.

Die Netzwerk-Switches, die Sie für das Grid-Netzwerk und das Client-Netzwerk verwenden, müssen ebenfalls für diese Geschwindigkeit konfiguriert sein. Für die konfigurierte Verbindungsgeschwindigkeit müssen Sie die entsprechenden Adapter oder Transceiver verwenden. Verwenden Sie die automatische Verbindungsgeschwindigkeit, wenn möglich, da diese Option sowohl die Verbindungsgeschwindigkeit als auch den FEC-Modus (Forward Error Correction) mit dem Link-Partner verhandelt.

Wenn Sie die 25-GbE-Verbindungsgeschwindigkeit für die SG6000- oder SG5700-Netzwerkports verwenden möchten:

- Verwenden Sie SFP28 Transceiver und SFP28 Twinax-Kabel oder optische Kabel.
- Wählen Sie für den SG6000 aus der Dropdown-Liste **Verbindungsgeschwindigkeit** die Option **Auto** aus.
- Wählen Sie für den SG5700 **25GbE** aus der Dropdown-Liste **Link Speed** aus.

3. Aktivieren oder deaktivieren Sie die StorageGRID-Netzwerke, die Sie verwenden möchten.

Das Grid-Netzwerk ist erforderlich. Dieses Netzwerk kann nicht deaktiviert werden.

- a. Wenn das Gerät nicht mit dem Admin-Netzwerk verbunden ist, deaktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Admin-Netzwerk.
- b. Wenn das Gerät mit dem Client-Netzwerk verbunden ist, aktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Client-Netzwerk.

Die Client-Netzwerkeinstellungen für die Daten-NIC-Ports werden nun angezeigt.

4. In der Tabelle finden Sie Informationen zum Konfigurieren des Port-Bond-Modus und des Netzwerk-Bond-Modus.

Dieses Beispiel zeigt:

- **Aggregate** und **LACP** ausgewählt für das Grid und die Client Netzwerke. Sie müssen für jedes Netzwerk ein eindeutiges VLAN-Tag angeben. Sie können Werte zwischen 0 und 4095 auswählen.
- **Active-Backup** für das Admin-Netzwerk ausgewählt.

Link Settings

Link speed

Port bond mode Fixed Aggregate

Choose Fixed port bond mode if you want to use ports 2 and 4 for the Grid Network and ports 1 and 3 for the Client Network (if enabled). Choose Aggregate port bond mode if you want all connected ports to share a single LACP bond for both the Grid and Client Networks.

Grid Network

Enable network

Network bond mode Active-Backup LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Admin Network

Enable network

Network bond mode Independent Active-Backup

Connect the Admin Network to ports 5 and 6. If necessary, you can make a temporary direct Ethernet connection by disconnecting ports 5 and 6, then connecting to port 6 and using link-local IP address 169.254.0.1 for access.

MAC Addresses d8:c4:97:2a:e4:95

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Client Network

Enable network

Network bond mode Active-Backup LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

5. Wenn Sie mit Ihrer Auswahl zufrieden sind, klicken Sie auf **Speichern**.



Wenn Sie Änderungen am Netzwerk oder an der Verbindung vorgenommen haben, über die Sie verbunden sind, können Sie die Verbindung verlieren. Wenn die Verbindung nicht innerhalb von 1 Minute wiederhergestellt wird, geben Sie die URL für den StorageGRID-Appliance-Installer erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:

`https://appliance_IP:8443`

Konfigurieren Sie StorageGRID-IP-Adressen

Sie verwenden das Installationsprogramm der StorageGRID-Appliance, um die IP-Adressen und Routinginformationen zu konfigurieren, die für die Service-Appliance oder den Speicher-Node der Appliance im StorageGRID-Grid-, Administrator- und Client-Netzwerk verwendet werden.

Wenn Sie mit ConfigBuilder eine JSON-Datei erstellen, können Sie IP-Adressen automatisch konfigurieren. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

Über diese Aufgabe

Sie müssen entweder auf jedem verbundenen Netzwerk eine statische IP-Adresse für das Gerät zuweisen oder einen permanenten Leasing für die Adresse des DHCP-Servers zuweisen.

Informationen zum Ändern der Verbindungskonfiguration finden Sie in den folgenden Anweisungen:

- "[Ändern der Link-Konfiguration der SGF6112-Appliance](#)"
- "[Ändern Sie die Verbindungskonfiguration des SG6000-CN Controllers](#)"
- "[Ändern Sie die Link-Konfiguration des E5700SG Controllers](#)"
- "[Ändern der Link-Konfiguration der Service-Appliance SG100 oder SG1000](#)"

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren > IP-Konfiguration** aus.

Die Seite IP-Konfiguration wird angezeigt.

2. Um das Grid-Netzwerk zu konfigurieren, wählen Sie entweder **statisch** oder **DHCP** im Abschnitt **Grid Network** der Seite aus.
3. Wenn Sie **statisch** ausgewählt haben, führen Sie die folgenden Schritte aus, um das Grid-Netzwerk zu konfigurieren:
 - a. Geben Sie die statische IPv4-Adresse unter Verwendung von CIDR-Notation ein.
 - b. Geben Sie das Gateway ein.

Wenn Ihr Netzwerk kein Gateway aufweist, geben Sie die gleiche statische IPv4-Adresse erneut ein.

- c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.



Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.

d. Klicken Sie Auf **Speichern**.

Wenn Sie die IP-Adresse ändern, können sich auch das Gateway und die Liste der Subnetze ändern.

Wenn die Verbindung zum Installationsprogramm für StorageGRID-Geräte unterbrochen wird, geben Sie die URL mithilfe der neuen statischen IP-Adresse, die Sie gerade zugewiesen haben, erneut ein.
Beispiel:

https://appliance_IP:8443

e. Bestätigen Sie, dass die Liste der Grid Network Subnets korrekt ist.

Wenn Sie Grid-Subnetze haben, ist das Grid-Netzwerk-Gateway erforderlich. Alle angegebenen Grid-Subnetze müssen über dieses Gateway erreichbar sein. Diese Grid-Netzwerknetze müssen beim Starten der StorageGRID-Installation auch in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert werden.



Die Standardroute wird nicht aufgeführt. Wenn das Client-Netzwerk nicht aktiviert ist, verwendet die Standardroute das Grid-Netzwerk-Gateway.

- Um ein Subnetz hinzuzufügen, klicken Sie auf das Insert-Symbol **+** Rechts neben dem letzten Eintrag.
- Um ein nicht verwendetes Subnetz zu entfernen, klicken Sie auf das Löschesymbol **x**.

f. Klicken Sie Auf **Speichern**.

4. Wenn Sie **DHCP** ausgewählt haben, führen Sie die folgenden Schritte aus, um das Grid-Netzwerk zu konfigurieren:

a. Nachdem Sie das Optionsfeld **DHCP** aktiviert haben, klicken Sie auf **Speichern**.

Die Felder **IPv4 Address**, **Gateway** und **Subnets** werden automatisch ausgefüllt. Wenn der DHCP-Server so konfiguriert ist, dass er einen MTU-Wert zuweist, wird das Feld **MTU** mit diesem Wert ausgefüllt, und das Feld ist schreibgeschützt.

Ihr Webbrowser wird automatisch an die neue IP-Adresse für das StorageGRID-Appliance-Installationsprogramm umgeleitet.

b. Bestätigen Sie, dass die Liste der Grid Network Subnets korrekt ist.

Wenn Sie Grid-Subnetze haben, ist das Grid-Netzwerk-Gateway erforderlich. Alle angegebenen Grid-Subnetze müssen über dieses Gateway erreichbar sein. Diese Grid-Netzwerknetze müssen beim Starten der StorageGRID-Installation auch in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert werden.



Die Standardroute wird nicht aufgeführt. Wenn das Client-Netzwerk nicht aktiviert ist, verwendet die Standardroute das Grid-Netzwerk-Gateway.

- Um ein Subnetz hinzuzufügen, klicken Sie auf das Insert-Symbol **+** Rechts neben dem letzten

Eintrag.

- Um ein nicht verwendetes Subnetz zu entfernen, klicken Sie auf das Löschsymbol ✕.
- c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.



Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.

a. Klicken Sie Auf **Speichern**.

5. Um das Admin-Netzwerk zu konfigurieren, wählen Sie im Abschnitt **Admin-Netzwerk** der Seite entweder **statisch** oder **DHCP** aus.



Um das Admin-Netzwerk zu konfigurieren, aktivieren Sie das Admin-Netzwerk auf der Seite Verbindungskonfiguration.

Admin Network

The Admin Network is a closed network used for system administration and maintenance. The Admin Network is typically a private network and does not need to be routable between sites.

IP Assignment Static DHCP

IPv4 Address (CIDR)

Gateway

Subnets (CIDR) **+**

MTU

6. Wenn Sie **statisch** ausgewählt haben, führen Sie die folgenden Schritte aus, um das Admin-Netzwerk zu konfigurieren:

a. Geben Sie die statische IPv4-Adresse mit CIDR-Schreibweise für Management-Port 1 auf dem Gerät

ein.

Management-Port 1 befindet sich links von den beiden 1-GbE-RJ45-Ports am rechten Ende der Appliance.

b. Geben Sie das Gateway ein.

Wenn Ihr Netzwerk kein Gateway aufweist, geben Sie die gleiche statische IPv4-Adresse erneut ein.

c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

d. Klicken Sie Auf **Speichern**.

Wenn Sie die IP-Adresse ändern, können sich auch das Gateway und die Liste der Subnetze ändern.

Wenn die Verbindung zum Installationsprogramm für StorageGRID-Geräte unterbrochen wird, geben Sie die URL mithilfe der neuen statischen IP-Adresse, die Sie gerade zugewiesen haben, erneut ein.
Beispiel:

https://appliance:8443

e. Bestätigen Sie, dass die Liste der Admin-Netzwerk-Subnetze korrekt ist.

Sie müssen überprüfen, ob alle Subnetze über das von Ihnen angegebene Gateway erreicht werden können.



Die Standardroute kann nicht für die Verwendung des Admin-Netzwerk-Gateways erstellt werden.

- Um ein Subnetz hinzuzufügen, klicken Sie auf das Insert-Symbol **+** Rechts neben dem letzten Eintrag.
- Um ein nicht verwendetes Subnetz zu entfernen, klicken Sie auf das Löschesymbol **x**.

f. Klicken Sie Auf **Speichern**.

7. Wenn Sie **DHCP** ausgewählt haben, führen Sie die folgenden Schritte aus, um das Admin-Netzwerk zu konfigurieren:

a. Nachdem Sie das Optionsfeld **DHCP** aktiviert haben, klicken Sie auf **Speichern**.

Die Felder **IPv4 Address**, **Gateway** und **Subnets** werden automatisch ausgefüllt. Wenn der DHCP-Server so konfiguriert ist, dass er einen MTU-Wert zuweist, wird das Feld **MTU** mit diesem Wert ausgefüllt, und das Feld ist schreibgeschützt.

Ihr Webbrowser wird automatisch an die neue IP-Adresse für das StorageGRID-Appliance-Installationsprogramm umgeleitet.

b. Bestätigen Sie, dass die Liste der Admin-Netzwerk-Subnetze korrekt ist.

Sie müssen überprüfen, ob alle Subnetze über das von Ihnen angegebene Gateway erreicht werden können.



Die Standardroute kann nicht für die Verwendung des Admin-Netzwerk-Gateways erstellt werden.

- Um ein Subnetz hinzuzufügen, klicken Sie auf das Insert-Symbol **+** Rechts neben dem letzten Eintrag.
- Um ein nicht verwendetes Subnetz zu entfernen, klicken Sie auf das Löschsymbol **x**.

c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

d. Klicken Sie Auf **Speichern**.

8. Um das Client-Netzwerk zu konfigurieren, wählen Sie entweder **statisch** oder **DHCP** im Abschnitt **Client-Netzwerk** der Seite aus.



Um das Client-Netzwerk zu konfigurieren, aktivieren Sie das Client-Netzwerk auf der Seite Verbindungskonfiguration.

Client Network

The Client Network is an open network used to provide access to client applications, including S3 and Swift. The Client Network enables grid nodes to communicate with any subnet reachable through the Client Network gateway. The Client Network does not become operational until you complete the StorageGRID configuration steps.

IP Assignment Static DHCP

IPv4 Address (CIDR)

Gateway

MTU

9. Wenn Sie **statisch** ausgewählt haben, führen Sie die folgenden Schritte aus, um das Client-Netzwerk zu konfigurieren:

- a. Geben Sie die statische IPv4-Adresse unter Verwendung von CIDR-Notation ein.
- b. Klicken Sie Auf **Speichern**.

c. Vergewissern Sie sich, dass die IP-Adresse für das Client-Netzwerk-Gateway korrekt ist.



Wenn das Client-Netzwerk aktiviert ist, wird die Standardroute angezeigt. Die Standardroute verwendet das Client-Netzwerk-Gateway und kann nicht auf eine andere Schnittstelle verschoben werden, während das Client-Netzwerk aktiviert ist.

d. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

e. Klicken Sie Auf **Speichern**.

10. Wenn Sie **DHCP** ausgewählt haben, führen Sie die folgenden Schritte aus, um das Client-Netzwerk zu konfigurieren:

a. Nachdem Sie das Optionsfeld **DHCP** aktiviert haben, klicken Sie auf **Speichern**.

Die Felder **IPv4 Address** und **Gateway** werden automatisch ausgefüllt. Wenn der DHCP-Server so konfiguriert ist, dass er einen MTU-Wert zuweist, wird das Feld **MTU** mit diesem Wert ausgefüllt, und das Feld ist schreibgeschützt.

Ihr Webbrowser wird automatisch an die neue IP-Adresse für das StorageGRID-Appliance-Installationsprogramm umgeleitet.

a. Vergewissern Sie sich, dass das Gateway korrekt ist.



Wenn das Client-Netzwerk aktiviert ist, wird die Standardroute angezeigt. Die Standardroute verwendet das Client-Netzwerk-Gateway und kann nicht auf eine andere Schnittstelle verschoben werden, während das Client-Netzwerk aktiviert ist.

b. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

Netzwerkverbindungen prüfen

Vergewissern Sie sich, dass Sie über die Appliance auf die StorageGRID-Netzwerke zugreifen können, die Sie verwenden. Um das Routing über Netzwerk-Gateways zu validieren, sollten Sie die Verbindung zwischen dem StorageGRID Appliance Installer und den IP-Adressen in verschiedenen Subnetzen testen. Sie können auch die MTU-Einstellung überprüfen.

Schritte

1. Klicken Sie in der Menüleiste des StorageGRID-Appliance-Installationsprogramms auf **Netzwerke konfigurieren > Ping und MTU-Test**.

Die Seite Ping und MTU Test wird angezeigt.

Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

Ping and MTU Test

Network	<input type="text" value="Grid"/>
Destination IPv4 Address or FQDN	<input type="text"/>
Test MTU	<input type="checkbox"/>
<input type="button" value="Test Connectivity"/>	

2. Wählen Sie aus dem Dropdown-Feld **Netzwerk** das Netzwerk aus, das Sie testen möchten: Grid, Admin oder Client.
3. Geben Sie die IPv4-Adresse oder den vollqualifizierten Domännennamen (FQDN) für einen Host in diesem Netzwerk ein.

Beispielsweise möchten Sie das Gateway im Netzwerk oder den primären Admin-Node pingen.

4. Aktivieren Sie optional das Kontrollkästchen **MTU testen**, um die MTU-Einstellung für den gesamten Pfad durch das Netzwerk zum Ziel zu überprüfen.

Sie können beispielsweise den Pfad zwischen dem Appliance-Node und einem Node an einem anderen Standort testen.

5. Klicken Sie Auf **Konnektivität Testen**.

Wenn die Netzwerkverbindung gültig ist, wird die Meldung „Ping Test bestanden“ angezeigt, wobei die Ausgabe des Ping-Befehls aufgelistet ist.

Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

Ping and MTU Test

Network	Grid	▼
Destination IPv4 Address or FQDN	10.96.104.223	
Test MTU	<input checked="" type="checkbox"/>	
Test Connectivity		

Ping test passed

Ping command output

```
PING 10.96.104.223 (10.96.104.223) 1472(1500) bytes of data.  
1480 bytes from 10.96.104.223: icmp_seq=1 ttl=64 time=0.318 ms  
  
--- 10.96.104.223 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.318/0.318/0.318/0.000 ms  
  
Found MTU 1500 for 10.96.104.223 via br0
```

Verwandte Informationen

- ["Netzwerkverbindungen konfigurieren"](#)
- ["MTU-Einstellung ändern"](#)

Überprüfen Sie Netzwerkverbindungen auf Portebene

Damit der Zugriff zwischen dem Installationsprogramm der StorageGRID Appliance und anderen Nodes nicht durch Firewalls beeinträchtigt wird, vergewissern Sie sich, dass der Installer von StorageGRID eine Verbindung zu einem bestimmten TCP-Port oder einem Satz von Ports an der angegebenen IP-Adresse oder dem angegebenen Adressbereich herstellen kann.

Über diese Aufgabe

Mithilfe der Liste der im StorageGRID-Appliance-Installationsprogramm bereitgestellten Ports können Sie die Verbindung zwischen der Appliance und den anderen Nodes im Grid-Netzwerk testen.

Darüber hinaus können Sie die Konnektivität auf den Admin- und Client-Netzwerken sowie auf UDP-Ports testen, wie sie für externe NFS- oder DNS-Server verwendet werden. Eine Liste dieser Ports finden Sie im ["Netzwerkportreferenz"](#).



Die in der Tabelle für die Portkonnektivität aufgeführten Netznetzwerkports sind nur für StorageGRID Version 11.7 gültig. Um zu überprüfen, welche Ports für jeden Node-Typ korrekt sind, sollten Sie immer die Netzwerkrichtlinien für Ihre Version von StorageGRID lesen.

Schritte

1. Klicken Sie im Installationsprogramm der StorageGRID-Appliance auf **Netzwerke konfigurieren > Port Connectivity Test (nmap)**.

Die Seite Port Connectivity Test wird angezeigt.

In der Tabelle für die Portkonnektivität werden Node-Typen aufgeführt, für die im Grid-Netzwerk TCP-Konnektivität erforderlich ist. Für jeden Node-Typ werden in der Tabelle die Grid-Netzwerkanschlüsse aufgeführt, auf die Ihre Appliance Zugriff haben sollte.

Sie können die Verbindung zwischen den in der Tabelle aufgeführten Appliance-Ports und den anderen Nodes im Grid-Netzwerk testen.

2. Wählen Sie im Dropdown-Menü **Netzwerk** das Netzwerk aus, das Sie testen möchten: **Grid**, **Admin** oder **Client**.
3. Geben Sie einen Bereich von IPv4-Adressen für die Hosts in diesem Netzwerk an.

Beispielsweise möchten Sie das Gateway im Netzwerk oder den primären Admin-Node aufsuchen.

Geben Sie einen Bereich mit einem Bindestrich an, wie im Beispiel gezeigt.

4. Geben Sie eine TCP-Portnummer, eine Liste von Ports, die durch Kommas getrennt sind, oder eine Reihe von Ports ein.

Port Connectivity Test

Network	<input type="text" value="Grid"/>
IPv4 Address Ranges	<input type="text" value="10.224.6.160-161"/>
Port Ranges	<input type="text" value="22,2022"/>
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
	<input type="button" value="Test Connectivity"/>

5. Klicken Sie Auf **Konnektivität Testen**.
 - Wenn die ausgewählten Netzwerkverbindungen auf Portebene gültig sind, wird die Meldung „Verbindungstest bestanden“ in einem grünen Banner angezeigt. Die Ausgabe des nmap-Befehls ist unter dem Banner aufgeführt.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- Wenn eine Netzwerkverbindung auf Portebene zum Remote-Host hergestellt wird, der Host jedoch nicht auf einem oder mehreren der ausgewählten Ports hört, wird die Meldung „Verbindungstest fehlgeschlagen“ in einem gelben Banner angezeigt. Die Ausgabe des nmap-Befehls ist unter dem Banner aufgeführt.

Jeder Remote-Port, auf den der Host nicht hört, hat den Status „Geschlossen“. Beispielsweise sieht dieses gelbe Banner, wenn der Node, zu dem eine Verbindung hergestellt werden soll, bereits installiert ist und der StorageGRID-NMS-Service auf diesem Node noch nicht ausgeführt wird.

🚩 Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
1504/tcp  closed evb-elm
1505/tcp  open  funkproxy
1506/tcp  open  utcd
1508/tcp  open  diagmond
7443/tcp  open  oracleas-https
9999/tcp  open  abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- Wenn für einen oder mehrere ausgewählte Ports keine Netzwerkverbindung auf Portebene hergestellt werden kann, wird die Meldung „Verbindungstest für Port fehlgeschlagen“ in einem roten Banner angezeigt. Die Ausgabe des nmap-Befehls ist unter dem Banner aufgeführt.

Das rote Banner zeigt an, dass eine TCP-Verbindung zu einem Port auf dem Remote-Host hergestellt wurde, aber dem Sender wurde nichts zurückgegeben. Wenn keine Antwort zurückgegeben wird, hat der Port einen Status „gefiltert“ und wird wahrscheinlich durch eine Firewall blockiert.



Ports mit „closed“ werden ebenfalls aufgeführt.

❗ Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
79/tcp    filtered finger
80/tcp    open  http
443/tcp   open  https
1504/tcp  closed evb-elm
1505/tcp  open  funkproxy
1506/tcp  open  utcd
1508/tcp  open  diagmond
7443/tcp  open  oracleas-https
9999/tcp  open  abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

Konfiguration von SANtricity System Manager (SG6000 und SG5700)

Mit SANtricity System Manager lässt sich der Status von Storage Controllern, Storage-Festplatten und anderen Hardwarekomponenten im Storage Controller-Shelf überwachen. Sie können außerdem einen Proxy für AutoSupport der E-Series konfigurieren, mit dem Sie AutoSupport Meldungen von der Appliance senden können, ohne den Managementport zu verwenden.

Einrichten und Zugreifen auf SANtricity System Manager

Sie müssen möglicherweise auf SANtricity System Manager auf dem Storage Controller zugreifen, um die Hardware im Storage Controller Shelf zu überwachen oder um E-Series AutoSupport zu konfigurieren.

Bevor Sie beginnen

- Sie verwenden ein ["Unterstützter Webbrowser"](#).
- Für den Zugriff auf den SANtricity System Manager über den Grid-Manager haben Sie StorageGRID installiert, und Sie verfügen über die Berechtigung zum Administrator der Storage-Appliance oder zum Root-Zugriff.
- Um über das Installationsprogramm für das StorageGRID-Gerät auf den SANtricity-System-Manager zuzugreifen, verfügen Sie über den Benutzernamen und das Kennwort des SANtricity-System-Managers.
- Für den direkten Zugriff auf SANtricity System Manager über einen Webbrowser verfügen Sie über den Benutzernamen und das Passwort für den SANtricity System Manager Administrator.



Sie müssen über SANtricity-Firmware 8.70 oder höher verfügen, um mithilfe des Grid-Managers oder des StorageGRID-Appliance-Installationsprogramms auf SANtricity System Manager zuzugreifen. Sie können Ihre Firmware-Version mithilfe des StorageGRID-Appliance-Installationsprogramms überprüfen und wählen **Hilfe > Info**.



Der Zugriff auf den SANtricity System Manager über den Grid Manager oder über den Appliance Installer beschränkt sich im Allgemeinen nur auf die Überwachung der Hardware und die Konfiguration von E-Series AutoSupport. Viele Funktionen und Vorgänge in SANtricity System Manager, beispielsweise ein Firmware-Upgrade, gelten nicht für die Überwachung Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Installations- und Wartungsanweisungen für Ihr Gerät.

Über diese Aufgabe

Es gibt drei Möglichkeiten, auf den SANtricity System Manager zuzugreifen, je nachdem, in welcher Phase des Installations- und Konfigurationsprozesses Sie sich befinden:

- Wenn die Appliance noch nicht als Knoten in Ihrem StorageGRID-System bereitgestellt wurde, sollten Sie die Registerkarte Erweitert im StorageGRID-Appliance-Installationsprogramm verwenden.



Sobald der Knoten bereitgestellt ist, können Sie den StorageGRID Appliance Installer zum Zugriff auf den SANtricity System Manager nicht mehr verwenden.

- Wenn die Appliance als Node in Ihrem StorageGRID-System bereitgestellt wurde, verwenden Sie die Registerkarte SANtricity System Manager auf der Seite Nodes im Grid Manager.
- Wenn Sie das Installationsprogramm oder den Grid-Manager der StorageGRID Appliance nicht verwenden können, können Sie über einen mit dem Managementport verbundenen Webbrowser direkt auf den SANtricity System Manager zugreifen.

Diese Vorgehensweise umfasst Schritte für den ersten Zugriff auf den SANtricity System Manager. Wenn Sie SANtricity System Manager bereits eingerichtet haben, fahren Sie mit fort [Schritt für die Hardware-Warnmeldungen konfigurieren](#).



Wenn Sie entweder den Grid-Manager oder den StorageGRID-Appliance-Installer verwenden, können Sie auf SANtricity System Manager zugreifen, ohne den Management-Port der Appliance konfigurieren oder verbinden zu müssen.

Mit SANtricity System Manager überwachen Sie Folgendes:

- Performance-Daten wie die Performance auf Storage-Array-Ebene, I/O-Latenz, CPU-Auslastung und Durchsatz
- Status der Hardwarekomponenten
- Unterstützung von Funktionen, einschließlich Anzeige von Diagnosedaten

Mit SANtricity System Manager können Sie die folgenden Einstellungen konfigurieren:

- E-Mail-Warnmeldungen, SNMP-Warnmeldungen oder Syslog-Warnmeldungen für die Komponenten im Storage Controller-Shelf
- AutoSupport-Einstellungen der E-Series für die Komponenten im Storage Controller Shelf

Weitere Informationen zur E-Series AutoSupport finden Sie im ["NetApp E-Series Systems Documentation Site"](#).

- Laufwerkssicherheitsschlüssel, die zum Entsperren gesicherter Laufwerke erforderlich sind (dieser Schritt ist erforderlich, wenn die Laufwerksicherheitsfunktion aktiviert ist)
- Administratorpasswort für den Zugriff auf SANtricity System Manager

Schritte

1. Führen Sie einen der folgenden Schritte aus:

- Verwenden Sie das StorageGRID-Appliance-Installationsprogramm, und wählen Sie **Erweitert > SANtricity-Systemmanager**
- Verwenden Sie den Grid-Manager und wählen Sie **NODES > aus *appliance Storage Node* > SANtricity System Manager**



Wenn diese Optionen nicht verfügbar sind oder die Anmeldeseite nicht angezeigt wird, verwenden Sie die [IP-Adressen für die Storage Controller](#). Greifen Sie auf SANtricity System Manager zu, indem Sie die Storage Controller-IP aufrufen.

2. Legen Sie das Administratorpasswort fest oder geben Sie es ein.

SANtricity System Manager verwendet ein einziges Administrator Kennwort, das von allen Benutzern verwendet wird.

Set Up SANtricity® System Manager

More (10 total) >

1 Welcome 2 Verify Hardware 3 Verify Hosts 4 Select Applications 5 Define Workloads 6 Acc...

Welcome to the SANtricity® System Manager! With System Manager, you can...

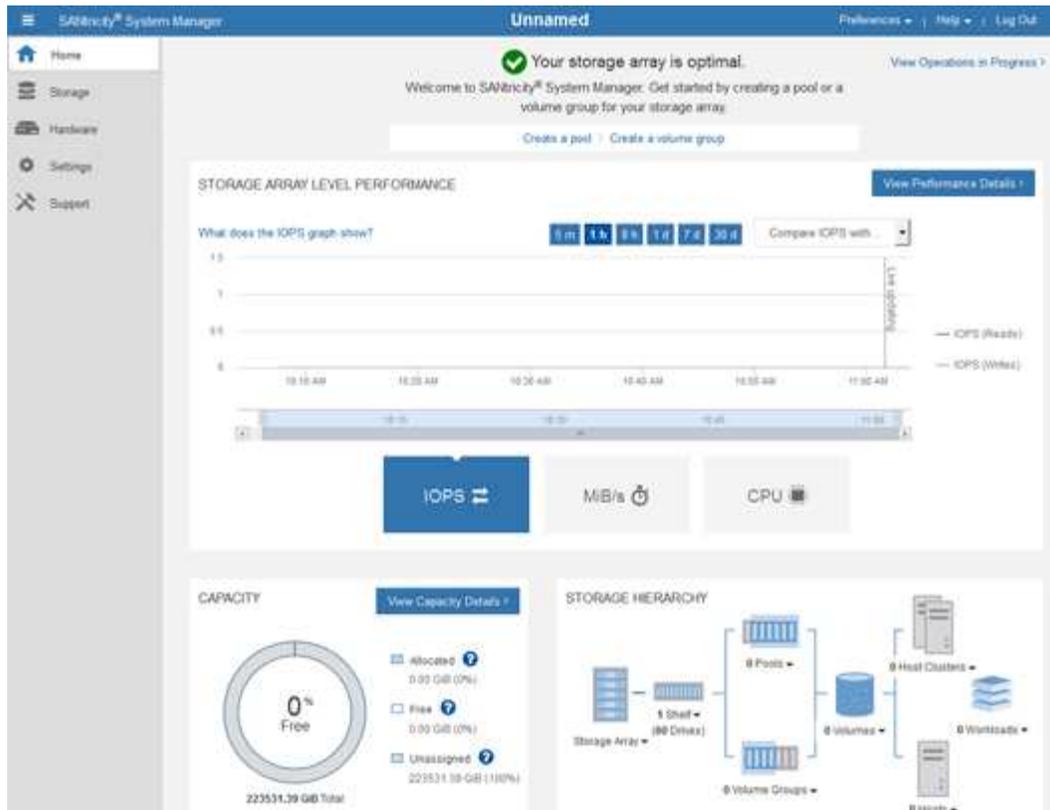
- Configure your storage array and set up alerts.
- Monitor and troubleshoot any problems when they occur.
- Keep track of how your system is performing in real time.

Cancel Next >

3. Wählen Sie **Abbrechen**, um den Assistenten zu schließen.



Schließen Sie den Einrichtungsassistenten für eine StorageGRID Appliance nicht ab.



4. Hardware-Warnmeldungen konfigurieren.
 - a. Wählen Sie **Hilfe**, um die Online-Hilfe für SANtricity System Manager zu öffnen.
 - b. Verwenden Sie den Abschnitt **Einstellungen > Alarme** der Online-Hilfe, um mehr über Warnungen zu erfahren.
 - c. Folgen Sie den Anweisungen „How to“, um E-Mail-Warnmeldungen, SNMP-Warnmeldungen oder Syslog-Warnmeldungen einzurichten.
5. Managen Sie AutoSupport für die Komponenten im Storage Controller Shelf.
 - a. Wählen Sie **Hilfe**, um die Online-Hilfe für SANtricity System Manager zu öffnen.
 - b. Im Abschnitt **SUPPORT > Support Center** der Online-Hilfe erfahren Sie mehr über die AutoSupport-Funktion.
 - c. Folgen Sie den Anweisungen „Anleitung“, um AutoSupport zu managen.

Spezielle Anweisungen zum Konfigurieren eines StorageGRID-Proxys zum Senden von E-Series AutoSupport-Meldungen ohne Verwendung des Management-Ports finden Sie unter "[Anweisungen zur Konfiguration von Speicher-Proxy-Einstellungen](#)".
6. Wenn die Laufwerkssicherheitsfunktion für die Appliance aktiviert ist, erstellen und verwalten Sie den Sicherheitsschlüssel.
 - a. Wählen Sie **Hilfe**, um die Online-Hilfe für SANtricity System Manager zu öffnen.
 - b. Verwenden Sie den Abschnitt **Einstellungen > System > Sicherheitsschlüsselverwaltung** der Online-Hilfe, um mehr über Drive Security zu erfahren.
 - c. Befolgen Sie die Anweisungen „Anleitung“, um den Sicherheitsschlüssel zu erstellen und zu verwalten.
7. Ändern Sie optional das Administratorpasswort.

- a. Wählen Sie **Hilfe**, um die Online-Hilfe für SANtricity System Manager zu öffnen.
- b. Verwenden Sie den Abschnitt **Home > Storage Array Administration** der Online-Hilfe, um mehr über das Administrator-Passwort zu erfahren.
- c. Befolgen Sie die Anweisungen „Anleitung“, um das Passwort zu ändern.

Überprüfen Sie den Hardwarestatus in SANtricity System Manager

Mit SANtricity System Manager können Sie die einzelnen Hardwarekomponenten im Storage Controller-Shelf überwachen und verwalten. Darüber hinaus werden Hardware-Diagnose- und Umgebungsinformationen, z. B. Komponententemperaturen oder Problemen mit den Laufwerken, überprüft.

Bevor Sie beginnen

- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Für den Zugriff auf den SANtricity System Manager über den Grid-Manager verfügen Sie über eine Administratorberechtigung oder Root-Zugriff der Storage-Appliance.
- Um über das Installationsprogramm für das StorageGRID-Gerät auf den SANtricity-System-Manager zuzugreifen, verfügen Sie über den Benutzernamen und das Kennwort des SANtricity-System-Managers.
- Für den direkten Zugriff auf SANtricity System Manager über einen Webbrowser verfügen Sie über den Benutzernamen und das Passwort für den SANtricity System Manager Administrator.



Sie müssen über SANtricity-Firmware 8.70 oder höher verfügen, um mithilfe des Grid-Managers oder des StorageGRID-Appliance-Installationsprogramms auf SANtricity System Manager zuzugreifen.

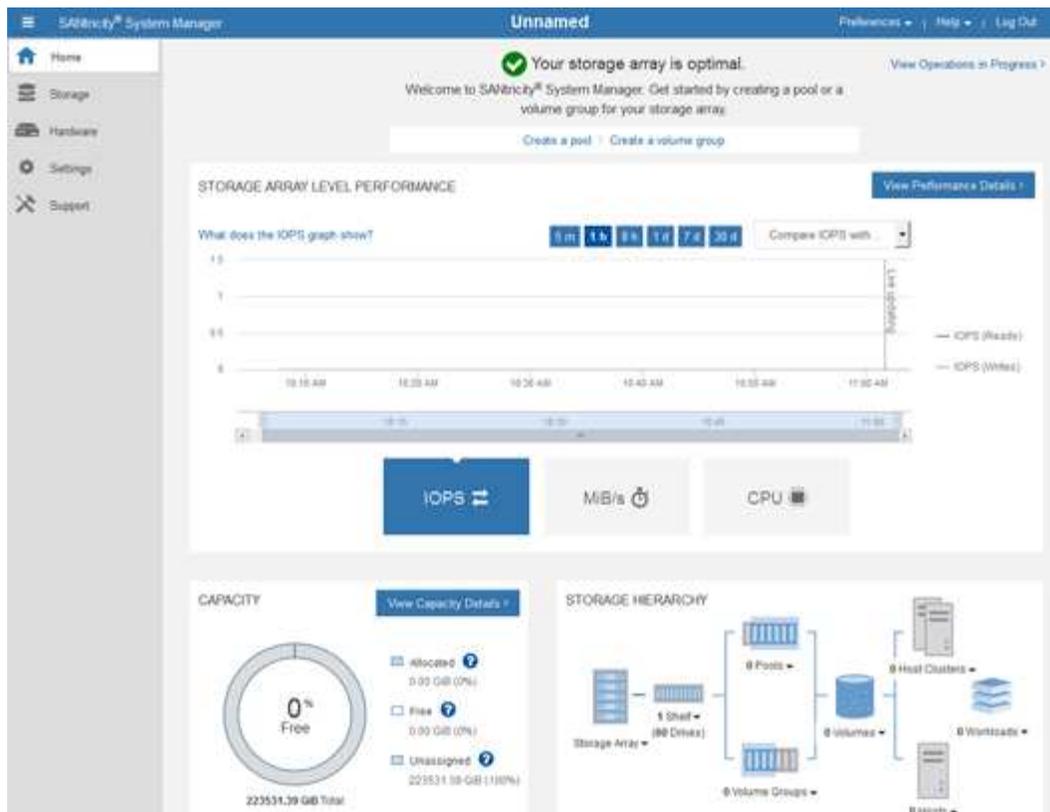


Der Zugriff auf den SANtricity System Manager über den Grid Manager oder über den Appliance Installer beschränkt sich im Allgemeinen nur auf die Überwachung der Hardware und die Konfiguration von E-Series AutoSupport. Viele Funktionen und Vorgänge in SANtricity System Manager, beispielsweise ein Firmware-Upgrade, gelten nicht für die Überwachung Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Installations- und Wartungsanweisungen für Ihr Gerät.

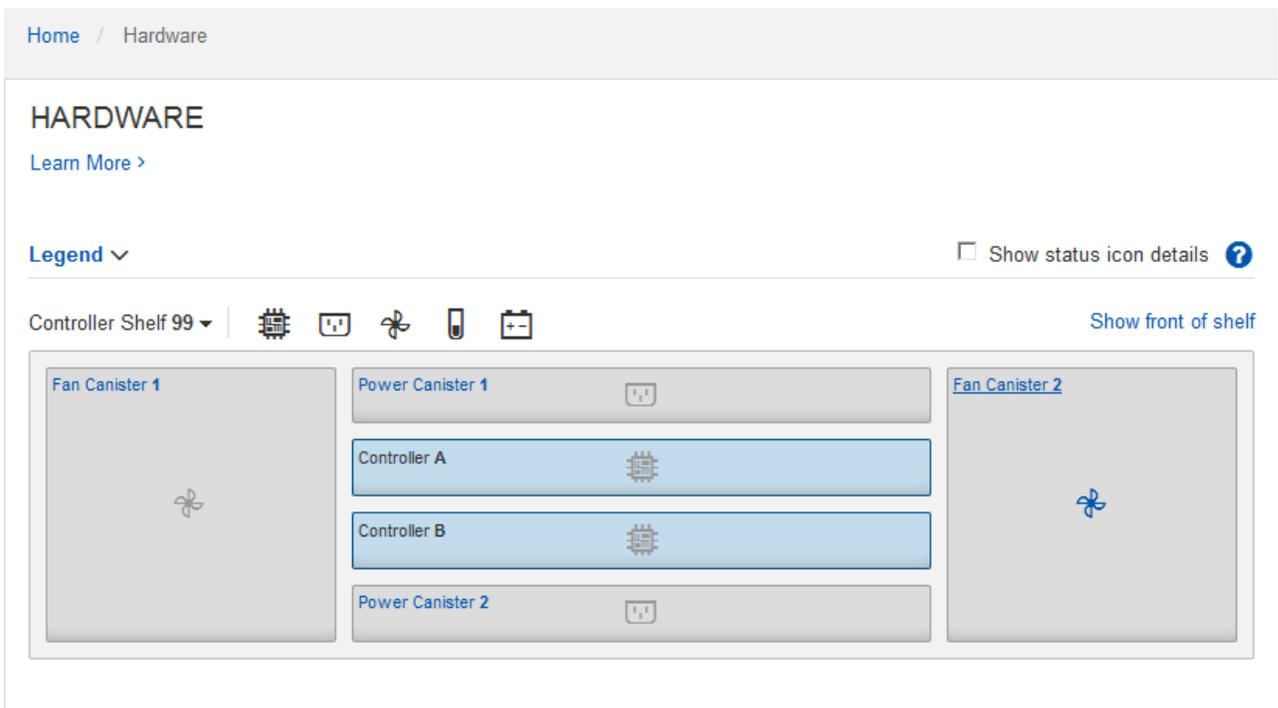
Schritte

1. [Greifen Sie auf SANtricity System Manager zu](#).
2. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des Administrators ein.
3. Klicken Sie auf **Abbrechen**, um den Einrichtungsassistenten zu schließen und die Startseite des SANtricity-System-Managers anzuzeigen.

Die Startseite von SANtricity System Manager wird angezeigt. In SANtricity System Manager wird das Controller Shelf als Storage-Array bezeichnet.



4. Überprüfen Sie die angezeigten Informationen für die Appliance-Hardware und vergewissern Sie sich, dass alle Hardwarekomponenten den Status „optimal“ aufweisen.
 - a. Klicken Sie auf die Registerkarte **Hardware**.
 - b. Klicken Sie auf **Zurück von Regal anzeigen**.



Von der Rückseite des Shelves können Sie sowohl Storage-Controller als auch den Akku in jedem Storage Controller, die beiden Power Kanister, die beiden Lüfter-Kanister und Erweiterungs-Shelves (falls vorhanden)

anzeigen. Sie können auch Komponententemperaturen anzeigen.

- a. Um die Einstellungen für jeden Speicher-Controller anzuzeigen, wählen Sie den Controller aus, und wählen Sie im Kontextmenü **Einstellungen anzeigen** aus.
- b. Um die Einstellungen für andere Komponenten auf der Rückseite des Shelf anzuzeigen, wählen Sie die Komponente aus, die Sie anzeigen möchten.
- c. Klicken Sie auf **Vorderseite des Regals**, und wählen Sie die Komponente aus, die Sie anzeigen möchten.

Von der Vorderseite des Shelves können die Laufwerke und die Laufwerksfächer für das Storage Controller-Shelf oder die Erweiterungs-Shelves (falls vorhanden) angezeigt werden.

Falls der Status einer Komponente Achtung erfordert, führen Sie die Schritte im Recovery Guru zur Lösung des Problems durch oder wenden Sie sich an den technischen Support.

Legen Sie IP-Adressen für Storage Controller mithilfe des StorageGRID Appliance Installer fest

Management-Port 1 auf jedem Storage-Controller verbindet die Appliance mit dem Managementnetzwerk für SANtricity System Manager. Wenn Sie vom Installationsprogramm der StorageGRID Appliance nicht auf den SANtricity System Manager zugreifen können, legen Sie eine statische IP-Adresse für jeden Storage Controller fest, um sicherzustellen, dass Ihre Managementverbindung zur Hardware und zur Controller-Firmware im Controller-Shelf nicht verloren geht.

Bevor Sie beginnen

- Sie verwenden einen beliebigen Management-Client, der eine Verbindung zum StorageGRID-Admin-Netzwerk herstellen kann, oder Sie haben einen Service-Laptop.
- Der Client- oder Service-Laptop verfügt über einen unterstützten Webbrowser.

Über diese Aufgabe

Adressen, die durch DHCP zugewiesen werden, können jederzeit geändert werden. Weisen Sie den Controllern statische IP-Adressen zu, um einen konsistenten Zugriff zu gewährleisten.



Befolgen Sie dieses Verfahren nur, wenn Sie keinen Zugriff auf den SANtricity-System-Manager vom Installationsprogramm der StorageGRID-Appliance (**Erweitert > SANtricity-System-Manager**) oder vom Grid-Manager (**KNOTEN > SANtricity-System-Manager**) haben.

Schritte

1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:

`https://Appliance_Controller_IP:8443`

Für *Appliance_Controller_IP*, Verwenden Sie die IP-Adresse für die Appliance in einem beliebigen StorageGRID-Netzwerk.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Hardware Konfigurieren > Storage Controller-Netzwerkconfiguration**.

Die Seite Speichercontroller-Netzwerkconfiguration wird angezeigt.

3. Wählen Sie je nach Netzwerkconfiguration **aktiviert** für IPv4, IPv6 oder beides.
4. Notieren Sie sich die automatisch angezeigte IPv4-Adresse.

DHCP ist die Standardmethode, um dem Management-Port des Storage Controllers eine IP-Adresse zuzuweisen.



Es kann einige Minuten dauern, bis die DHCP-Werte angezeigt werden.

IPv4 Address Assignment Static DHCP

IPv4 Address (CIDR)

Default Gateway

5. Legen Sie optional eine statische IP-Adresse für den Management-Port des Storage Controllers fest.



Sie sollten entweder eine statische IP für den Management-Port zuweisen oder einen permanenten Leasing für die Adresse auf dem DHCP-Server zuweisen.

- Wählen Sie **Statisch**.
- Geben Sie die IPv4-Adresse unter Verwendung der CIDR-Schreibweise ein.
- Geben Sie das Standard-Gateway ein.

IPv4 Address Assignment Static DHCP

IPv4 Address (CIDR)

Default Gateway

- Klicken Sie Auf **Speichern**.

Es kann einige Minuten dauern, bis Ihre Änderungen angewendet werden.

Wenn Sie eine Verbindung zu SANtricity System Manager herstellen, verwenden Sie die neue statische IP-Adresse als URL:

`https://Storage_Controller_IP`

Konfiguration der BMC-Schnittstelle (SGF6112, SG6000, SG100 und SG1000)

BMC-Schnittstelle: Überblick (SGF6112, SG6000, SG100 und SG1000)

Die Benutzeroberfläche des Baseboard Management Controllers (BMC) auf der SGF6112-, SG6000- oder Services-Appliance liefert Statusinformationen zur Hardware und ermöglicht Ihnen die Konfiguration von SNMP-Einstellungen und anderen Optionen für die Appliances.

Gehen Sie wie folgt vor, um den BMC bei der Installation des Geräts zu konfigurieren:

- ["Ändern Sie das Admin- oder Root-Passwort für die BMC-Schnittstelle"](#)

- "Legen Sie die IP-Adresse für den BMC-Managementport fest"
- "Greifen Sie auf die BMC-Schnittstelle zu"
- "Konfigurieren Sie die SNMP-Einstellungen"
- "E-Mail-Benachrichtigungen für BMC-Warnungen einrichten"

Wenn die Appliance bereits in einem Grid installiert wurde und StorageGRID-Software ausgeführt wird, gehen Sie wie folgt vor:



- "Stellen Sie das Gerät in den Wartungsmodus" Um auf das Installationsprogramm für die StorageGRID Appliance zuzugreifen.
- Siehe "Legen Sie die IP-Adresse für den BMC-Managementport fest" Für Informationen über den Zugriff auf die BMC-Schnittstelle mithilfe des StorageGRID-Appliance-Installationsprogramms.

Ändern Sie das Admin- oder Root-Passwort für die BMC-Schnittstelle

Aus Sicherheitsgründen müssen Sie das Kennwort für den Admin- oder Root-Benutzer des BMC ändern.

Bevor Sie beginnen

Der Management-Client verwendet ein "Unterstützter Webbrowser".

Über diese Aufgabe

Wenn Sie die Appliance zum ersten Mal installieren, verwendet der BMC ein Standardkennwort für den Admin- oder Root-Benutzer. Sie müssen das Passwort für den Administrator oder Root-Benutzer ändern, um Ihr System zu sichern.

Der Standardbenutzer hängt davon ab, wann Sie Ihre StorageGRID-Appliance installiert haben. Der Standardbenutzer ist **admin** für neue Installationen und **root** für ältere Installationen.

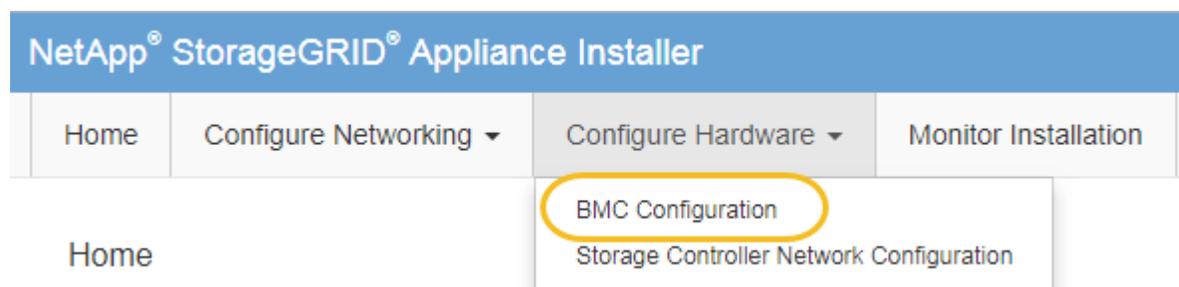
Schritte

1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:
https://Appliance_IP:8443

Für *Appliance_IP*, Verwenden Sie die IP-Adresse für die Appliance in einem beliebigen StorageGRID-Netzwerk.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Hardware konfigurieren > BMC-Konfiguration**.



Die Seite Baseboard Management Controller Configuration wird angezeigt.

3. Geben Sie in den beiden Feldern ein neues Passwort für das Admin- oder Root-Konto ein.
4. Klicken Sie Auf **Speichern**.

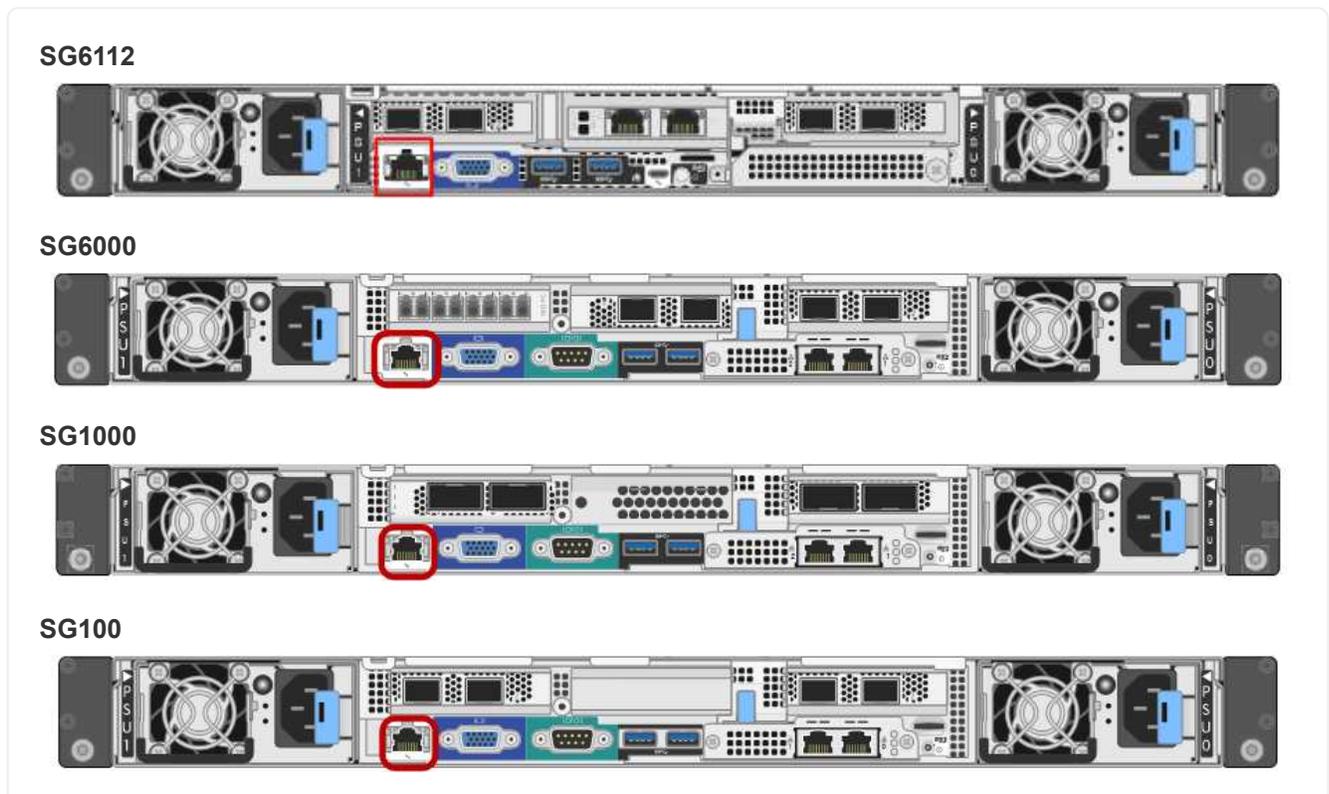
Legen Sie die IP-Adresse für den BMC-Managementport fest

Bevor Sie auf die BMC-Schnittstelle zugreifen können, konfigurieren Sie die IP-Adresse für den BMC-Verwaltungsport auf den SGF6112-, SG6000-CN-Controllern oder Service-Appliances.

Wenn Sie mit ConfigBuilder eine JSON-Datei erstellen, können Sie IP-Adressen automatisch konfigurieren. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

Bevor Sie beginnen

- Der Management-Client verwendet ein "[Unterstützter Webbrowser](#)".
- Sie verwenden jeden Management-Client, der eine Verbindung zu einem StorageGRID-Netzwerk herstellen kann.
- Der BMC-Management-Port ist mit dem Managementnetzwerk verbunden, das Sie verwenden möchten.



Über diese Aufgabe

Zu Support-Zwecken ermöglicht der BMC-Management-Port einen niedrigen Hardwarezugriff.



Sie sollten diesen Port nur mit einem sicheren, vertrauenswürdigen, internen Managementnetzwerk verbinden. Wenn kein solches Netzwerk verfügbar ist, lassen Sie den BMC-Port nicht verbunden oder blockiert, es sei denn, eine BMC-Verbindung wird vom technischen Support angefordert.

Schritte

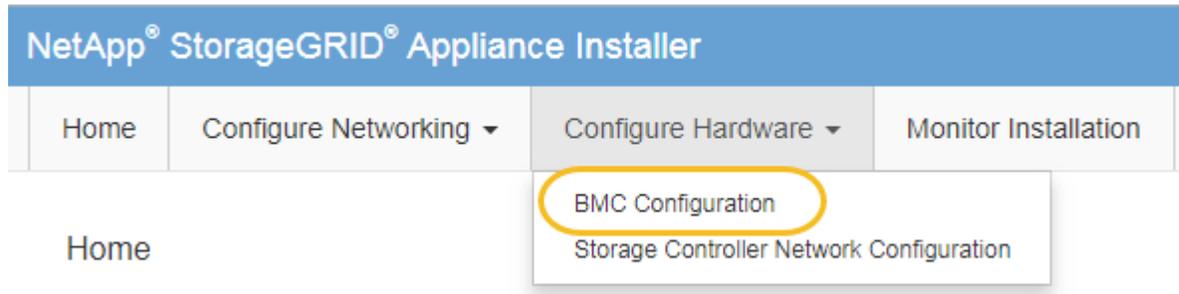
1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:

https://Appliance_IP:8443

Für `Appliance_IP`, Verwenden Sie die IP-Adresse für die Appliance in einem beliebigen StorageGRID-Netzwerk.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Hardware konfigurieren > BMC-Konfiguration**.



Die Seite Baseboard Management Controller Configuration wird angezeigt.

3. Notieren Sie sich die automatisch angezeigte IPv4-Adresse.

DHCP ist die Standardmethode zum Zuweisen einer IP-Adresse zu diesem Port.



Es kann einige Minuten dauern, bis die DHCP-Werte angezeigt werden.

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input type="radio"/> Static	<input checked="" type="radio"/> DHCP
MAC Address	<input type="text" value="d8:c4:97:28:50:62"/>	
IPv4 Address (CIDR)	<input type="text" value="10.224.3.225/21"/>	
Default gateway	<input type="text" value="10.224.0.1"/>	

4. Legen Sie optional eine statische IP-Adresse für den BMC-Verwaltungspost fest.



Sie sollten entweder eine statische IP für den BMC-Verwaltungspost zuweisen oder einen permanenten Leasing für die Adresse auf dem DHCP-Server zuweisen.

a. Wählen Sie **Statisch**.

b. Geben Sie die IPv4-Adresse unter Verwendung der CIDR-Schreibweise ein.

c. Geben Sie das Standard-Gateway ein.

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input checked="" type="radio"/> Static	<input type="radio"/> DHCP
MAC Address	<input type="text" value="d8:c4:97:28:50:62"/>	
IPv4 Address (CIDR)	<input type="text" value="10.224.3.225/21"/>	
Default gateway	<input type="text" value="10.224.0.1"/>	

d. Klicken Sie Auf **Speichern**.

Es kann einige Minuten dauern, bis Ihre Änderungen angewendet werden.

Greifen Sie auf die BMC-Schnittstelle zu

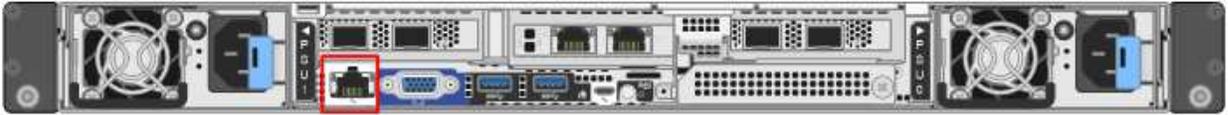
Sie können auf die BMC-Schnittstelle über die DHCP- oder statische IP-Adresse für den BMC-Verwaltungsport auf den folgenden Appliance-Modellen zugreifen:

- SGF6112
- SG6000
- SG1000
- SG100

Bevor Sie beginnen

- Der Management-Client verwendet ein "[Unterstützter Webbrowser](#)".
- Der BMC-Managementport der Appliance ist mit dem zu verwendenden Managementnetzwerk verbunden.

SGF6112



SG6000



SG1000



SG100



Schritte

1. Geben Sie die URL für die BMC-Schnittstelle ein:

`https://BMC_Port_IP`

Für `BMC_Port_IP`, Verwenden Sie die DHCP- oder statische IP-Adresse für den BMC-Management-Port.

Die BMC-Anmeldeseite wird angezeigt.



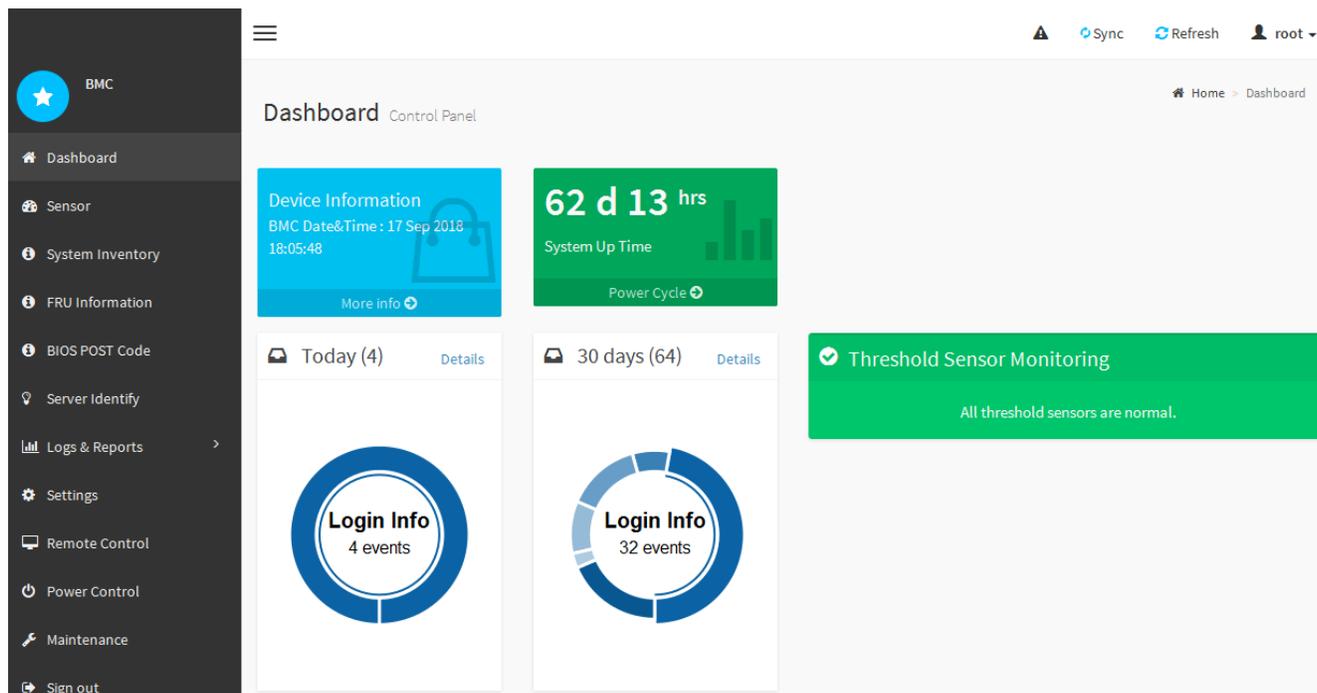
Wenn Sie noch nicht konfiguriert haben `BMC_Port_IP`, Folgen Sie den Anweisungen in "[Konfigurieren Sie die BMC-Schnittstelle](#)". Wenn Sie diese Vorgehensweise aufgrund eines Hardwareproblems nicht ausführen können und noch keine BMC-IP-Adresse konfiguriert haben, können Sie möglicherweise weiterhin auf den BMC zugreifen. Standardmäßig erhält der BMC über DHCP eine IP-Adresse. Wenn DHCP im BMC-Netzwerk aktiviert ist, kann Ihr Netzwerkadministrator die dem BMC-MAC zugewiesene IP-Adresse angeben, die auf dem Etikett auf der Vorderseite des Geräts aufgedruckt ist. Wenn DHCP im BMC-Netzwerk nicht aktiviert ist, reagiert der BMC nach einigen Minuten nicht und weist sich selbst die standardmäßige statische IP zu `192.168.0.120`. Möglicherweise müssen Sie Ihren Laptop direkt mit dem BMC-Port verbinden und die Netzwerkeinstellung ändern, um Ihrem Laptop eine IP-Adresse wie zuzuweisen `192.168.0.200/24`, Um zu suchen `192.168.0.120`.

2. Geben Sie den Admin- oder Root-Benutzernamen und das Passwort ein. Geben Sie dabei das Passwort ein, das Sie bei Ihrer Einstellung festgelegt haben "[Das Standard-Root-Passwort wurde geändert](#)":



Der Standardbenutzer hängt davon ab, wann Sie Ihre StorageGRID-Appliance installiert haben. Der Standardbenutzer ist **admin** für neue Installationen und **root** für ältere Installationen.

3. Wählen Sie **Sign me in** aus.



- Erstellen Sie optional weitere Benutzer, indem Sie **Einstellungen > Benutzerverwaltung** wählen und auf einen beliebigen Benutzer “disabled” klicken.



Wenn sich Benutzer zum ersten Mal anmelden, werden sie möglicherweise aufgefordert, ihr Passwort zu ändern, um die Sicherheit zu erhöhen.

Konfigurieren Sie die SNMP-Einstellungen für BMC

Wenn Sie mit der Konfiguration von SNMP für Hardware vertraut sind, können Sie die SNMP-Einstellungen für die SGF6112-, SG6000- und Service-Appliances über die BMC-Schnittstelle konfigurieren. Sie können sichere Community-Strings bereitstellen, SNMP-Trap aktivieren und bis zu fünf SNMP-Ziele angeben.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Sie haben Erfahrung in der Konfiguration von SNMP-Einstellungen für SNMPv1-v2c Geräte.



Die durch diese Vorgehensweise vorgenommenen BMC-Einstellungen bleiben möglicherweise nicht erhalten, wenn das Gerät ausfällt und ersetzt werden muss. Stellen Sie sicher, dass Sie über eine Aufzeichnung aller Einstellungen verfügen, die Sie angewendet haben, so dass sie nach einem Hardware-Austausch bei Bedarf leicht wieder angewendet werden können.

Schritte

1. Wählen Sie im BMC-Dashboard **Einstellungen > SNMP-Einstellungen** aus.
2. Wählen Sie auf der Seite SNMP-Einstellungen die Option **SNMP V1/V2** aktivieren und geben Sie dann eine schreibgeschützte Community-Zeichenfolge und eine Read-Write Community-Zeichenfolge an.

Die schreibgeschützte Community-Zeichenfolge ist wie eine Benutzer-ID oder ein Passwort. Sie sollten diesen Wert ändern, um zu verhindern, dass Eindringlinge Informationen über Ihr Netzwerk-Setup erhalten. Die Lese-Schreib-Community-Zeichenfolge schützt das Gerät vor nicht autorisierten Änderungen.

3. Wählen Sie optional **Trap aktivieren** aus, und geben Sie die erforderlichen Informationen ein.



Geben Sie die Ziel-IP für jeden SNMP-Trap unter Verwendung einer IP-Adresse ein. Vollständig qualifizierte Domännennamen werden nicht unterstützt.

Aktivieren Sie Traps, wenn die Appliance sofortige Benachrichtigungen an eine SNMP-Konsole senden soll, wenn sie sich in einem ungewöhnlichen Zustand befindet. Je nach Gerät können Traps auf Hardwareausfälle verschiedener Komponenten, auf Verbindungsabstände, Temperaturschwellenwerte oder hohen Datenverkehr hinweisen.

4. Klicken Sie optional auf **Test-Trap senden**, um Ihre Einstellungen zu testen.

5. Wenn die Einstellungen korrekt sind, klicken Sie auf **Speichern**.

E-Mail-Benachrichtigungen für BMC-Warnungen einrichten

Wenn Sie möchten, dass E-Mail-Benachrichtigungen bei Auftreten von Warnungen gesendet werden, verwenden Sie die BMC-Schnittstelle, um SMTP-Einstellungen, Benutzer, LAN-Ziele, Warnungsrichtlinien und Ereignisfilter zu konfigurieren.



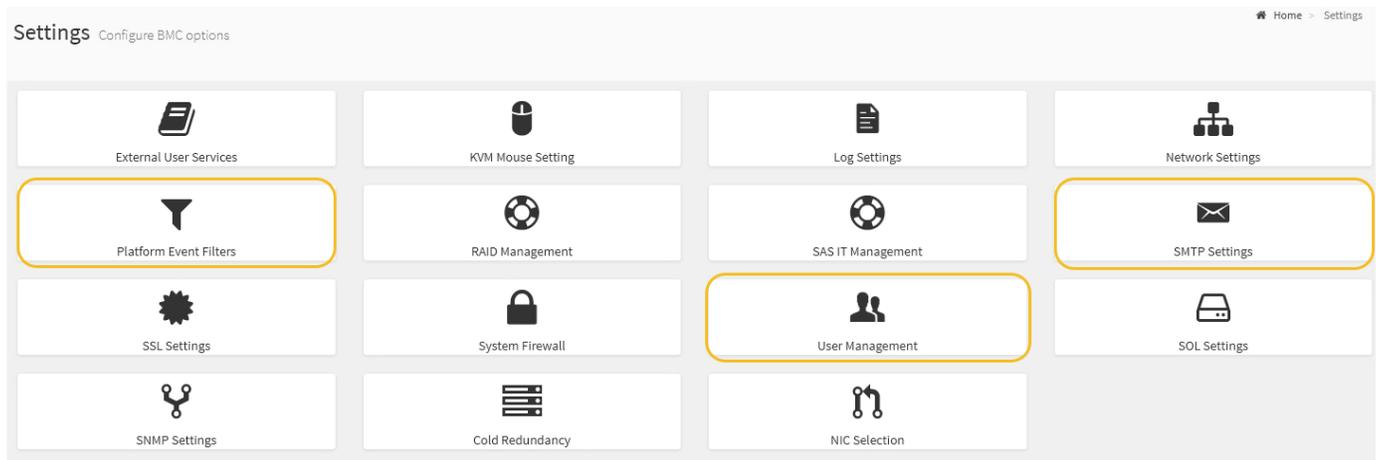
BMC-Einstellungen, die durch dieses Verfahren vorgenommen werden, bleiben möglicherweise nicht erhalten, wenn der SG6000-CN-Controller oder die Services-Appliance ausfällt und ersetzt werden muss. Stellen Sie sicher, dass Sie über eine Aufzeichnung aller Einstellungen verfügen, die Sie angewendet haben, so dass sie nach einem Hardware-Austausch bei Bedarf leicht wieder angewendet werden können.

Bevor Sie beginnen

Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.

Über diese Aufgabe

In der BMC-Schnittstelle verwenden Sie die Optionen **SMTP-Einstellungen**, **Benutzerverwaltung** und **Platform Event Filters** auf der Seite Einstellungen, um E-Mail-Benachrichtigungen zu konfigurieren.



Schritte

1. "Konfigurieren Sie die SNMP-Einstellungen für BMC".
 - a. Wählen Sie **Einstellungen > SMTP-Einstellungen**.
 - b. Geben Sie für die Absender-E-Mail-ID eine gültige E-Mail-Adresse ein.

Diese E-Mail-Adresse wird als von-Adresse angegeben, wenn der BMC E-Mail sendet.

2. Richten Sie Benutzer für den Empfang von Warnungen ein.
 - a. Wählen Sie im BMC-Dashboard die Option **Einstellungen > Benutzerverwaltung** aus.
 - b. Fügen Sie mindestens einen Benutzer hinzu, um Benachrichtigungen zu erhalten.

Die für einen Benutzer konfigurierte E-Mail-Adresse ist die Adresse, an die BMC Warnmeldungen sendet. Sie können beispielsweise einen generischen Benutzer wie „notification-user,“ hinzufügen und die E-Mail-Adresse einer E-Mail-Verteilerliste für das technische Support-Team verwenden.

3. Konfigurieren Sie das LAN-Ziel für Meldungen.
 - a. Wählen Sie **Einstellungen > Plattformereignisfilter > LAN-Ziele**.
 - b. Konfigurieren Sie mindestens ein LAN-Ziel.
 - Wählen Sie als Zieltyp **E-Mail** aus.
 - Wählen Sie für BMC-Benutzername einen Benutzernamen aus, den Sie zuvor hinzugefügt haben.
 - Wenn Sie mehrere Benutzer hinzugefügt haben und möchten, dass alle von ihnen Benachrichtigungs-E-Mails erhalten, fügen Sie für jeden Benutzer ein LAN-Ziel hinzu.
 - c. Eine Testwarnung senden.
4. Konfigurieren von Meldungsrichtlinien, um festzulegen, wann und wo BMC Alarme sendet
 - a. Wählen Sie **Einstellungen > Plattformereignisfilter > Benachrichtigungsrichtlinien** Aus.
 - b. Konfigurieren Sie mindestens eine Meldungsrichtlinie für jedes LAN-Ziel.
 - Wählen Sie für die Policengruppennummer **1** aus.
 - Wählen Sie für Policy Action * immer Warnung an dieses Ziel senden* aus.
 - Wählen Sie für LAN-Kanal **1** aus.
 - Wählen Sie in der Zielauswahl das LAN-Ziel für die Richtlinie aus.
5. Ereignisfilter konfigurieren, um Warnmeldungen für verschiedene Ereignistypen an die entsprechenden Benutzer zu leiten.
 - a. Wählen Sie **Einstellungen > Plattformereignisfilter > Ereignisfilter**.
 - b. Geben Sie für die Nummer der Meldungsrichtlinie **1** ein.
 - c. Erstellen Sie Filter für jedes Ereignis, über das die Meldungsrichtlinie-Gruppe benachrichtigt werden soll.
 - Sie können Ereignisfilter für Energieaktionen, bestimmte Sensorereignisse oder alle Ereignisse erstellen.
 - Wenn Sie unsicher sind, welche Ereignisse überwacht werden sollen, wählen Sie **Alle Sensoren** für den Sensortyp und **Alle Ereignisse** für Ereignisoptionen. Wenn Sie unerwünschte Benachrichtigungen erhalten, können Sie Ihre Auswahl später ändern.

Optional: Node-Verschlüsselung aktivieren

Wenn Sie die Node-Verschlüsselung aktivieren, können die Festplatten Ihrer Appliance durch eine sichere KMS-Verschlüsselung (Key Management Server) gegen physischen Verlust oder die Entfernung vom Standort geschützt werden. Während der Appliance-Installation müssen Sie die Node-Verschlüsselung auswählen und aktivieren. Die

Knotenverschlüsselung kann nach dem Start der KMS-Verschlüsselung nicht deaktiviert werden.

Wenn Sie ConfigBuilder zum Generieren einer JSON-Datei verwenden, können Sie die Node-Verschlüsselung automatisch aktivieren. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

Bevor Sie beginnen

Überprüfen Sie die Informationen über "[Konfigurieren von KMS](#)".

Über diese Aufgabe

Eine Appliance mit aktivierter Node-Verschlüsselung stellt eine Verbindung zum externen Verschlüsselungsmanagement-Server (KMS) her, der für den StorageGRID-Standort konfiguriert ist. Jeder KMS (oder KMS-Cluster) verwaltet die Schlüssel für alle Appliance-Nodes am Standort. Diese Schlüssel verschlüsseln und entschlüsseln die Daten auf jedem Laufwerk in einer Appliance mit aktivierter Node-Verschlüsselung.

Ein KMS kann im Grid Manager vor oder nach der Installation der Appliance in StorageGRID eingerichtet werden. Weitere Informationen zur KMS- und Appliance-Konfiguration finden Sie in den Anweisungen zur Administration von StorageGRID.

- Wenn ein KMS vor der Installation der Appliance eingerichtet wird, beginnt die KMS-kontrollierte Verschlüsselung, wenn Sie die Node-Verschlüsselung auf der Appliance aktivieren und diese zu einem StorageGRID Standort hinzufügen, an dem der KMS konfiguriert wird.
- Wenn vor der Installation der Appliance kein KMS eingerichtet wird, wird für jede Appliance, deren Node-Verschlüsselung aktiviert ist, KMS-gesteuerte Verschlüsselung durchgeführt, sobald ein KMS konfiguriert ist und für den Standort, der den Appliance-Node enthält, verfügbar ist.



Wenn eine Appliance mit aktivierter Node-Verschlüsselung installiert wird, wird ein temporärer Schlüssel zugewiesen. Die Daten auf der Appliance werden erst dann geschützt, wenn die Appliance mit dem Key Management System (KMS) verbunden und ein KMS-Sicherheitsschlüssel festgelegt ist. Siehe "[Übersicht über die KMS-Appliance-Konfiguration](#)". Finden Sie weitere Informationen.

Ohne den KMS-Schlüssel, der zur Entschlüsselung der Festplatte benötigt wird, können die Daten auf der Appliance nicht abgerufen werden und gehen effektiv verloren. Dies ist der Fall, wenn der Entschlüsselungsschlüssel nicht vom KMS abgerufen werden kann. Der Schlüssel ist nicht mehr zugänglich, wenn ein Kunde die KMS-Konfiguration löscht, ein KMS-Schlüssel abläuft, die Verbindung zum KMS verloren geht oder die Appliance aus dem StorageGRID System entfernt wird, wo die KMS-Schlüssel installiert sind.

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.

`https://Controller_IP:8443`

Controller_IP Die IP-Adresse des Compute-Controllers (nicht des Storage-Controllers) in einem der drei StorageGRID-Netzwerke.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.



Nachdem die Appliance mit einem KMS-Schlüssel verschlüsselt wurde, können die Gerätelaufwerke nicht entschlüsselt werden, ohne denselben KMS-Schlüssel zu verwenden.

2. Wählen Sie **Hardware Konfigurieren** > **Node Encryption**.

The screenshot shows the 'NetApp® StorageGRID® Appliance Installer' interface. At the top, there is a navigation bar with 'Home', 'Configure Networking', 'Configure Hardware', 'Monitor Installation', and 'Advanced'. Below this, the 'Node Encryption' section is active. It contains a warning message: 'You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.' Below the warning, there is a checkbox labeled 'Enable node encryption' which is checked. A 'Save' button is visible below the checkbox. At the bottom, the 'Key Management Server Details' section is partially visible.

3. Wählen Sie **Node-Verschlüsselung aktivieren**.

Vor der Installation der Appliance können Sie die Option **Enable Node Encryption** deaktivieren, ohne dass es zu Datenverlust kommt. Sobald die Installation beginnt, greift der Appliance-Node auf die KMS-Verschlüsselungsschlüssel im StorageGRID System zu und beginnt mit der Festplattenverschlüsselung. Sie können die Node-Verschlüsselung nicht deaktivieren, nachdem die Appliance installiert wurde.



Nachdem Sie eine Appliance mit aktivierter Knotenverschlüsselung zu einem StorageGRID-Standort mit KMS hinzugefügt haben, können Sie die KMS-Verschlüsselung für den Knoten nicht mehr verwenden.

4. Wählen Sie **Speichern**.

5. Implementieren Sie die Appliance als Node in Ihrem StorageGRID System.

DIE KMS-gesteuerte Verschlüsselung beginnt, wenn die Appliance auf die für Ihre StorageGRID Site konfigurierten KMS-Schlüssel zugreift. Das Installationsprogramm zeigt während des KMS-Verschlüsselungsprozesses Fortschrittsmeldungen an. Dies kann je nach Anzahl der Festplatten-Volumes in der Appliance einige Minuten dauern.



Die Appliances werden anfänglich mit einem zufälligen Verschlüsselungsschlüssel ohne KMS konfiguriert, der jedem Festplatten-Volume zugewiesen wird. Die Laufwerke werden mit diesem temporären Verschlüsselungsschlüssel verschlüsselt, der nicht sicher ist, bis die Appliance mit aktivierter Node-Verschlüsselung auf die KMS-Schlüssel zugreift, die für Ihre StorageGRID-Site konfiguriert wurden.

Nachdem Sie fertig sind

Wenn sich der Appliance-Node im Wartungsmodus befindet, können Sie den Verschlüsselungsstatus, die KMS-Details und die verwendeten Zertifikate anzeigen. Siehe "[Überwachung der Node-Verschlüsselung im Wartungsmodus](#)" Zur Information.

Optional: Ändern des RAID-Modus

Bei einigen Appliance-Modellen können Sie zu einem anderen RAID-Modus auf der Appliance wechseln, um Ihre Speicher- und Recovery-Anforderungen zu erfüllen. Sie

können den Modus nur ändern, bevor Sie den Appliance-Speicherknoten bereitstellen.

Wenn Sie mit ConfigBuilder eine JSON-Datei erstellen, können Sie den RAID-Modus automatisch ändern. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

Über diese Aufgabe

Wenn die Appliance unterstützt, können Sie eine der folgenden Optionen für die Volume-Konfiguration auswählen:

- **Dynamic Disk Pools (DDP)**: Dieser Modus verwendet zwei Paritätslaufwerke für je acht Datenlaufwerke. Dies ist der Standard- und empfohlene Modus für alle Appliances. Im Vergleich zu RAID 6 erzielt DDP eine bessere System-Performance, kürzere Wiederherstellungszeiten nach Laufwerksausfällen und ein vereinfachtes Management. DDP bietet auch Schutz vor Schubladenverlusten in SG5760 Appliances.



Aufgrund der beiden SSDs bietet DDP in SG6060 Appliances keinen Schubladenschutz. Der Schutz vor Schubladenverlusten ist in allen Erweiterungs-Shelfs, die zu einem SG6060 hinzugefügt werden, wirksam.

- **DDP16**: In diesem Modus werden für alle 16 Datenlaufwerke zwei Paritätslaufwerke verwendet. Dies führt im Vergleich zu DDP zu einer höheren Storage-Effizienz. Im Vergleich zu RAID 6 bietet DDP16 eine bessere Systemperformance, kürzere Wiederherstellungszeiten nach Laufwerksausfällen, benutzerfreundliches Management und vergleichbare Storage-Effizienz. Um den DDP16-Modus zu verwenden, muss Ihre Konfiguration mindestens 20 Laufwerke enthalten. DDP16 bietet keinen Schubladenschutz.
- **RAID 6**: Dieser Modus verwendet zwei Paritätslaufwerke pro 16 oder mehr Datenlaufwerken. Es handelt sich um ein Hardware-Sicherungsschema, das Paritätsstreifen auf jeder Festplatte verwendet und zwei Festplattenausfälle innerhalb des RAID-Satzes zulässt, bevor Daten verloren gehen. Für die Verwendung des RAID 6-Modus muss Ihre Konfiguration mindestens 20 Laufwerke enthalten. Obwohl RAID 6 die Storage-Effizienz der Appliance im Vergleich zu DDP steigern kann, wird dies in den meisten StorageGRID Umgebungen nicht empfohlen.



Wenn bereits Volumes konfiguriert wurden oder bereits StorageGRID installiert war, werden die Volumes durch eine Änderung des RAID-Modus entfernt und ersetzt. Alle Daten auf diesen Volumes gehen verloren.

SG6000

Bevor Sie beginnen

- Sie verwenden jeden Client, der eine Verbindung zu StorageGRID herstellen kann.
- Der Client verfügt über eine "[Unterstützter Webbrowser](#)".

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.

`https://Controller_IP:8443`

Controller_IP Die IP-Adresse des Compute-Controllers (nicht des Storage-Controllers) in einem der drei StorageGRID-Netzwerke.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Erweitert > RAID-Modus**.
3. Wählen Sie auf der Seite **RAID-Modus konfigurieren** den gewünschten RAID-Modus aus der Dropdown-Liste Modus aus.
4. Klicken Sie Auf **Speichern**.

SG5760

Bevor Sie beginnen

- Sie haben ein SG5760 mit 60 Laufwerken. Wenn SG5712 vorhanden ist, müssen Sie den DDP-Standardmodus verwenden.
- Sie verwenden jeden Client, der eine Verbindung zu StorageGRID herstellen kann.
- Der Client verfügt über eine "[Unterstützter Webbrowser](#)".

Schritte

1. Öffnen Sie mithilfe des Service-Laptops einen Webbrowser, und greifen Sie auf das Installationsprogramm der StorageGRID-Appliance: + zu

`https://E5700SG_Controller_IP:8443`

Wo *E5700SG_Controller_IP* Gibt eine der IP-Adressen für den E5700SG-Controller an.

2. Wählen Sie **Erweitert > RAID-Modus**.
3. Wählen Sie auf der Seite **RAID-Modus konfigurieren** den gewünschten RAID-Modus aus der Dropdown-Liste Modus aus.
4. Klicken Sie Auf **Speichern**.

Verwandte Informationen

["NetApp E-Series Systems Documentation Site"](#)

Optional: Netzwerkports für Appliance neu zuordnen

Optional können Sie die internen Ports auf einem Appliance-Node verschiedenen externen Ports neu zuordnen. Aufgrund eines Firewall-Problems müssen Sie

möglicherweise Ports neu zuordnen.

Bevor Sie beginnen

- Sie haben zuvor auf das Installationsprogramm für StorageGRID-Geräte zugegriffen.

Über diese Aufgabe

Für Load Balancer-Endpunkte können keine neu zugeordneten Ports verwendet werden. Wenn Sie einen neu zugeordneten Port entfernen müssen, führen Sie die Schritte unter aus "[Entfernen Sie die Port-Remaps](#)".

Schritte

1. Wählen Sie im Installationsprogramm des StorageGRID-Geräts die Option **Netzwerk konfigurieren > Ports neu zusammenfassen**.

Die Seite Remap Port wird angezeigt.

2. Wählen Sie aus dem Dropdown-Feld **Netzwerk** das Netzwerk für den Port aus, den Sie neu zuordnen möchten: Grid, Administrator oder Client.
3. Wählen Sie aus dem Dropdown-Feld **Protokoll** das IP-Protokoll TCP oder UDP aus.
4. Wählen Sie aus dem Dropdown-Feld **Remap Direction** aus, welche Verkehrsrichtung Sie für diesen Port neu zuordnen möchten: Inbound, Outbound oder Bi-direktional.
5. Geben Sie für **Original Port** die Nummer des Ports ein, den Sie neu zuordnen möchten.
6. Geben Sie für den * Port zugeordnet* die Nummer des Ports ein, den Sie stattdessen verwenden möchten.
7. Wählen Sie **Regel Hinzufügen**.

Die neue Port-Zuordnung wird der Tabelle hinzugefügt, und die erneute Zuordnung wird sofort wirksam.

8. Um eine Port-Zuordnung zu entfernen, aktivieren Sie das Optionsfeld für die Regel, die Sie entfernen möchten, und wählen Sie **Ausgewählte Regel entfernen** aus.

Implementieren des Appliance-Node

Appliance-Storage-Node implementieren

Nach der Installation und Konfiguration der Storage Appliance können Sie sie als Storage Node in einem StorageGRID System bereitstellen. Wenn Sie eine Appliance als Speicherknoten bereitstellen, verwenden Sie das StorageGRID-Appliance-Installationsprogramm, das in der Appliance enthalten ist.

Bevor Sie beginnen

- Wenn Sie einen Appliance-Node klonen, fahren Sie mit fort "[Klonen von Appliance-Nodes](#)" Prozess.
- Das Gerät wurde in einem Rack oder Schrank installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des Installationsprogramms der StorageGRID Appliance wurden Netzwerkverbindungen, IP-Adressen und (falls erforderlich) die Port-Neuzuordnung für die Appliance konfiguriert.
- Sie kennen eine der IP-Adressen, die dem Computing-Controller der Appliance zugewiesen sind. Sie können die IP-Adresse für jedes angeschlossene StorageGRID-Netzwerk verwenden.
- Der primäre Admin-Node für das StorageGRID System wurde bereitgestellt.
- Alle Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte

aufgeführt sind, wurden in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.

- Sie verfügen über einen Service-Laptop mit einem unterstützten Webbrowser.

Über diese Aufgabe

Jede Storage Appliance arbeitet als einzelner Storage-Node. Jede Appliance kann eine Verbindung zum Grid-Netzwerk, dem Admin-Netzwerk und dem Client-Netzwerk herstellen

Um einen Appliance-Speicherknoten in einem StorageGRID-System bereitzustellen, greifen Sie auf das Installationsprogramm der StorageGRID-Appliance zu und führen Sie die folgenden Schritte aus:

- Sie geben die IP-Adresse des primären Admin-Knotens und den Namen des Speicherknoten an oder bestätigen sie.
- Sie starten die Implementierung und warten, bis die Volumes konfiguriert und die Software installiert ist.
- Wenn die Installation die Installationsaufgaben der Appliance gemeinsam durchlaufen hat, setzen Sie die Installation fort, indem Sie sich beim Grid Manager anmelden, alle Grid-Nodes genehmigen und den Installations- und Implementierungsprozess von StorageGRID abschließen.



Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess mithilfe des automatisierten `configure-sga.py` Installationskript für Geräte.

- Wenn Sie eine Erweiterung oder Wiederherstellung durchführen, befolgen Sie die entsprechenden Anweisungen:
 - Informationen zum Hinzufügen eines Appliance-Storage-Knotens zu einem vorhandenen StorageGRID-System finden Sie in den Anweisungen für "[Grid-Nodes werden hinzugefügt](#)".
 - Informationen zum Bereitstellen eines Appliance Storage Node als Teil eines Wiederherstellungsvorgangs finden Sie in den Anweisungen "[Wiederherstellen eines Appliance Storage Node](#)".

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.

`https://Controller_IP:8443`

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Node name

Node name

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

- Legen Sie im Abschnitt * Primary Admin Node Connection* fest, ob Sie die IP-Adresse für den primären Admin Node angeben müssen.

Wenn Sie zuvor andere Knoten in diesem Rechenzentrum installiert haben, kann der StorageGRID-Appliance-Installer diese IP-Adresse automatisch erkennen, vorausgesetzt, dass der primäre Admin-Knoten oder mindestens ein anderer Grid-Node mit ADMIN_IP konfiguriert ist, im selben Subnetz vorhanden ist.

- Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	<ul style="list-style-type: none"> a. Deaktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie Auf Speichern. d. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.
Automatische Erkennung aller verbundenen primären Admin-Nodes	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Warten Sie, bis die Liste der erkannten IP-Adressen angezeigt wird. c. Wählen Sie den primären Admin-Node für das Grid aus, in dem dieser Appliance-Speicher-Node bereitgestellt werden soll. d. Klicken Sie Auf Speichern. e. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.

4. Geben Sie im Feld **Node Name** den Systemnamen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und klicken Sie auf **Save**.

Der Name, der hier angezeigt wird, ist der Systemname des Appliance-Node. Systemnamen sind für interne StorageGRID-Vorgänge erforderlich und können nicht geändert werden.

5. Bestätigen Sie im Abschnitt **Installation**, dass der aktuelle Status „bereit zum Starten der Installation von `node name` In das Grid mit primärem Admin-Node `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.



Wenn Sie die Storage Node-Appliance als Ziel für das Klonen von Nodes bereitstellen, beenden Sie den Bereitstellungsprozess hier, und fahren Sie mit fort "[Node-Klonen](#)".

6. Klicken Sie auf der Startseite des StorageGRID-Appliance-Installationsprogramms auf **Installation starten**.

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.



Wenn Sie manuell auf die Seite Monitor Installation zugreifen müssen, klicken Sie auf **Monitor Installation**.

7. Wenn in Ihrem Grid mehrere Speicherknoten für Geräte enthalten sind, wiederholen Sie diese Schritte für jede Appliance.



Wenn Sie mehrere Appliance Storage Nodes gleichzeitig bereitstellen müssen, können Sie den Installationsprozess mithilfe des automatisierten `configure-sga.py` Installationskript für Geräte.

Implementieren des Services-Appliance-Nodes

Sie können eine Services-Appliance als primären Admin-Node, als nicht-primärer Admin-Node oder als Gateway-Node bereitstellen. Sowohl die SG100- als auch die SG1000-Appliances können gleichzeitig als Gateway-Nodes und Admin-Nodes (primär oder nicht primär) betrieben werden.

Services-Appliance als primärer Admin-Node bereitstellen

Wenn Sie eine Services-Appliance als primären Administratorknoten bereitstellen, verwenden Sie das auf der Appliance enthaltene StorageGRID-Appliance-Installationsprogramm, um die StorageGRID-Software zu installieren, oder Sie laden die gewünschte Softwareversion hoch. Sie müssen den primären Admin-Node installieren und konfigurieren, bevor Sie andere Node-Typen installieren. Ein primärer Admin-Node kann eine Verbindung mit dem Grid-Netzwerk und dem optionalen Admin-Netzwerk und dem Client-Netzwerk herstellen, wenn ein oder beide konfiguriert sind.

Bevor Sie beginnen

- Das Gerät wurde in einem Rack oder Schrank installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des Installationsprogramms der StorageGRID Appliance wurden Netzwerkverbindungen, IP-Adressen und (falls erforderlich) die Port-Neuzuordnung für die Appliance konfiguriert.
- Sie haben einen Service-Laptop mit einem "[Unterstützter Webbrowser](#)".
- Sie kennen eine der IP-Adressen, die der Appliance zugewiesen sind. Sie können die IP-Adresse für jedes angeschlossene StorageGRID-Netzwerk verwenden.

Über diese Aufgabe

So installieren Sie StorageGRID auf einem primären Administrator-Node einer Appliance:

- Sie verwenden das Installationsprogramm für StorageGRID-Appliances, um die StorageGRID-Software zu installieren. Wenn Sie eine andere Version der Software installieren möchten, laden Sie sie zuerst mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.
- Sie warten, bis die Software installiert ist.
- Nach der Installation der Software wird die Appliance automatisch neu gestartet.

Schritte

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse für das Gerät ein.

`https://services_appliance_IP:8443`

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie im Abschnitt **dieser Knoten** die Option **Hauptadministrator** aus.
3. Geben Sie im Feld **Knotenname** den Namen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und klicken Sie auf **Speichern**.

Der Node-Name wird diesem Appliance-Node im StorageGRID-System zugewiesen. Sie wird auf der Seite

Grid Nodes im Grid Manager angezeigt.

4. Führen Sie optional folgende Schritte aus, um eine andere Version der StorageGRID-Software zu installieren:

a. Laden Sie das Installationsarchiv herunter:

["NetApp Downloads mit StorageGRID Appliance"](#)

b. Extrahieren Sie das Archiv.

c. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **StorageGRID-Software hochladen**.

d. Klicken Sie auf **Entfernen**, um das aktuelle Softwarepaket zu entfernen.

The screenshot shows the 'NetApp StorageGRID Appliance Installer' interface. At the top, there is a blue header with the title. Below the header is a navigation bar with tabs: Home, Configure Networking (dropdown), Configure Hardware (dropdown), Monitor Installation, and Advanced (dropdown). The main content area is titled 'Upload StorageGRID Software' and contains a paragraph of instructions. Below this is a section titled 'Current StorageGRID Installation Software' which displays the following information:

Version	11.3.0
Package Name	storagegrid-webscale-images-11-3-0_11.3.0-20190806.1731.4064510_amd64.deb

Below the table is a 'Remove' button.

e. Klicken Sie auf **Durchsuchen** für das Softwarepaket, das Sie heruntergeladen und extrahiert haben, und klicken Sie dann auf **Durchsuchen** für die Prüfsummendatei.

The screenshot shows the 'NetApp StorageGRID Appliance Installer' interface, similar to the previous one. The navigation bar is the same. The main content area is titled 'Upload StorageGRID Software' and contains the same instructions. Below this is a section titled 'Current StorageGRID Installation Software' which displays the following information:

Version	None
Package Name	None

Below this is a section titled 'Upload StorageGRID Installation Software' which contains two 'Browse' buttons:

Software Package	<input type="button" value="Browse"/>
Checksum File	<input type="button" value="Browse"/>

f. Wählen Sie **Home**, um zur Startseite zurückzukehren.

5. Vergewissern Sie sich, dass der aktuelle Status „bereit ist“, die Installation des primären Admin Node-Namens mit der Softwareversion x.y zu starten und dass die Schaltfläche **Installation starten** aktiviert ist.



Wenn Sie die Admin-Node-Appliance als Ziel für das Klonen von Nodes bereitstellen, beenden Sie den Bereitstellungsprozess hier, und fahren Sie mit fort "[Node-Klonen](#)".

6. Klicken Sie auf der Startseite des StorageGRID-Appliance-Installationsprogramms auf **Installation starten**.

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type: Primary Admin (with Load Balancer)

Node name: xlr8r-8

Cancel Save

Installation

Current state: Ready to start installation of xlr8r-8 as primary Admin Node of a new grid running StorageGRID 11.6.0.

Start Installation

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.



Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, klicken Sie in der Menüleiste auf **Monitor-Installation**.

Services-Appliance als Gateway oder nicht-primärer Admin-Node implementieren

Wenn Sie eine Services-Appliance als Gateway-Node oder als nicht-primärer Admin-Node bereitstellen, verwenden Sie das Installationsprogramm für StorageGRID-Appliances, das in der Appliance enthalten ist.

Bevor Sie beginnen

- Das Gerät wurde in einem Rack oder Schrank installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des Installationsprogramms der StorageGRID Appliance wurden Netzwerkverbindungen, IP-Adressen und (falls erforderlich) die Port-Neuzuordnung für die Appliance konfiguriert.
- Der primäre Admin-Node für das StorageGRID System wurde bereitgestellt.

- Alle Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte aufgeführt sind, wurden in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- Sie haben einen Service-Laptop mit einem ["Unterstützter Webbrowser"](#).
- Sie kennen die IP-Adresse, die der Appliance zugewiesen ist. Sie können die IP-Adresse für jedes angeschlossene StorageGRID-Netzwerk verwenden.

Über diese Aufgabe

So installieren Sie StorageGRID auf einem Services Appliance-Node:

- Sie geben die IP-Adresse des primären Admin-Knotens und den Namen des Appliance-Nodes an oder bestätigen sie.
- Sie starten die Installation und warten, bis die Software installiert ist.

Die Installation wird durch die Installationsaufgaben für den Gateway Node der Appliance partway angehalten. Um die Installation fortzusetzen, melden Sie sich beim Grid Manager an, genehmigen alle Grid-Nodes und schließen den StorageGRID-Installationsprozess ab. Für die Installation eines nicht primären Admin-Knotens ist keine Genehmigung erforderlich.



Implementieren Sie die SG100 und SG1000 Service Appliances nicht am selben Standort. Das kann zu einer unvorhersehbaren Performance führen.



Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess automatisieren. Siehe ["Automatisierung der Appliance-Installation und -Konfiguration"](#).

Schritte

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse für das Gerät ein.

`https://Controller_IP:8443`

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Legen Sie im Abschnitt primäre Administratorknoten-Verbindung fest, ob Sie die IP-Adresse für den primären Admin-Node angeben müssen.

Wenn Sie zuvor andere Knoten in diesem Rechenzentrum installiert haben, kann der StorageGRID-Appliance-Installer diese IP-Adresse automatisch erkennen, vorausgesetzt, dass der primäre Admin-Knoten oder mindestens ein anderer Grid-Node mit ADMIN_IP konfiguriert ist, im selben Subnetz vorhanden ist.

3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	<ul style="list-style-type: none"> a. Deaktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie Auf Speichern. d. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.
Automatische Erkennung aller verbundenen primären Admin-Nodes	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Warten Sie, bis die Liste der erkannten IP-Adressen angezeigt wird. c. Wählen Sie den primären Admin-Node für das Grid aus, in dem dieser Appliance-Speicher-Node bereitgestellt werden soll. d. Klicken Sie Auf Speichern. e. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.

4. Geben Sie im Feld **Node Name** den Systemnamen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und klicken Sie auf **Save**.

Der Name, der hier angezeigt wird, ist der Systemname des Appliance-Node. Systemnamen sind für interne StorageGRID-Vorgänge erforderlich und können nicht geändert werden.

5. Führen Sie optional folgende Schritte aus, um eine andere Version der StorageGRID-Software zu installieren:

- a. Laden Sie das Installationsarchiv herunter:

["NetApp Downloads mit StorageGRID Appliance"](#)

- b. Extrahieren Sie das Archiv.
- c. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > StorageGRID-Software hochladen**.
- d. Klicken Sie auf **Entfernen**, um das aktuelle Softwarepaket zu entfernen.

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking ▾ | Configure Hardware ▾ | Monitor Installation | Advanced ▾

Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

Current StorageGRID Installation Software

Version	11.3.0
Package Name	storagegrid-webscale-images-11-3-0_11.3.0-20190806.1731.4064510_amd64.deb

- e. Klicken Sie auf **Durchsuchen** für das Softwarepaket, das Sie heruntergeladen und extrahiert haben, und klicken Sie dann auf **Durchsuchen** für die Prüfsummendatei.

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking ▾ | Configure Hardware ▾ | Monitor Installation | Advanced ▾

Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

Current StorageGRID Installation Software

Version	None
Package Name	None

Upload StorageGRID Installation Software

Software Package	<input type="button" value="Browse"/>
Checksum File	<input type="button" value="Browse"/>

- f. Wählen Sie **Home**, um zur Startseite zurückzukehren.

6. Überprüfen Sie im Abschnitt Installation, ob der aktuelle Status „bereit zum Starten der Installation von ist *node name* In das Grid mit primärem Admin-Node *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.

7. Klicken Sie auf der Startseite des StorageGRID-Appliance-Installationsprogramms auf **Installation starten**.

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type

Node name

Cancel

Save

Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

Connection state **Connection to 172.16.6.32 ready**

Cancel

Save

Installation

Current state **Ready to start installation of GW-SG1000-003-074 into grid with Admin Node 172.16.6.32 running StorageGRID 11.6.0, using StorageGRID software downloaded from the Admin Node.**

Start Installation

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.



Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, klicken Sie in der Menüleiste auf **Monitor-Installation**.

8. Wenn Ihr Grid mehrere Appliance-Nodes enthält, wiederholen Sie die vorherigen Schritte für jede Appliance.

Überwachen Sie die Appliance-Installation

Das Installationsprogramm der StorageGRID Appliance stellt den Status bereit, bis die Installation abgeschlossen ist. Nach Abschluss der Softwareinstallation wird die Appliance neu gestartet.

Beispiel 1. Schritte

Storage Appliance

1. Um den Installationsfortschritt zu überwachen, klicken Sie auf **Installation überwachen**.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage		Running
Step	Progress	Status
Connect to storage controller		Complete
Clear existing configuration		Complete
Configure volumes		Creating volume StorageGRID-obj-00
Configure host settings		Pending

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt 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 Speicher-Controller her, löscht alle vorhandenen Konfigurationen, erstellt Raids gemäß dem konfigurierten RAID-Modus, weist Volumes für die StorageGRID-Software und den Objektdatenspeicher zu und konfiguriert Hostereinstellungen.

2. Installieren Sie das Betriebssystem

In dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID auf die Appliance.

3. Überwachen Sie den Installationsfortschritt weiter, bis die Phase **StorageGRID installieren** angehalten wird. Auf der eingebetteten Konsole wird eine Meldung angezeigt, in der Sie aufgefordert werden, diesen Knoten auf dem Admin-Knoten mithilfe des Grid-Managers zu genehmigen. Fahren Sie mit dem nächsten Schritt fort.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

4. Wechseln Sie zum Grid-Manager des Knotens „primärer Administrator“, genehmigen Sie den ausstehenden Speicherknoten und führen Sie den StorageGRID-Installationsprozess durch.

Wenn Sie im Grid Manager auf **Installieren** klicken, wird Stufe 3 abgeschlossen und Stufe 4, **Installation abschließen**, beginnt. Wenn Phase 4 abgeschlossen ist, wird der Controller neu gestartet.

Service-Appliance

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt 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**

In dieser Phase löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken in der Appliance und konfiguriert die Hosteinstellungen.

◦ **2. Installieren Sie das Betriebssystem**

In dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID auf die Appliance.

3. Fahren Sie mit der Überwachung des Installationsfortschritts fort, bis einer der folgenden Prozesse erfolgt ist:

- Für alle Appliance-Knoten außer dem primären Admin-Node wird die Install StorageGRID-Phase angehalten, und eine Meldung wird in der eingebetteten Konsole angezeigt. Sie werden aufgefordert, diesen Knoten über den Grid-Manager genehmigen zu lassen. Fahren Sie mit dem nächsten Schritt fort.
- Für die Installation des primären Admin-Knotens der Appliance müssen Sie den Knoten nicht genehmigen. Das Gerät wird neu gestartet. Sie können den nächsten Schritt überspringen.



Während der Installation eines primären Administrator-Knotens der Appliance wird eine fünfte Phase angezeigt (siehe Beispielbildschirm mit vier Phasen). Wenn die fünfte Phase länger als 10 Minuten in Bearbeitung ist, aktualisieren Sie die Webseite manuell.

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

```
Connected (unencrypted) to: QEMU
/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...
```

4. Wechseln Sie zum Grid-Manager des Knotens „primärer Administrator“, genehmigen Sie den ausstehenden Grid-Node und schließen Sie den StorageGRID-Installationsprozess ab.

Wenn Sie im Grid Manager auf **Installieren** klicken, wird Stufe 3 abgeschlossen und Stufe 4, **Installation abschließen**, beginnt. Wenn Phase 4 abgeschlossen ist, wird das Gerät neu gestartet.

Starten Sie die Appliance neu, während das Installationsprogramm der StorageGRID Appliance ausgeführt wird

Möglicherweise müssen Sie die Appliance neu starten, während das Installationsprogramm der StorageGRID-Appliance ausgeführt wird. Sie müssen die Appliance beispielsweise neu starten, wenn die Installation fehlschlägt.

Über diese Aufgabe

Dieses Verfahren gilt nur, wenn die Appliance das Installationsprogramm für die StorageGRID-Appliance ausführt. Nach Abschluss der Installation funktioniert dieser Schritt nicht mehr, da das Installationsprogramm für StorageGRID-Geräte nicht mehr verfügbar ist.

Schritte

1. Klicken Sie im Installationsprogramm der StorageGRID-Appliance auf **Erweitert > Controller neu starten**, und wählen Sie dann eine der folgenden Optionen aus:
 - Wählen Sie **Neustart in StorageGRID** aus, um den Controller neu zu starten, wobei der Knoten wieder in das Raster integriert wird. Wählen Sie diese Option, wenn Sie im Wartungsmodus ausgeführt werden und den Node in den normalen Betrieb zurückkehren möchten.
 - Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. (Diese Option ist nur verfügbar, wenn sich der Controller im Wartungsmodus befindet.) Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Das Gerät wird neu gestartet.

Fehlerbehebung bei Hardwareinstallation (SGF6112)

Wenn während der Installation Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu Hardware-Setup- und Konnektivitätsproblemen überprüfen.

Startcodes anzeigen (SGF6112)

Wenn Sie das Gerät mit Strom versorgen, protokolliert der BMC eine Reihe von Startcodes. Sie können diese Codes auf einer grafischen Konsole anzeigen, die mit dem

BMC-Management-Port verbunden ist.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Wenn Sie Seriell-über-LAN (SOL) verwenden möchten, haben Sie Erfahrung mit IPMI SOL-Konsolenanwendungen.

Schritte

1. Wählen Sie eine der folgenden Methoden, um die Startcodes für den Gerätesteuerung anzuzeigen, und sammeln Sie die erforderlichen Geräte.

Methode	Erforderliche Ausrüstung
VGA-Konsole	<ul style="list-style-type: none">• VGA-fähiger Monitor• VGA-Kabel
KVM	<ul style="list-style-type: none">• RJ-45-Kabel
Serieller Port	<ul style="list-style-type: none">• SERIELLES DB-9-Kabel• Serielles virtuelles Terminal
SOL	<ul style="list-style-type: none">• Serielles virtuelles Terminal

2. Wenn Sie eine VGA-Konsole verwenden, führen Sie die folgenden Schritte aus:
 - a. Schließen Sie einen VGA-fähigen Monitor an den VGA-Anschluss auf der Rückseite des Geräts an.
 - b. Zeigen Sie die Codes an, die auf dem Monitor angezeigt werden.
3. Wenn Sie BMC KVM verwenden, führen Sie die folgenden Schritte aus:
 - a. Stellen Sie eine Verbindung zum BMC-Verwaltungsanschluss her, und melden Sie sich bei der BMC-Webschnittstelle an.
 - b. Wählen Sie **Fernbedienung**.
 - c. Starten Sie KVM.
 - d. Zeigen Sie die Codes auf dem virtuellen Monitor an.
4. Wenn Sie einen seriellen Port und ein Terminal verwenden, führen Sie die folgenden Schritte aus:
 - a. Schließen Sie den seriellen USB-Anschluss an der Rückseite des Geräts an.
 - b. Einstellungen verwenden `115200 8-N-1`.
 - c. Zeigen Sie die Codes an, die über der seriellen Klemme gedruckt wurden.
5. Wenn Sie SOL verwenden, führen Sie die folgenden Schritte aus:
 - a. Stellen Sie mithilfe der BMC-IP-Adresse und der Anmeldedaten eine Verbindung zum IPMI SOL her.

```
ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
```
 - b. Die Codes auf dem virtuellen seriellen Terminal anzeigen.
6. Verwenden Sie die Tabelle, um die Codes für Ihr Gerät zu suchen.

Codieren	Zeigt An
HI	Das Master-Boot-Skript wurde gestartet.
HP	Das System prüft, ob die NIC-Firmware (Network Interface Card) aktualisiert werden muss.
RB	Das System wird nach dem Anwenden von Firmware-Updates neu gebootet.
FP	Die Update-Prüfungen der Hardware-Subsystem-Firmware wurden abgeschlossen. Die Kommunikationsdienste zwischen den Controllern werden gestartet.
HZ	Das System prüft gerade auf vorhandene StorageGRID Installationsdaten.
HO	Die StorageGRID Appliance wird ausgeführt.
HOCHVERFÜGBARKEIT	StorageGRID wird ausgeführt.

Verwandte Informationen

["Greifen Sie auf die BMC-Schnittstelle zu"](#)

Fehlercodes anzeigen (SGF6112)

Wenn beim Starten der Appliance ein Hardwarefehler auftritt, meldet der BMC einen Fehlercode. Bei Bedarf können Sie diese Fehlercodes über die BMC-Schnittstelle anzeigen und dann mit dem technischen Support zusammenarbeiten, um das Problem zu lösen.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.

Schritte

1. Wählen Sie im BMC-Dashboard **BIOS POST Code** aus.
2. Überprüfen Sie die angezeigten Informationen für den aktuellen Code und den vorherigen Code.

Wenn einer der folgenden Fehlercodes angezeigt wird, wenden Sie sich an den technischen Support, um das Problem zu beheben.

Codieren	Zeigt An
0x0E	Der Mikrocode wurde nicht gefunden
0x0F	Mikrocode nicht geladen

Codieren	Zeigt An
0x50	Speicherinitialisierungsfehler. Ungültiger Speichertyp oder inkompatible Speichergeschwindigkeit.
0x51	Speicherinitialisierungsfehler. Der SPD-Lesewert ist fehlgeschlagen.
0x52	Speicherinitialisierungsfehler. Ungültige Speichergröße oder Speichermodule stimmen nicht überein.
0x53	Speicherinitialisierungsfehler. Kein verwendbarer Speicher erkannt.
0x54	Nicht angegebener Speicherinitialisierungsfehler
0x55	Speicher nicht installiert
0x56	Ungültiger CPU-Typ oder ungültige Geschwindigkeit
0x57	CPU-Diskrepanz
0x58	CPU-Selbsttest fehlgeschlagen oder möglicher CPU-Cache-Fehler
0x59	Der CPU-Microcode wurde nicht gefunden oder das Microcode-Update ist fehlgeschlagen
0x5A	Interner CPU-Fehler
0x5B	PPI zurücksetzen ist nicht verfügbar
0x5C	PEI-Phase BMC Selbsttest fehlgeschlagen
0xD0	CPU-Initialisierungsfehler
0xD1	Initialisierungsfehler der Nordbrücke
0xD2	Initialisierungsfehler Südbrücke
0xD3	Einige Architekturprotokolle sind nicht verfügbar
0xD4	Fehler bei der PCI-Ressourcenzuweisung. Nicht mehr zur Verfügung.
0xD5	Kein Speicherplatz für Legacy Option ROM
0xD6	Es wurden keine Ausgabegeräte für die Konsole gefunden

Codieren	Zeigt An
0xD7	Es wurden keine Geräte für den Konsoleneingang gefunden
0xD8	Ungültiges Passwort
0xD9	Fehler beim Laden der Boot-Option (LoadImage hat Fehler zurückgegeben)
0xDA	Boot-Option fehlgeschlagen (StartImage-Fehler zurückgegeben)
0xDB	Flash-Update fehlgeschlagen
0xDC	Das Rücksetzprotokoll ist nicht verfügbar
0xDD	DXE-Phase BMC-Selbsttestfehler
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERN
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL

Codieren	Zeigt An
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

Hardware-Setup scheint zu hängen (SGF6112)

Das Installationsprogramm von StorageGRID Appliance ist möglicherweise nicht verfügbar, wenn Hardwarefehler oder Verkabelungsfehler eine Ausführung der Appliance verhindern.

Schritte

1. Überprüfen Sie die LEDs am Gerät sowie die im BMC angezeigten Boot- und Fehlercodes.
2. Wenn Sie Hilfe bei der Behebung eines Problems benötigen, wenden Sie sich an den technischen Support.

Verwandte Informationen

- ["Startcodes anzeigen \(SGF6112\)"](#)
- ["Fehlercodes anzeigen \(SGF6112\)"](#)

Verbindungsprobleme beheben (SGF6112)

Wenn während der Installation der StorageGRID-Appliance Verbindungsprobleme auftreten, führen Sie die hier aufgeführten Korrekturmaßnahmen durch.

Verbindung zum Gerät nicht möglich

Wenn Sie keine Verbindung zur Services-Appliance herstellen können, liegt möglicherweise ein Netzwerkproblem vor, oder die Hardwareinstallation wurde möglicherweise nicht erfolgreich abgeschlossen.

Schritte

1. Versuchen Sie, das Gerät mit der IP-Adresse des Geräts zu pinggen :
ping appliance_IP
2. Wenn Sie keine Antwort vom Ping erhalten, bestätigen Sie, dass Sie die richtige IP-Adresse verwenden.

Sie können die IP-Adresse der Appliance im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk verwenden.
3. Wenn die IP-Adresse korrekt ist, überprüfen Sie die Geräteverkabelung, QSFP- oder SFP-Transceiver und die Netzwerkeinrichtung.
4. Wenn ein physischer Zugang zur Appliance verfügbar ist, können Sie eine direkte Verbindung zur

permanenten Link-lokalen IP verwenden 169.254.0.1 Um die Controller-Netzwerkconfiguration zu überprüfen und bei Bedarf zu aktualisieren. Detaillierte Anweisungen finden Sie in Schritt 2 unter "[Rufen Sie das Installationsprogramm für StorageGRID-Appliances auf](#)".

Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

5. Wenn der Ping erfolgreich war, öffnen Sie einen Webbrowser.
6. Geben Sie die URL für das StorageGRID-Appliance-Installationsprogramm ein:

`https://appliances_controller_IP:8443`

Die Startseite wird angezeigt.

Fehlerbehebung bei der Hardwareinstallation (SG6000 oder SG5700)

Wenn während der Installation Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu Hardware-Setup- und Konnektivitätsproblemen überprüfen.

Anzeigen von Boot-up-Codes (SG6000-CN-Controller)

Wenn Sie das Gerät mit Strom versorgen, protokolliert der BMC eine Reihe von Startcodes für den SG6000-CN-Controller. Sie können diese Codes auf verschiedene Arten anzeigen.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Wenn Sie Seriell-über-LAN (SOL) verwenden möchten, haben Sie Erfahrung mit IPMI SOL-Konsolenanwendungen.

Schritte

1. Wählen Sie eine der folgenden Methoden, um die Startcodes für den Gerätesteuerung anzuzeigen, und sammeln Sie die erforderlichen Geräte.

Methode	Erforderliche Ausrüstung
VGA-Konsole	<ul style="list-style-type: none">• VGA-fähiger Monitor• VGA-Kabel
KVM	<ul style="list-style-type: none">• RJ-45-Kabel
Serieller Port	<ul style="list-style-type: none">• SERIELLES DB-9-Kabel• Serielles virtuelles Terminal
SOL	<ul style="list-style-type: none">• Serielles virtuelles Terminal

2. Wenn Sie eine VGA-Konsole verwenden, führen Sie die folgenden Schritte aus:
 - a. Schließen Sie einen VGA-fähigen Monitor an den VGA-Anschluss auf der Rückseite des Geräts an.

- b. Zeigen Sie die Codes an, die auf dem Monitor angezeigt werden.
- 3. Wenn Sie BMC KVM verwenden, führen Sie die folgenden Schritte aus:
 - a. Stellen Sie eine Verbindung zum BMC-Verwaltungsanschluss her, und melden Sie sich bei der BMC-Webschnittstelle an.
 - b. Wählen Sie **Fernbedienung**.
 - c. Starten Sie KVM.
 - d. Zeigen Sie die Codes auf dem virtuellen Monitor an.
- 4. Wenn Sie einen seriellen Port und ein Terminal verwenden, führen Sie die folgenden Schritte aus:
 - a. Schließen Sie den seriellen Anschluss DB-9 an der Rückseite des Geräts an.
 - b. Einstellungen verwenden 115200 8-N-1.
 - c. Zeigen Sie die Codes an, die über der seriellen Klemme gedruckt wurden.
- 5. Wenn Sie SOL verwenden, führen Sie die folgenden Schritte aus:

- a. Stellen Sie mithilfe der BMC-IP-Adresse und der Anmeldedaten eine Verbindung zum IPMI SOL her.

```
ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
```



In einigen Fällen kann der Standardbenutzername sein `root` statt `admin`.

- a. Die Codes auf dem virtuellen seriellen Terminal anzeigen.

- 6. Verwenden Sie die Tabelle, um die Codes für Ihr Gerät zu suchen.

Codieren	Zeigt An
HI	Das Master-Boot-Skript wurde gestartet.
HP	Das System prüft, ob die NIC-Firmware (Network Interface Card) aktualisiert werden muss.
RB	Das System wird nach dem Anwenden von Firmware-Updates neu gebootet.
FP	Die Update-Prüfungen der Hardware-Subsystem-Firmware wurden abgeschlossen. Die Kommunikationsdienste zwischen den Controllern werden gestartet.

Codieren	Zeigt An
ER	<p>Nur für Appliance-Storage-Node:</p> <p>Das System wartet auf die Konnektivität mit den Storage Controllern und die Synchronisierung mit dem Betriebssystem SANtricity.</p> <p>Hinweis: Wenn der Start-up-Vorgang nicht über diese Phase läuft, führen Sie folgende Schritte aus:</p> <ol style="list-style-type: none"> Vergewissern Sie sich, dass die vier Verbindungskabel zwischen dem SG6000-CN Controller und den beiden Speichercontrollern sicher angeschlossen sind. Ersetzen Sie bei Bedarf ein oder mehrere Kabel, und versuchen Sie es erneut. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.
HZ	Das System prüft gerade auf vorhandene StorageGRID Installationsdaten.
HO	Das Installationsprogramm für StorageGRID-Appliance wird ausgeführt.
HOCHVERFÜGBARKEIT	StorageGRID wird ausgeführt.

Fehlercodes anzeigen (SG6000-CN-Controller)

Wenn beim Starten des SG6000-CN Controllers ein Hardwarefehler auftritt, meldet der BMC einen Fehlercode. Bei Bedarf können Sie diese Fehlercodes über die BMC-Schnittstelle anzeigen und dann mit dem technischen Support zusammenarbeiten, um das Problem zu lösen.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.

Schritte

1. Wählen Sie im BMC-Dashboard **BIOS POST Code** aus.
2. Überprüfen Sie die angezeigten Informationen für den aktuellen Code und den vorherigen Code.

Wenn einer der folgenden Fehlercodes angezeigt wird, wenden Sie sich an den technischen Support, um das Problem zu beheben.

Codieren	Zeigt An
0x0E	Der Mikrocode wurde nicht gefunden
0x0F	Mikrocode nicht geladen

Codieren	Zeigt An
0x50	Speicherinitialisierungsfehler. Ungültiger Speichertyp oder inkompatible Speichergeschwindigkeit.
0x51	Speicherinitialisierungsfehler. Der SPD-Lesewert ist fehlgeschlagen.
0x52	Speicherinitialisierungsfehler. Ungültige Speichergröße oder Speichermodule stimmen nicht überein.
0x53	Speicherinitialisierungsfehler. Kein verwendbarer Speicher erkannt.
0x54	Nicht angegebener Speicherinitialisierungsfehler
0x55	Speicher nicht installiert
0x56	Ungültiger CPU-Typ oder ungültige Geschwindigkeit
0x57	CPU-Diskrepanz
0x58	CPU-Selbsttest fehlgeschlagen oder möglicher CPU-Cache-Fehler
0x59	Der CPU-Mikrocode wurde nicht gefunden oder das Microcode-Update ist fehlgeschlagen
0x5A	Interner CPU-Fehler
0x5B	PPI zurücksetzen ist nicht verfügbar
0x5C	PEI-Phase BMC Selbsttest fehlgeschlagen
0xD0	CPU-Initialisierungsfehler
0xD1	Initialisierungsfehler der Nordbrücke
0xD2	Initialisierungsfehler Südbrücke
0xD3	Einige Architekturprotokolle sind nicht verfügbar
0xD4	Fehler bei der PCI-Ressourcenzuweisung. Nicht mehr zur Verfügung.
0xD5	Kein Speicherplatz für Legacy Option ROM
0xD6	Es wurden keine Ausgabegeräte für die Konsole gefunden

Codieren	Zeigt An
0xD7	Es wurden keine Geräte für den Konsoleneingang gefunden
0xD8	Ungültiges Passwort
0xD9	Fehler beim Laden der Boot-Option (LoadImage hat Fehler zurückgegeben)
0xDA	Boot-Option fehlgeschlagen (StartImage-Fehler zurückgegeben)
0xDB	Flash-Update fehlgeschlagen
0xDC	Das Rücksetzprotokoll ist nicht verfügbar
0xDD	DXE-Phase BMC-Selbsttestfehler
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERN
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL

Codieren	Zeigt An
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

Hardware-Setup scheint zu hängen (SG6000 oder SG5700)

Der StorageGRID-Appliance-Installer ist möglicherweise nicht verfügbar, wenn Hardwarefehler oder Verkabelungsfehler die Speicher-Controller oder den Appliance-Controller daran hindern, ihre Boot-Verarbeitung abzuschließen.

Beispiel 2. Schritte

SG6000

1. Sehen Sie sich für die Speichercontroller die Codes in den sieben-Segment-Anzeigen an.

Während die Hardware beim Einschalten initialisiert wird, zeigen die beiden sieben Segmente eine Reihe von Codes an. Wenn die Hardware erfolgreich gebootet wurde, werden beide sieben Segmente angezeigt 99.

2. Überprüfen Sie die LEDs am SG6000-CN-Controller sowie die im BMC angezeigten Boot- und Fehlercodes.
3. Wenn Sie Hilfe bei der Behebung eines Problems benötigen, wenden Sie sich an den technischen Support.

SG5700

1. Sehen Sie sich die Codes auf den sieben Segmenten an.

Während die Hardware beim Einschalten initialisiert wird, zeigen die beiden sieben Segmente eine Reihe von Codes an. Wenn die Hardware erfolgreich gebootet wurde, werden in den sieben Segmenten verschiedene Codes für jeden Controller angezeigt.

2. Überprüfen Sie die Codes auf der Anzeige der sieben Segmente für den E5700SG-Controller.



Installation und Bereitstellung nehmen Zeit in Anspruch. Einige Installationsphasen melden dem StorageGRID-Appliance-Installationsprogramm keine Aktualisierungen für mehrere Minuten.

Wenn ein Fehler auftritt, blinkt die Sieben-Segment-Anzeige eine Sequenz, z. B. ER.

3. Um zu verstehen, was diese Codes bedeuten, lesen Sie die folgenden Ressourcen:

Controller	Referenz
E5700SG Controller	<ul style="list-style-type: none">• „status-Indikatoren am E5700SG-Controller“• „HE error: Fehler beim Synchronisieren mit SANtricity OS Software“
E2800 Controller	<i>E5700 and E2800 System Monitoring Guide</i> Hinweis: die für den E5700 Controller der E-Series beschriebenen Codes gelten nicht für den E5700SG Controller in der Appliance.

4. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

Verwandte Informationen

- ["Statusanzeigen anzeigen anzeigen anzeigen"](#)
- ["NetApp E-Series Systems Documentation Site"](#)

- ["HE-Fehler: Fehler beim Synchronisieren mit SANtricity OS Software"](#)
- ["E5700 und E2800 – System Monitoring Guide"](#)
- ["Anzeigen von Boot-up-Codes \(SG6000-CN-Controller\)"](#)
- ["Fehlercodes anzeigen \(SG6000-CN-Controller\)"](#)

Fehlerbehebung bei Verbindungsproblemen (SG6000 oder SG5700)

Wenn während der Installation der StorageGRID-Appliance Verbindungsprobleme auftreten, führen Sie die hier aufgeführten Korrekturmaßnahmen durch.

Es konnte keine Verbindung zur SG6000 Appliance hergestellt werden

Wenn Sie keine Verbindung zur Appliance herstellen können, liegt möglicherweise ein Netzwerkproblem vor, oder die Hardwareinstallation wurde möglicherweise nicht erfolgreich abgeschlossen.

Schritte

1. Wenn Sie keine Verbindung zum SANtricity-System-Manager herstellen können:
 - a. Versuchen Sie, die Appliance mit der IP-Adresse für entweder Storage Controller im Managementnetzwerk für SANtricity System Manager zu pingen:
ping Storage_Controller_IP
 - b. Wenn Sie keine Antwort vom Ping erhalten, bestätigen Sie, dass Sie die richtige IP-Adresse verwenden.

Verwenden Sie die IP-Adresse für Management-Port 1 auf einem Storage Controller.
 - c. Wenn die IP-Adresse korrekt ist, überprüfen Sie die Geräteverkabelung und das Netzwerk-Setup.

Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.
 - d. Wenn der Ping erfolgreich war, öffnen Sie einen Webbrowser.
 - e. Geben Sie die URL für SANtricity System Manager ein:
https://Storage_Controller_IP

Die Login-Seite für SANtricity System Manager wird angezeigt.
2. Wenn Sie keine Verbindung zum SG6000-CN Controller herstellen können:
 - a. Versuchen Sie, das Gerät mit der IP-Adresse für den SG6000-CN-Controller zu pingen:
ping SG6000-CN_Controller_IP
 - b. Wenn Sie keine Antwort vom Ping erhalten, bestätigen Sie, dass Sie die richtige IP-Adresse verwenden.

Sie können die IP-Adresse der Appliance im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk verwenden.
 - c. Wenn die IP-Adresse korrekt ist, überprüfen Sie die Geräteverkabelung, SFP-Transceiver und das Netzwerk-Setup.
 - d. Wenn physischer Zugriff auf das SG6000-CN verfügbar ist, können Sie eine direkte Verbindung zur permanenten Link-lokalen IP verwenden 169.254.0.1 Um die Controller-Netzwerkconfiguration zu überprüfen und bei Bedarf zu aktualisieren. Detaillierte Anweisungen finden Sie in Schritt 2 unter ["Zugriff auf das Installationsprogramm der StorageGRID Appliance"](#).

Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

- e. Wenn der Ping erfolgreich war, öffnen Sie einen Webbrowser.
- f. Geben Sie die URL für das StorageGRID-Appliance-Installationsprogramm ein:
https://SG6000-CN_Controller_IP:8443

Die Startseite wird angezeigt.

SG6060 Erweiterungs-Shelfs werden im Appliance Installer nicht angezeigt

Wenn Sie Erweiterungseinschübe für das SG6060 installiert haben und diese nicht im Installationsprogramm der StorageGRID Appliance angezeigt werden, sollten Sie überprüfen, ob die Shelfs vollständig installiert und eingeschaltet wurden.

Über diese Aufgabe

Sie können überprüfen, ob die Erweiterungs-Shelfs mit der Appliance verbunden sind, indem Sie die folgenden Informationen im Installationsprogramm der StorageGRID Appliance anzeigen:

- Die **Home** Seite enthält eine Nachricht über Erweiterungsregale.



The storage system contains 2 expansion shelves.

- Die Seite **Erweitert > RAID-Modus** zeigt anhand der Anzahl der Laufwerke an, ob das Gerät Erweiterungseinschübe enthält oder nicht. Im folgenden Screenshot werden beispielsweise zwei SSDs und 178 HDDs angezeigt. Ein SG6060 mit zwei Erweiterungs-Shelfs enthält insgesamt 180 Laufwerke.

Configure RAID Mode

This appliance contains the following drives.

Type	Size	Number of drives
SSD	800 GB	2
HDD	11.8 TB	178

Wenn die Seiten des Installationsprogramms für StorageGRID-Geräte nicht angeben, dass Erweiterungs-Shelfs vorhanden sind, gehen Sie wie folgt vor.

Schritte

1. Vergewissern Sie sich, dass alle erforderlichen Kabel fest angeschlossen sind. Siehe "[Kabelgerät \(SG6000\)](#)".
2. Stellen Sie sicher, dass Sie die Erweiterungs-Shelfs eingeschaltet haben. Siehe "[Anschließen des Netzes und Anwenden der Stromversorgung \(SG6000\)](#)".
3. Wenn Sie Hilfe bei der Behebung eines Problems benötigen, wenden Sie sich an den technischen Support.

Es konnte keine Verbindung zur SG5700 Appliance hergestellt werden

Wenn Sie keine Verbindung zur Appliance herstellen können, liegt möglicherweise ein Netzwerkproblem vor, oder die Hardwareinstallation wurde möglicherweise nicht erfolgreich abgeschlossen.

Schritte

1. Wenn Sie keine Verbindung zum SANtricity-System-Manager herstellen können:

a. Versuchen Sie, die Appliance mithilfe der IP-Adresse für den E2800 Controller im Managementnetzwerk für SANtricity System Manager zu pingen:

ping E2800_Controller_IP

b. Wenn Sie keine Antwort vom Ping erhalten, bestätigen Sie, dass Sie die richtige IP-Adresse verwenden.

Verwenden Sie die IP-Adresse für den Management-Port 1 auf dem E2800-Controller.

c. Wenn die IP-Adresse korrekt ist, überprüfen Sie die Geräteverkabelung und das Netzwerk-Setup.

Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

d. Wenn der Ping erfolgreich war, öffnen Sie einen Webbrowser.

e. Geben Sie die URL für SANtricity System Manager ein:

https://E2800_Controller_IP

Die Login-Seite für SANtricity System Manager wird angezeigt.

2. Wenn keine Verbindung zum E5700SG Controller hergestellt werden kann:

a. Versuchen Sie, die Appliance mithilfe der IP-Adresse für den E5700SG-Controller zu pingen:

ping E5700SG_Controller_IP

b. Wenn Sie keine Antwort vom Ping erhalten, bestätigen Sie, dass Sie die richtige IP-Adresse verwenden.

Sie können die IP-Adresse der Appliance im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk verwenden.

c. Wenn die IP-Adresse korrekt ist, überprüfen Sie die Geräteverkabelung, SFP-Transceiver und das Netzwerk-Setup.

Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

d. Wenn der Ping erfolgreich war, öffnen Sie einen Webbrowser.

e. Geben Sie die URL für das StorageGRID-Appliance-Installationsprogramm ein:

https://E5700SG_Controller_IP:8443

Die Startseite wird angezeigt.

Verwandte Informationen

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

HE-Fehler: Fehler beim Synchronisieren mit SANtricity OS Software (SG5700)

Auf der 7-Segment-Anzeige auf dem Compute-Controller wird ein HE-Fehlercode angezeigt, wenn der StorageGRID-Appliance-Installer nicht mit der SANtricity OS-Software synchronisiert werden kann.

Über diese Aufgabe

Wenn ein HE-Fehlercode angezeigt wird, führen Sie diese Korrekturmaßnahme durch.

Schritte

1. Überprüfen Sie die Integrität der beiden SAS Interconnect-Kabel und vergewissern Sie sich, dass sie sicher angeschlossen sind.
2. Ersetzen Sie je nach Bedarf ein oder beide Kabel, und versuchen Sie es erneut.
3. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

Fehlerbehebung bei der Hardwareinstallation (SG100 und SG1000)

Wenn während der Installation Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu Hardware-Setup- und Konnektivitätsproblemen überprüfen.

Boot-up-Codes anzeigen (SG100 und SG1000)

Wenn Sie das Gerät mit Strom versorgen, protokolliert der BMC eine Reihe von Startcodes. Sie können diese Codes auf einer grafischen Konsole anzeigen, die mit dem BMC-Management-Port verbunden ist.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Wenn Sie Seriell-über-LAN (SOL) verwenden möchten, haben Sie Erfahrung mit IPMI SOL-Konsolenanwendungen.

Schritte

1. Wählen Sie eine der folgenden Methoden, um die Startcodes für den Gerätesteuerung anzuzeigen, und sammeln Sie die erforderlichen Geräte.

Methode	Erforderliche Ausrüstung
VGA-Konsole	<ul style="list-style-type: none">• VGA-fähiger Monitor• VGA-Kabel
KVM	<ul style="list-style-type: none">• RJ-45-Kabel
Serieller Port	<ul style="list-style-type: none">• SERIELLES DB-9-Kabel• Serielles virtuelles Terminal
SOL	<ul style="list-style-type: none">• Serielles virtuelles Terminal

2. Wenn Sie eine VGA-Konsole verwenden, führen Sie die folgenden Schritte aus:
 - a. Schließen Sie einen VGA-fähigen Monitor an den VGA-Anschluss auf der Rückseite des Geräts an.
 - b. Zeigen Sie die Codes an, die auf dem Monitor angezeigt werden.
3. Wenn Sie BMC KVM verwenden, führen Sie die folgenden Schritte aus:
 - a. Stellen Sie eine Verbindung zum BMC-Verwaltungsanschluss her, und melden Sie sich bei der BMC-

Webschnittstelle an.

- b. Wählen Sie **Fernbedienung**.
 - c. Starten Sie KVM.
 - d. Zeigen Sie die Codes auf dem virtuellen Monitor an.
4. Wenn Sie einen seriellen Port und ein Terminal verwenden, führen Sie die folgenden Schritte aus:
- a. Schließen Sie den seriellen Anschluss DB-9 an der Rückseite des Geräts an.
 - b. Einstellungen verwenden 115200 8-N-1.
 - c. Zeigen Sie die Codes an, die über der seriellen Klemme gedruckt wurden.
5. Wenn Sie SOL verwenden, führen Sie die folgenden Schritte aus:
- a. Stellen Sie mithilfe der BMC-IP-Adresse und der Anmeldedaten eine Verbindung zum IPMI SOL her.

```
ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
```



In einigen Fällen kann der Standardbenutzername sein `root` Statt `admin`.

- a. Die Codes auf dem virtuellen seriellen Terminal anzeigen.
6. Verwenden Sie die Tabelle, um die Codes für Ihr Gerät zu suchen.

Codieren	Zeigt An
HI	Das Master-Boot-Skript wurde gestartet.
HP	Das System prüft, ob die NIC-Firmware (Network Interface Card) aktualisiert werden muss.
RB	Das System wird nach dem Anwenden von Firmware-Updates neu gebootet.
FP	Die Update-Prüfungen der Hardware-Subsystem-Firmware wurden abgeschlossen. Die Kommunikationsdienste zwischen den Controllern werden gestartet.
HZ	Das System prüft gerade auf vorhandene StorageGRID Installationsdaten.
HO	Die StorageGRID Appliance wird ausgeführt.
HOCHVERFÜGBARKEIT	StorageGRID wird ausgeführt.

Verwandte Informationen

["Greifen Sie auf die BMC-Schnittstelle zu"](#)

Fehlercodes anzeigen (SG100 und SG1000)

Wenn beim Starten der Appliance ein Hardwarefehler auftritt, meldet der BMC einen

Fehlercode. Bei Bedarf können Sie diese Fehlercodes über die BMC-Schnittstelle anzeigen und dann mit dem technischen Support zusammenarbeiten, um das Problem zu lösen.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.

Schritte

1. Wählen Sie im BMC-Dashboard **BIOS POST Code** aus.
2. Überprüfen Sie die angezeigten Informationen für den aktuellen Code und den vorherigen Code.

Wenn einer der folgenden Fehlercodes angezeigt wird, wenden Sie sich an den technischen Support, um das Problem zu beheben.

Codieren	Zeigt An
0x0E	Der Mikrocode wurde nicht gefunden
0x0F	Mikrocode nicht geladen
0x50	Speicherinitialisierungsfehler. Ungültiger Speichertyp oder inkompatible Speichergeschwindigkeit.
0x51	Speicherinitialisierungsfehler. Der SPD-Lesewert ist fehlgeschlagen.
0x52	Speicherinitialisierungsfehler. Ungültige Speichergröße oder Speichermodule stimmen nicht überein.
0x53	Speicherinitialisierungsfehler. Kein verwendbarer Speicher erkannt.
0x54	Nicht angegebener Speicherinitialisierungsfehler
0x55	Speicher nicht installiert
0x56	Ungültiger CPU-Typ oder ungültige Geschwindigkeit
0x57	CPU-Diskrepanz
0x58	CPU-Selbsttest fehlgeschlagen oder möglicher CPU-Cache-Fehler
0x59	Der CPU-Mikrocode wurde nicht gefunden oder das Microcode-Update ist fehlgeschlagen
0x5A	Interner CPU-Fehler
0x5B	PPI zurücksetzen ist nicht verfügbar

Codieren	Zeigt An
0x5C	PEI-Phase BMC Selbsttest fehlgeschlagen
0xD0	CPU-Initialisierungsfehler
0xD1	Initialisierungsfehler der Nordbrücke
0xD2	Initialisierungsfehler Südbrücke
0xD3	Einige Architekturprotokolle sind nicht verfügbar
0xD4	Fehler bei der PCI-Ressourcenzuweisung. Nicht mehr zur Verfügung.
0xD5	Kein Speicherplatz für Legacy Option ROM
0xD6	Es wurden keine Ausgabegeräte für die Konsole gefunden
0xD7	Es wurden keine Geräte für den Konsoleneingang gefunden
0xD8	Ungültiges Passwort
0xD9	Fehler beim Laden der Boot-Option (LoadImage hat Fehler zurückgegeben)
0xDA	Boot-Option fehlgeschlagen (StartImage-Fehler zurückgegeben)
0xDB	Flash-Update fehlgeschlagen
0xDC	Das Rücksetzprotokoll ist nicht verfügbar
0xDD	DXE-Phase BMC-Selbsttestfehler
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY

Codieren	Zeigt An
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERN
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

Hardware-Setup scheint zu hängen (SG100 und SG1000)

Das Installationsprogramm von StorageGRID Appliance ist möglicherweise nicht verfügbar, wenn Hardwarefehler oder Verkabelungsfehler eine Ausführung der Appliance verhindern.

Schritte

1. Überprüfen Sie die LEDs am Gerät sowie die im BMC angezeigten Boot- und Fehlercodes.
2. Wenn Sie Hilfe bei der Behebung eines Problems benötigen, wenden Sie sich an den technischen Support.

Verwandte Informationen

- ["Boot-up-Codes anzeigen \(SG100 und SG1000\)"](#)
- ["Fehlercodes anzeigen \(SG100 und SG1000\)"](#)

Fehlerbehebung bei Verbindungsproblemen (SG100 und SG1000)

Wenn während der Installation der StorageGRID-Appliance Verbindungsprobleme

auftreten, führen Sie die hier aufgeführten Korrekturmaßnahmen durch.

Verbindung zum Gerät nicht möglich

Wenn Sie keine Verbindung zur Services-Appliance herstellen können, liegt möglicherweise ein Netzwerkproblem vor, oder die Hardwareinstallation wurde möglicherweise nicht erfolgreich abgeschlossen.

Schritte

1. Versuchen Sie, das Gerät mit der IP-Adresse des Geräts zu pinggen :
`ping services_appliance_IP`
2. Wenn Sie keine Antwort vom Ping erhalten, bestätigen Sie, dass Sie die richtige IP-Adresse verwenden.

Sie können die IP-Adresse der Appliance im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk verwenden.
3. Wenn die IP-Adresse korrekt ist, überprüfen Sie die Geräteverkabelung, QSFP- oder SFP-Transceiver und die Netzwerkeinrichtung.
4. Wenn ein physischer Zugang zur Appliance verfügbar ist, können Sie eine direkte Verbindung zur permanenten Link-lokalen IP verwenden 169.254.0.1 Um die Controller-Netzwerkconfiguration zu überprüfen und bei Bedarf zu aktualisieren. Detaillierte Anweisungen finden Sie in Schritt 2 unter "[Rufen Sie das Installationsprogramm für StorageGRID-Appliances auf](#)".

Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

5. Wenn der Ping erfolgreich war, öffnen Sie einen Webbrowser.
6. Geben Sie die URL für das StorageGRID-Appliance-Installationsprogramm ein:
`https://appliances_controller_IP:8443`

Die Startseite wird angezeigt.

Installieren Sie Red hat Enterprise Linux oder CentOS

Red hat Enterprise Linux oder CentOS: Übersicht installieren

Die Installation eines StorageGRID Systems in einer Red hat Enterprise Linux (RHEL) oder CentOS Linux Umgebung umfasst drei wichtige Schritte.

1. **Vorbereitung:** Bei der Planung und Vorbereitung führen Sie folgende Aufgaben aus:
 - Erfahren Sie mehr über die Hardware- und Storage-Anforderungen für StorageGRID.
 - Erfahren Sie mehr über die Besonderheiten von "[StorageGRID Networking](#)" Damit Sie Ihr Netzwerk entsprechend konfigurieren können.
 - Ermitteln und Vorbereiten der physischen oder virtuellen Server, die Sie für das Hosten Ihrer StorageGRID Grid Nodes verwenden möchten
 - Auf den Servern, die Sie vorbereitet haben:
 - Installieren Sie Linux
 - Konfigurieren Sie das Hostnetzwerk
 - Hostspeicher konfigurieren

- Die Container-Engine einbauen
 - Installieren Sie die StorageGRID Host Services
2. * Bereitstellung*: Bereitstellung von Grid-Knoten mit der entsprechenden Benutzeroberfläche. Wenn Sie Grid-Nodes implementieren, werden diese als Teil des StorageGRID Systems erstellt und mit einem oder mehreren Netzwerken verbunden.
- a. Verwenden Sie die Linux-Befehlszeile und die Node-Konfigurationsdateien, um auf den in Schritt 1 vorbereiteten Hosts softwarebasierte Grid-Nodes bereitzustellen.
 - b. Verwenden Sie das Installationsprogramm für StorageGRID Appliance, um StorageGRID Appliance-Nodes bereitzustellen.



Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im StorageGRID Installationsverfahren enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie im "[Schnellstart für die Hardwareinstallation](#)" Anleitung für das Gerät finden.

3. **Konfiguration**: Wenn alle Knoten bereitgestellt wurden, verwenden Sie den Grid Manager, um das Grid zu konfigurieren und die Installation abzuschließen.

Diese Anweisungen empfehlen einen Standardansatz zur Implementierung und Konfiguration eines StorageGRID Systems. Siehe auch die Informationen über folgende alternative Ansätze:

- Verwendung eines Standard-Orchestrierungs-Frameworks wie Ansible, Puppet oder Chef zur Installation von RHEL oder CentOS, zur Konfiguration von Netzwerk und Storage, zur Installation der Container Engine und des StorageGRID Host Service sowie zur Implementierung von Virtual Grid-Nodes
- Automatisieren Sie die Implementierung und Konfiguration des StorageGRID Systems mit einem Python-Konfigurationsskript (im Installationsarchiv bereitgestellt).
- Automatisieren Sie die Implementierung und Konfiguration von Appliance-Grid-Nodes mit einem Python-Konfigurationsskript (erhältlich über das Installationsarchiv oder über das Installationsprogramm von StorageGRID Appliance).
- Als fortschrittlicher Entwickler von StorageGRID-Implementierungen sollten Sie die Installation VON REST-APIs verwenden, um die Installation von StorageGRID Grid-Nodes zu automatisieren.

Planung und Vorbereitung der Installation von Red hat oder CentOS

Vor der Installation (Red hat oder CentOS)

Bevor Sie Grid-Nodes implementieren und StorageGRID konfigurieren, müssen Sie mit den Schritten und Anforderungen für den Abschluss des Verfahrens vertraut sein.

Bei den Implementierungs- und Konfigurationsverfahren für StorageGRID ist bereits die Architektur und der Betrieb des StorageGRID Systems bekannt.

Sie können einen oder mehrere Standorte gleichzeitig implementieren. Alle Standorte müssen jedoch die Mindestanforderungen erfüllen, die für mindestens drei Storage-Nodes bestehen.

Vor dem Starten einer StorageGRID-Installation müssen folgende Schritte durchgeführt werden:

- Verstehen Sie die Computing-Anforderungen, einschließlich der minimalen CPU- und RAM-Anforderungen für jeden Node.
- Erfahren Sie, wie StorageGRID diverse Netzwerke unterstützt, um die Trennung von Datenverkehr,

Sicherheit und Verwaltung zu gewährleisten, und planen Sie, welche Netzwerke Sie mit den einzelnen StorageGRID Nodes verbinden möchten.

Siehe StorageGRID "[Netzwerkrichtlinien](#)".

- Ermitteln der Storage- und Performance-Anforderungen der einzelnen Grid-Nodes
- Ermitteln Sie eine Reihe von Servern (physische, virtuelle oder beides), die als Aggregat ausreichend Ressourcen zur Unterstützung der Anzahl und des Typs der zu implementierenden StorageGRID Nodes bieten.
- Verstehen Sie die "[Anforderungen für die Node-Migration](#)", Wenn Sie planmäßige Wartungsarbeiten auf physischen Hosts ohne Serviceunterbrechung durchführen möchten.
- Sammeln Sie alle Netzwerkinformationen im Voraus. Sammeln Sie, sofern Sie kein DHCP verwenden, die IP-Adressen für die einzelnen Grid-Nodes sowie die IP-Adressen der zu verwendenden DNS- und NTP-Server.
- Installation, Anschluss und Konfiguration der gesamten erforderlichen Hardware – einschließlich aller StorageGRID Appliances – gemäß den Spezifikationen



Wenn bei der StorageGRID-Installation keine StorageGRID Appliance (Hardware) Storage Nodes verwendet werden, müssen Sie Hardware-RAID-Storage mit batteriegestütztem Schreib-Cache (BBWC) verwenden. StorageGRID unterstützt die Verwendung von Virtual Storage Area Networks (VSANs), Software-RAID oder keinen RAID-Schutz.



Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im StorageGRID Installationsverfahren enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie unter "[Appliance-Hardware installieren](#)".

- Legen Sie fest, welche der verfügbaren Implementierungs- und Konfigurationstools Sie verwenden möchten.

Erforderliche Materialien

Bevor Sie StorageGRID installieren, müssen Sie die erforderlichen Materialien erfassen und vorbereiten.

Element	Hinweise
NetApp StorageGRID Lizenz	Sie benötigen eine gültige, digital signierte NetApp Lizenz. Hinweis: Eine Non-Production-Lizenz, die für Tests und Proof of Concept Grids verwendet werden kann, ist im StorageGRID-Installationsarchiv enthalten.
StorageGRID Installationsarchiv	Unbedingt " Laden Sie das StorageGRID-Installationsarchiv herunter und extrahieren Sie die Dateien ".

Element	Hinweise
Service-Laptop	<p>Das StorageGRID System wird über einen Service-Laptop installiert.</p> <p>Der Service-Laptop muss Folgendes haben:</p> <ul style="list-style-type: none"> • Netzwerkport • SSH-Client (z. B. PuTTY) • "Unterstützter Webbrowser"
StorageGRID-Dokumentation	<ul style="list-style-type: none"> • "Versionshinweise" • "Anweisungen für die Administration von StorageGRID"

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Sie müssen das StorageGRID-Installationsarchiv herunterladen und die erforderlichen Dateien extrahieren.

Schritte

1. Wechseln Sie zum ["NetApp Download-Seite für StorageGRID"](#).
2. Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version, oder wählen Sie eine andere Version aus dem Dropdown-Menü aus und wählen Sie **Go**.
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
4. Wenn eine Vorsichtshinweis/MustRead-Anweisung angezeigt wird, lesen Sie sie und aktivieren Sie das Kontrollkästchen.



Nachdem Sie die StorageGRID Version installiert haben, müssen Sie alle erforderlichen Hotfixes anwenden. Weitere Informationen finden Sie im ["Hotfix-Verfahren in der Recovery- und Wartungsanleitung"](#).

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



Wählen Sie die aus .zip Datei, wenn Windows auf dem Service-Laptop ausgeführt wird.

7. Speichern und extrahieren Sie die Archivdatei.
8. Wählen Sie aus der folgenden Liste die benötigten Dateien aus.

Die benötigten Dateien hängen von der geplanten Grid-Topologie und der Implementierung des StorageGRID Systems ab.



Die in der Tabelle aufgeführten Pfade beziehen sich auf das Verzeichnis der obersten Ebene, das vom extrahierten Installationsarchiv installiert wird

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	RPM Paket für die Installation der StorageGRID Node Images auf Ihren RHEL- oder CentOS-Hosts.
	RPM Paket für die Installation des StorageGRID Host Service auf Ihren RHEL- oder CentOS-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können. Sie können dieses Skript auch für Ping Federate verwenden.
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel für die Ansible-Rolle und das Playbook zur Konfiguration von RHEL- oder CentOS-Hosts für die Implementierung von StorageGRID Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.

Pfad und Dateiname	Beschreibung
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.

CPU- und RAM-Anforderungen erfüllt

Überprüfen und konfigurieren Sie vor dem Installieren der StorageGRID Software die Hardware so, dass sie zur Unterstützung des StorageGRID Systems bereit ist.

Informationen zu unterstützten Servern finden Sie im "[NetApp Interoperabilitäts-Matrix-Tool](#)".

Jeder StorageGRID Node benötigt die folgenden Mindestanforderungen:

- CPU-Cores: 8 pro Node
- RAM: Mindestens 24 GB pro Node und 2 bis 16 GB weniger als der gesamte System-RAM, abhängig von der verfügbaren RAM-Gesamtkapazität und der Anzahl der nicht-StorageGRID-Software, die auf dem System ausgeführt wird

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



Überwachen Sie Ihre CPU- und Arbeitsspeicherauslastung regelmäßig, um sicherzustellen, dass diese Ressourcen Ihre Workloads weiterhin erfüllen. Beispielsweise würde eine Verdoppelung der RAM- und CPU-Zuweisung für virtuelle Storage-Nodes ähnliche Ressourcen bereitstellen wie für die StorageGRID Appliance-Nodes. Wenn die Menge der Metadaten pro Node 500 GB überschreitet, sollten Sie darüber hinaus den RAM pro Node auf 48 GB oder mehr erhöhen. Informationen zum Management von Objekt-Metadaten-Storage, zum Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten und zum Monitoring der CPU- und Arbeitsspeicherauslastung finden Sie in den Anweisungen für "[Administration](#)", "[Monitoring](#)", und "[Aktualisierung](#)" StorageGRID:

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

Wenn Sie Virtual Machines als Hosts verwenden und die Größe und Anzahl der VMs kontrollieren können, sollten Sie für jeden StorageGRID Node eine einzelne VM verwenden und die Größe der VM entsprechend

festlegen.

Bei Produktionsimplementierungen sollten nicht mehrere Storage-Nodes auf derselben physischen Speicherhardware oder einem virtuellen Host ausgeführt werden. Jeder Storage-Node in einer einzelnen StorageGRID-Implementierung sollte sich in einer eigenen, isolierten Ausfall-Domäne befinden. Sie können die Langlebigkeit und Verfügbarkeit von Objektdaten maximieren, wenn sichergestellt wird, dass ein einzelner Hardwareausfall nur einen einzelnen Storage-Node beeinträchtigen kann.

Siehe auch "[Storage- und Performance-Anforderungen erfüllt](#)".

Storage- und Performance-Anforderungen erfüllt

Sie müssen die Storage-Anforderungen für StorageGRID-Nodes verstehen, damit Sie ausreichend Speicherplatz für die Erstkonfiguration und die künftige Storage-Erweiterung bereitstellen können.

StorageGRID Nodes erfordern drei logische Storage-Kategorien:

- **Container Pool** — Performance-Tier (10K SAS oder SSD) Speicher für die Knoten-Container, die dem Container-Engine-Speichertreiber zugewiesen wird, wenn Sie die Container-Engine auf den Hosts installieren und konfigurieren, die Ihre StorageGRID-Knoten unterstützen.
- **Systemdaten** — Performance-Tier (10.000 SAS oder SSD) Speicher für persistenten Speicher pro Node von Systemdaten und Transaktionsprotokollen, die die StorageGRID Host Services nutzen und einzelnen Nodes zuordnen werden.
- **Objektdaten** — Performance-Tier (10.000 SAS oder SSD) Storage und Capacity-Tier (NL-SAS/SATA) Massenspeicher für die persistente Speicherung von Objektdaten und Objekt-Metadaten.

Sie müssen RAID-gestützte Blockgeräte für alle Speicherkategorien verwenden. Nicht redundante Festplatten, SSDs oder JBODs werden nicht unterstützt. Sie können für jede der Storage-Kategorien gemeinsam genutzten oder lokalen RAID-Speicher verwenden. Wenn Sie jedoch die Funktion zur Node-Migration in StorageGRID verwenden möchten, müssen Sie sowohl System- als auch Objektdaten auf Shared Storage speichern. Weitere Informationen finden Sie unter "[Anforderungen für die Container-Migration für Nodes](#)".

Performance-Anforderungen erfüllt

Die Performance der für den Container-Pool verwendeten Volumes, Systemdaten und Objektmetadaten wirkt sich erheblich auf die Gesamt-Performance des Systems aus. Sie sollten Performance-Tier-Storage (10.000 SAS oder SSD) für diese Volumes verwenden, um eine angemessene Festplatten-Performance in Bezug auf Latenz, Input/Output Operations per Second (IOPS) und Durchsatz sicherzustellen. Sie können Capacity-Tier (NL-SAS/SATA)-Storage für den persistenten Storage von Objektdaten verwenden.

Für die Volumes, die für den Container-Pool, Systemdaten und Objektdaten verwendet werden, muss ein Write-Back-Caching aktiviert sein. Der Cache muss sich auf einem geschützten oder persistenten Medium befinden.

Anforderungen an Hosts, die NetApp ONTAP Storage nutzen

Wenn der StorageGRID-Node Storage verwendet, der einem NetApp ONTAP System zugewiesen ist, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

Anzahl der erforderlichen Hosts

Jeder StorageGRID Standort erfordert mindestens drei Storage-Nodes.



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Storage Node auf einem einzelnen physischen oder virtuellen Host aus. Die Verwendung eines dedizierten Hosts für jeden Speicherknoten stellt eine isolierte Ausfalldomäne zur Verfügung.

Andere Node-Typen wie Admin-Nodes oder Gateway-Nodes können auf denselben Hosts implementiert oder je nach Bedarf auf ihren eigenen dedizierten Hosts implementiert werden.

Anzahl der Storage-Volumes pro Host

In der folgenden Tabelle ist die Anzahl der für jeden Host erforderlichen Storage Volumes (LUNs) und die Mindestgröße für jede LUN angegeben, basierend darauf, welche Nodes auf diesem Host implementiert werden.

Die maximale getestete LUN-Größe beträgt 39 TB.



Diese Nummern gelten für jeden Host, nicht für das gesamte Raster.

LUN-Zweck	Storage-Kategorie	Anzahl LUNs	Minimale Größe/LUN
Storage-Pool für Container-Engine	Container-Pool	1	Gesamtzahl der Nodes × 100 GB
/var/local Datenmenge	Systemdaten	1 für jeden Node auf diesem Host	90 GB
Storage-Node	Objektdaten	3 für jeden Speicherknoten auf diesem Host Hinweis: ein softwarebasierter Speicherknoten kann 1 bis 16 Speicher-Volumes haben; es werden mindestens 3 Speicher-Volumes empfohlen.	12 TB (4 TB/LUN) SIEHE Storage-Anforderungen für Storage-Nodes Finden Sie weitere Informationen.
Prüfprotokolle für Admin-Node	Systemdaten	1 für jeden Admin-Node auf diesem Host	200 GB

LUN-Zweck	Storage-Kategorie	Anzahl LUNs	Minimale Größe/LUN
Admin-Node-Tabellen	Systemdaten	1 für jeden Admin-Node auf diesem Host	200 GB



Je nach konfigurierter Audit-Ebene die Größe der Benutzereingaben wie S3-Objektschlüsselname, Und wie viele Audit-Log-Daten Sie erhalten müssen, müssen Sie möglicherweise die Größe der Audit-Log-LUN auf jedem Admin-Node erhöhen. Im Allgemeinen generiert ein Grid ca. 1 KB Audit-Daten pro S3-Vorgang, Das heißt, eine 200 GB LUN würde 70 Millionen Operationen pro Tag oder 800 Operationen pro Sekunde für zwei bis drei Tage unterstützen.

Minimaler Speicherplatz für einen Host

In der folgenden Tabelle ist der erforderliche Mindestspeicherplatz für jeden Node-Typ aufgeführt. Anhand dieser Tabelle können Sie bestimmen, welcher Storage-Mindestbetrag für den Host in jeder Storage-Kategorie bereitgestellt werden muss. Dabei können Sie festlegen, welche Nodes auf diesem Host implementiert werden.



Disk Snapshots können nicht zur Wiederherstellung von Grid Nodes verwendet werden. Lesen Sie stattdessen den Abschnitt "[Recovery von Grid Nodes](#)" Verfahren für jeden Node-Typ.

Node-Typ	Container-Pool	Systemdaten	Objektdaten
Storage-Node	100 GB	90 GB	4,000 GB
Admin-Node	100 GB	490 GB (3 LUNs)	<i>Nicht zutreffend</i>
Gateway-Node	100 GB	90 GB	<i>Nicht zutreffend</i>
Archiv-Node	100 GB	90 GB	<i>Nicht zutreffend</i>

Beispiel: Berechnung der Storage-Anforderungen für einen Host

Angenommen, Sie planen, drei Nodes auf demselben Host zu implementieren: Einen Storage-Node, einen Admin-Node und einen Gateway-Node. Sie sollten dem Host mindestens neun Storage Volumes zur Verfügung stellen. Es sind mindestens 300 GB Performance-Tier-Storage für die Node-Container, 670 GB Performance-Tier-Storage für Systemdaten und Transaktionsprotokolle und 12 TB Kapazitäts-Tier Storage für Objektdaten erforderlich.

Node-Typ	LUN-Zweck	Anzahl LUNs	Die LUN-Größe
Storage-Node	Storage-Pool für Container-Engine	1	300 GB (100 GB/Node)
Storage-Node	<code>/var/local</code> Datenmenge	1	90 GB
Storage-Node	Objektdaten	3	12 TB (4 TB/LUN)

Node-Typ	LUN-Zweck	Anzahl LUNs	Die LUN-Größe
Admin-Node	/var/local Datenmenge	1	90 GB
Admin-Node	Prüfprotokolle für Admin- Node	1	200 GB
Admin-Node	Admin-Node-Tabellen	1	200 GB
Gateway-Node	/var/local Datenmenge	1	90 GB
Gesamt		9	Container-Pool: 300 GB Systemdaten: 670 GB Objektdaten: 12,000 GB

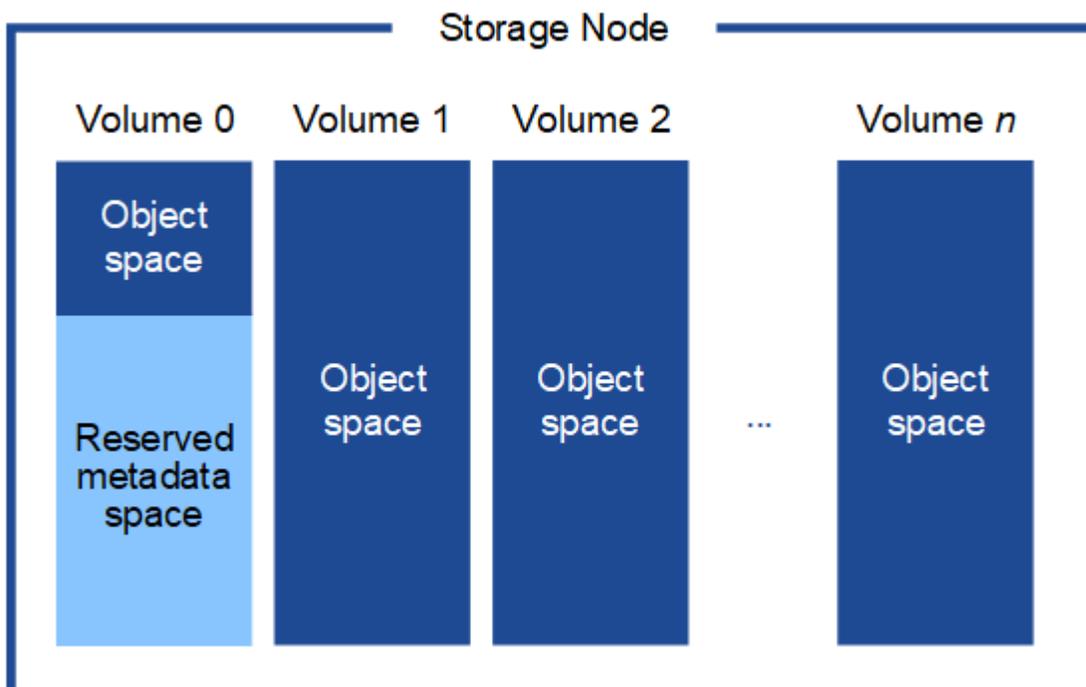
Storage-Anforderungen für Storage-Nodes

Ein softwarebasierter Speicher-Node kann 1 bis 16 Speicher-Volumes haben - 3 oder mehr Speicher-Volumes werden empfohlen. Jedes Storage-Volume sollte 4 TB oder größer sein.



Ein Appliance-Speicherknoten kann bis zu 48 Speicher-Volumes haben.

Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objekt-Metadaten auf dem Storage Volume 0 jedes Storage-Nodes. Alle verbleibenden Speicherplatz auf dem Storage-Volume 0 und anderen Storage-Volumes im Storage-Node werden ausschließlich für Objektdaten verwendet.



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

Wenn Sie Volume 0 eines neuen Storage-Node Speicherplatz zuweisen, müssen Sie sicherstellen, dass für den Anteil aller Objekt-Metadaten des Node ausreichend Speicherplatz vorhanden ist.

- Mindestens müssen Sie Volume 0 mindestens 4 TB zuweisen.



Wenn Sie nur ein Storage-Volume für einen Storage-Node verwenden und dem Volume 4 TB oder weniger zuweisen, hat der Storage-Node beim Start möglicherweise den Schreibgeschützten Storage-Status und speichert nur Objekt-Metadaten.



Wenn Sie Volume 0 weniger als 500 GB zuweisen (nur für den nicht-produktiven Einsatz), sind 10 % der Kapazität des Speicher-Volumes für Metadaten reserviert.

- Wenn Sie ein neues System installieren (StorageGRID 11.6 oder höher) und jeder Speicherknoten mindestens 128 GB RAM hat, weisen Sie Volume 0 mindestens 8 TB zu. Bei Verwendung eines größeren Werts für Volume 0 kann der zulässige Speicherplatz für Metadaten auf jedem Storage Node erhöht werden.
- Verwenden Sie bei der Konfiguration verschiedener Storage-Nodes für einen Standort, falls möglich, die gleiche Einstellung für Volume 0. Wenn ein Standort Storage-Nodes unterschiedlicher Größe enthält, bestimmt der Storage-Node mit dem kleinsten Volume 0 die Metadaten-Kapazität dieses Standorts.

Weitere Informationen finden Sie unter "[Management von Objekt-Metadaten-Storage](#)".

Anforderungen für die Container-Migration für Nodes

Mit der Funktion zur Node-Migration können Sie einen Node manuell von einem Host auf einen anderen verschieben. Normalerweise befinden sich beide Hosts im selben physischen Datacenter.

Dank der Node-Migration können Sie physische Host-Wartungsarbeiten durchführen, ohne Grid-Vorgänge zu unterbrechen. Sie verschieben alle StorageGRID-Nodes nacheinander auf einen anderen Host, bevor Sie den physischen Host in den Offline-Modus versetzen. Die Migration von Nodes erfordert nur kurze Ausfallzeiten für jeden Node. Der Betrieb und die Verfügbarkeit von Grid-Services sollte dabei nicht beeinträchtigt werden.

Wenn Sie die StorageGRID-Node-Migrationsfunktion nutzen möchten, muss Ihre Implementierung zusätzliche Anforderungen erfüllen:

- Konsistente Netzwerkschnittstellennamen über Hosts in einem einzigen physischen Datacenter hinweg
- Shared Storage für StorageGRID Metadaten und Objekt-Repository-Volumes, auf die alle Hosts in einem einzigen physischen Datacenter zugreifen können So können Sie beispielsweise ein NetApp E-Series Storage-Array verwenden.

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

Bevor Sie eine Migration oder eine Hypervisor-Wartung durchführen, müssen Sie die Nodes ordnungsgemäß herunterfahren. Siehe Anweisungen für "[Herunterfahren eines Grid-Node](#)".

VMware Live Migration wird nicht unterstützt

OpenStack Live Migration und VMware Live vMotion sorgen dafür, dass die Uhr der Virtual Machine sprunghaft Zeit anspringt und werden für Grid-Nodes unabhängig vom Typ nicht unterstützt. Obwohl selten, falsche Uhrzeiten können zum Verlust von Daten oder Konfigurations-Updates führen.

Cold-Migration wird unterstützt. Bei der „Cold“-Migration sollten Sie die StorageGRID Nodes herunterfahren, bevor Sie sie zwischen Hosts migrieren. Siehe Anweisungen für ["Herunterfahren eines Grid-Node"](#).

Konsistente Namen von Netzwerkschnittstellen

Um einen Knoten von einem Host auf einen anderen zu verschieben, muss der StorageGRID-Hostdienst darauf vertrauen können, dass die externe Netzwerkverbindung, die der Knoten am aktuellen Standort hat, am neuen Standort dupliziert werden kann. Dies schafft Vertrauen durch die Verwendung konsistenter Netzwerk-Interface-Namen in den Hosts.

Angenommen, beispielsweise, dass StorageGRID NodeA, der auf Host1 ausgeführt wird, mit den folgenden Schnittstellenzuordnungen konfiguriert wurde:

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

Die linke Seite der Pfeile entspricht den traditionellen Schnittstellen, die aus einem StorageGRID-Container betrachtet werden (das sind die Grid-, Administrator- und Client-Netzwerk-Schnittstellen). Die rechte Seite der Pfeile entspricht den tatsächlichen Host-Schnittstellen, die diese Netzwerke bereitstellen. Dabei handelt es sich um drei VLAN-Schnittstellen, die derselben physischen Interface-Verbindung untergeordnet sind.

Nehmen Sie an, Sie möchten NodeA zu Host2 migrieren. Wenn Host2 auch Schnittstellen mit den Namen bond0.1001, bond0.1002 und bond0.1003 besitzt, ermöglicht das System die Verschiebung, vorausgesetzt, dass die „Gefällt mir“-Schnittstellen auf Host2 die gleiche Konnektivität wie auf Host1 bereitstellen. Wenn Host2 keine Schnittstellen mit demselben Namen hat, ist die Verschiebung nicht zulässig.

Es gibt viele Möglichkeiten, eine konsistente Netzwerkschnittstelle über mehrere Hosts hinweg zu benennen; siehe ["Konfigurieren des Hostnetzwerks"](#) Für einige Beispiele.

Shared Storage

Für schnelle Node-Migrationen mit geringem Overhead werden Node-Daten mit der StorageGRID Node-Migrationsfunktion nicht physisch verschoben. Stattdessen werden die Node-Migration als Export- und Importpaar durchgeführt:

1. Während des Vorgangs „Node Export“ wird eine kleine Menge von persistenten Zustandsdaten aus dem Node-Container extrahiert, der auf HostA ausgeführt wird und auf dem Systemdatenvolumen dieses Node zwischengespeichert wird. Anschließend wird der Knoten-Container auf HostA deaktiviert.
2. Während des Vorgangs „Node Import“ wird der Node-Container auf HostB, der die gleiche Netzwerkschnittstelle und die Blockspeicherzuordnungen verwendet, die auf HostA wirksam waren, instanziiert. Anschließend werden die im Cache gespeicherten Persistent State-Daten in die neue Instanz eingefügt.

In Anbetracht dieses Betriebsmodus müssen alle Systemdaten und Objekt-Storage-Volumes des Node sowohl von HostA als auch von HostB aus zugänglich sein, damit die Migration erlaubt und ausgeführt werden kann. Außerdem müssen sie auf dem Knoten mit Namen abgebildet worden sein, die garantiert auf die gleichen LUNs auf HostA und HostB verweisen.

Das folgende Beispiel zeigt eine Lösung für die Zuordnung von Blockgeräten für einen StorageGRID-Speicherknoten, bei dem auf den Hosts DM-Multipathing verwendet wird und in das Alias-Feld verwendet wurde `/etc/multipath.conf` Um konsistente, freundliche Blockgerätenamen zu liefern, die auf allen Hosts verfügbar sind.

```
/var/local  ───>  /dev/mapper/sgws-sn1-var-local
rangedb0    ───>  /dev/mapper/sgws-sn1-rangedb0
rangedb1    ───>  /dev/mapper/sgws-sn1-rangedb1
rangedb2    ───>  /dev/mapper/sgws-sn1-rangedb2
rangedb3    ───>  /dev/mapper/sgws-sn1-rangedb3
```

Implementierungstools

Sie profitieren möglicherweise von der Automatisierung der gesamten StorageGRID Installation oder eines Teils.

Eine Automatisierung der Implementierung kann in einem der folgenden Fälle von Nutzen sein:

- Sie verwenden bereits ein Standard-Orchestrierungs-Framework wie Ansible, Puppet oder Chef für die Implementierung und Konfiguration physischer oder virtueller Hosts.
- Sie beabsichtigen, mehrere StorageGRID Instanzen zu implementieren.
- Sie implementieren eine große, komplexe StorageGRID Instanz.

Der StorageGRID Host Service wird durch ein Paket installiert und unterstützt durch Konfigurationsdateien, die während einer manuellen Installation interaktiv erstellt oder vorab (oder programmgesteuert) vorbereitet werden können, um eine automatisierte Installation mithilfe von Standard-Orchestrierungs-Frameworks zu ermöglichen. StorageGRID bietet optionale Python-Skripte zur Automatisierung der Konfiguration von StorageGRID Appliances und dem gesamten StorageGRID-System (das „Grid“). Sie können diese Skripte direkt verwenden, oder Sie können sie überprüfen, um zu erfahren, wie Sie die verwenden "[REST-API für die StorageGRID Installation](#)" In den Grid-Implementierungs- und Konfigurations-Tools entwickeln Sie sich selbst.

Wenn Sie an der Automatisierung Ihrer gesamten StorageGRID-Implementierung oder eines Teils interessiert sind, lesen Sie die Seite "[Automatisieren Sie die Installation](#)" Vor Beginn des Installationsprozesses.

Vorbereiten der Hosts (Red hat oder CentOS)

Wie sich die Host-weiten Einstellungen während der Installation ändern

Auf Bare Metal-Systemen nimmt StorageGRID einige Änderungen am gesamten Host

vor sysctl Einstellungen.

Folgende Änderungen wurden 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 RAM
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 Linux auf allen Grid-Hosts installieren. Verwenden Sie die ["NetApp Interoperabilitäts-Matrix-Tool"](#) Um eine Liste der unterstützten Versionen zu erhalten.



Stellen Sie sicher, dass Ihr Betriebssystem auf Linux Kernel 4.15 oder höher aktualisiert wird.

Schritte

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



Bei Verwendung des Linux Standard-Installationsprogramms empfiehlt NetApp die Auswahl der Basiskonfiguration „Compute Node“, sofern verfügbar, oder der Basisumgebung „minimal install“. Installieren Sie keine grafischen Desktop-Umgebungen.

2. Stellen Sie sicher, dass alle Hosts Zugriff auf Paket-Repositoryys 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 zu erhalten.



Wenn Sie den Auslagerungsaustausch nicht vollständig deaktivieren, kann die Leistung erheblich gesenkt werden.

Konfiguration des Host-Netzwerks (Red hat Enterprise Linux oder CentOS)

Nach dem Abschluss der Linux-Installation auf Ihren Hosts müssen Sie möglicherweise eine zusätzliche Konfiguration durchführen, um auf jedem Host eine Reihe von Netzwerkschnittstellen vorzubereiten, die sich für die Zuordnung zu den später zu implementierenden StorageGRID Nodes eignen.

Bevor Sie beginnen

- Sie haben die geprüft ["StorageGRID Netzwerkrichtlinien"](#).
- Sie haben die Informationen zu überprüft ["Anforderungen für die Container-Migration für Nodes"](#).
- Wenn Sie virtuelle Hosts verwenden, haben Sie die gelesen [Überlegungen und Empfehlungen zum Klonen von MAC-Adressen](#) Vor dem Konfigurieren des Hostnetzwerks.



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

Über diese Aufgabe

Grid-Nodes müssen auf das Grid-Netzwerk und optional auf Admin- und Client-Netzwerke zugreifen können. Sie ermöglichen diesen Zugriff, indem Sie Zuordnungen erstellen, die die physische Schnittstelle des Hosts den virtuellen Schnittstellen für jeden Grid-Node zuordnen. Verwenden Sie bei der Erstellung von Host-Schnittstellen benutzerfreundliche Namen, um die Implementierung über alle Hosts hinweg zu vereinfachen und die Migration zu ermöglichen.

Die gleiche Schnittstelle kann von dem Host und einem oder mehreren Nodes gemeinsam genutzt werden. Beispielsweise können Sie für den Hostzugriff und den Netzwerkzugriff von Node-Admin dieselbe Schnittstelle verwenden, um die Wartung von Hosts und Nodes zu vereinfachen. Obwohl dieselbe Schnittstelle zwischen dem Host und den einzelnen Nodes gemeinsam genutzt werden kann, müssen alle unterschiedliche IP-Adressen haben. IP-Adressen können nicht zwischen Nodes oder zwischen dem Host und einem beliebigen Node gemeinsam genutzt 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 etwas dazwischen tun. Normalerweise würden Sie jedoch nicht die

gleiche Hostnetzwerkschnittstelle bereitstellen wie die Grid- und Admin-Netzwerkschnittstellen für einen einzelnen Knoten oder als Grid-Netzwerkschnittstelle für einen Knoten und die Client-Netzwerkschnittstelle für einen anderen.

Sie können diese Aufgabe auf unterschiedliche Weise ausführen. Wenn es sich bei Ihren Hosts beispielsweise um virtuelle Maschinen handelt und Sie für jeden Host einen oder zwei StorageGRID-Nodes bereitstellen, können Sie die korrekte Anzahl an Netzwerkschnittstellen im Hypervisor erstellen und eine 1:1-Zuordnung verwenden. Wenn Sie mehrere Nodes auf Bare-Metal-Hosts für die Produktion implementieren, können Sie die Unterstützung des Linux-Netzwerk-Stacks für VLAN und LACP nutzen, um Fehlertoleranz und Bandbreitenfreigabe zu erhalten. Die folgenden Abschnitte enthalten detaillierte Ansätze für beide Beispiele. Sie müssen keines dieser Beispiele verwenden; Sie können jeden Ansatz verwenden, der Ihren Anforderungen entspricht.



Verwenden Sie keine Bond- oder Bridge-Geräte direkt als Container-Netzwerkschnittstelle. Dies könnte den Anlauf eines Knotens verhindern, der durch ein Kernel-Problem verursacht wurde, indem MACLAN mit Bond- und Bridge-Geräten im Container-Namespaces verwendet wird. Verwenden Sie stattdessen ein Gerät ohne Bindung, z. B. ein VLAN- oder ein virtuelles Ethernet-Paar (veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Node-Konfigurationsdatei an.

Verwandte Informationen

["Erstellen von Knoten-Konfigurationsdateien"](#)

Überlegungen und Empfehlungen zum Klonen von MAC-Adressen

Das Klonen VON MAC-Adressen bewirkt, dass der Container die MAC-Adresse des Hosts verwendet und der Host die MAC-Adresse entweder einer von Ihnen angegebenen oder einer zufällig generierten Adresse verwendet. Verwenden Sie das Klonen von MAC-Adressen, um Netzwerkkonfigurationen im einfach zu vermeiden.

Aktivieren des MAC-Klonens

In bestimmten Umgebungen kann die Sicherheit durch das Klonen von MAC-Adressen erhöht werden, da es Ihnen ermöglicht, eine dedizierte virtuelle NIC für das Admin-Netzwerk, das Grid-Netzwerk und das Client-Netzwerk zu verwenden. Wenn der Container die MAC-Adresse der dedizierten NIC auf dem Host nutzen soll, können Sie keine Kompromissmodus-Netzwerkkonfigurationen mehr verwenden.



Das Klonen DER MAC-Adresse wurde für Installationen virtueller Server entwickelt und funktioniert möglicherweise nicht ordnungsgemäß bei allen Konfigurationen der physischen Appliance.



Wenn ein Knoten nicht gestartet werden kann, weil eine gezielte Schnittstelle für das MAC-Klonen belegt ist, müssen Sie die Verbindung möglicherweise auf „down“ setzen, bevor Sie den Knoten starten. Darüber hinaus kann es vorkommen, dass die virtuelle Umgebung das Klonen von MAC auf einer Netzwerkschnittstelle verhindert, während der Link aktiv ist. Wenn ein Knoten die MAC-Adresse nicht einstellt und aufgrund einer überlasteten Schnittstelle gestartet wird, kann das Problem durch Setzen des Links auf „down“ vor dem Starten des Knotens behoben werden.

Das Klonen VON MAC-Adressen ist standardmäßig deaktiviert und muss durch Knoten-Konfigurationsschlüssel festgelegt werden. Sie sollten die Aktivierung bei der Installation von StorageGRID aktivieren.

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 NIC des Hosts. Außerdem verwendet der Host dann die MAC-Adresse des angegebenen Containernetzwerks. Standardmäßig ist die Container-Adresse eine zufällig generierte Adresse, jedoch wenn Sie mithilfe des eine Adresse festgelegt haben `_NETWORK_MAC` Der Node-Konfigurationsschlüssel, diese Adresse wird stattdessen verwendet. Host und Container haben immer unterschiedliche MAC-Adressen.



Wenn das MAC-Klonen auf einem virtuellen Host aktiviert wird, ohne dass gleichzeitig der einfach austauschbare Modus auf dem Hypervisor aktiviert werden muss, kann dies dazu führen, dass Linux-Host-Netzwerke, die die Host-Schnittstelle verwenden, nicht mehr funktionieren.

Anwendungsfälle für DAS Klonen VON MAC

Es gibt zwei Anwendungsfälle, die beim Klonen von MAC berücksichtigt werden müssen:

- MAC-Klonen nicht aktiviert: Wenn der `_CLONE_MAC` Der Schlüssel in der Node-Konfigurationsdatei ist nicht festgelegt oder auf „false“ gesetzt. Der Host verwendet die Host-NIC-MAC und der Container verfügt über eine von StorageGRID generierte MAC, sofern im keine MAC angegeben ist `_NETWORK_MAC` Taste. Wenn im eine Adresse festgelegt ist `_NETWORK_MAC` Schlüssel, der Container wird die Adresse im angegeben `_NETWORK_MAC` Taste. Diese Schlüsselkonfiguration erfordert den Einsatz des promiskuitiven Modus.
- MAC-Klonen aktiviert: Wenn der `_CLONE_MAC` Schlüssel in der Node-Konfigurationsdatei ist auf „true“ gesetzt, der Container verwendet die Host-NIC MAC und der Host verwendet eine von StorageGRID generierte MAC, es sei denn, eine MAC wird im angegeben `_NETWORK_MAC` Taste. Wenn im eine Adresse festgelegt ist `_NETWORK_MAC` Schlüssel, der Host verwendet die angegebene Adresse anstelle einer generierten. In dieser Konfiguration von Schlüsseln sollten Sie nicht den promiskuous Modus verwenden.



Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen erlauben möchten, Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen zu empfangen und zu übertragen, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppen für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen auf **Accept** gesetzt sind. Die auf dem virtuellen Switch eingestellten Werte können von den Werten auf der Portgruppenebene außer Kraft gesetzt werden. Stellen Sie also sicher, dass die Einstellungen an beiden Stellen identisch sind.

Informationen zum Aktivieren des MAC-Klonens finden Sie im ["Anweisungen zum Erstellen von Node-Konfigurationsdateien"](#).

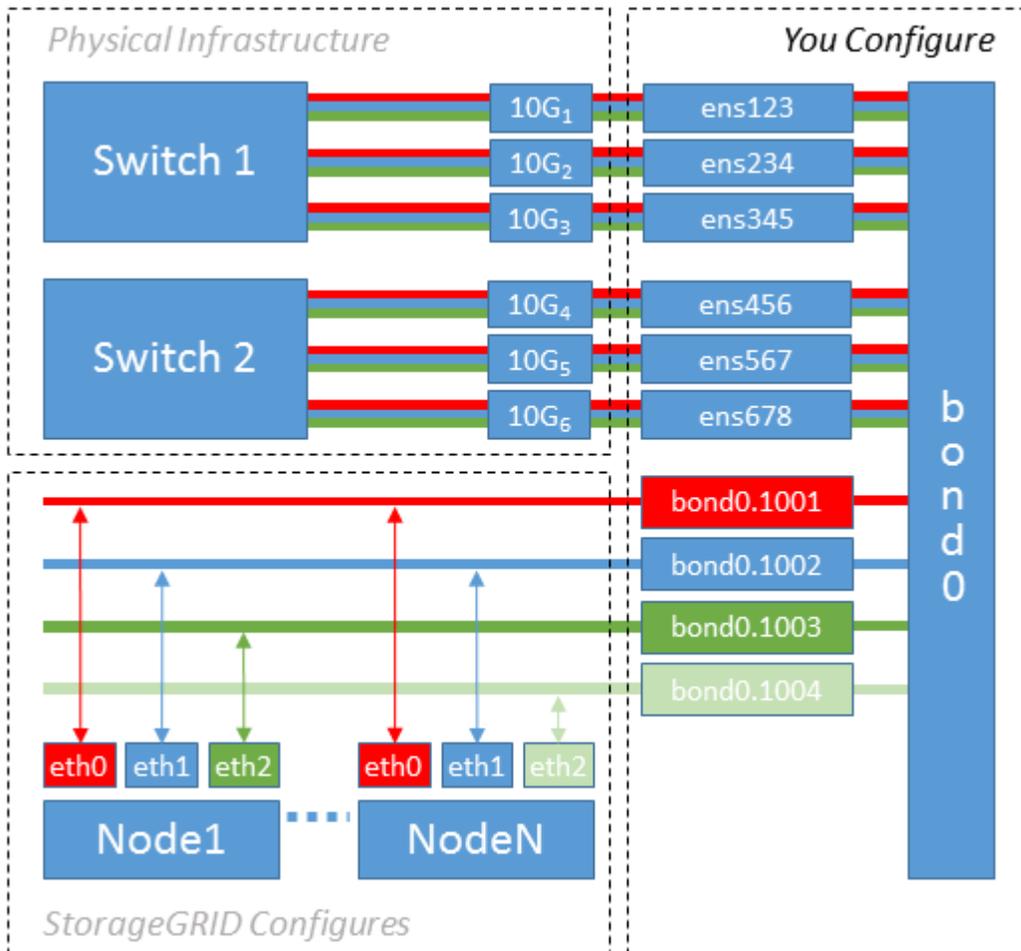
BEISPIEL FÜR DAS Klonen VON MAC

Beispiel für das MAC-Klonen bei einem Host mit einer MAC-Adresse von 11:22:33:44:55:66 für die Schnittstelle `ens256` und die folgenden Schlüssel in der Node-Konfigurationsdatei:

- ADMIN_NETWORK_TARGET = ens256

Um dieses Beispiel zu verstehen, stellen Sie vor, Sie verfügen über drei separate Subnetze für Grid, Admin und Client-Netzwerke in jedem Rechenzentrum. Die Subnetze sind in getrennten VLANs (1001, 1002 und 1003) angesiedelt und werden dem Host auf einem LACP-gebundenen Trunk-Port (bond0) präsentiert. Sie würden drei VLAN-Schnittstellen auf der Verbindung konfigurieren: Bond0.1001, bond0.1002 und bond0.1003.

Wenn für Node-Netzwerke auf demselben Host separate VLANs und Subnetze erforderlich sind, können Sie auf der Verbindung VLAN-Schnittstellen hinzufügen und sie dem Host zuordnen (in der Abbildung als bond0.1004 dargestellt).



Schritte

1. Aggregieren Sie alle physischen Netzwerkschnittstellen, die für die StorageGRID-Netzwerkverbindung in einer einzigen LACP-Verbindung verwendet werden.

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

2. Erstellen Sie VLAN-Schnittstellen, die diese Verbindung als ihr zugehöriges „physisches Gerät verwenden,“ using the standard VLAN interface naming convention `physdev-name.VLAN ID`.

Beachten Sie, dass für die Schritte 1 und 2 eine entsprechende Konfiguration an den Edge-Switches erforderlich ist, die die anderen Enden der Netzwerkverbindungen beenden. Die Edge-Switch-Ports müssen auch zu LACP-Port-Kanälen aggregiert, als Trunk konfiguriert und alle erforderlichen VLANs übergeben werden können.

Beispiele für Schnittstellenkonfigurationsdateien für dieses Netzwerkkonfigurationsschema pro Host

werden bereitgestellt.

Verwandte Informationen

["Beispiel /etc/sysconfig/Network-scripts"](#)

Hostspeicher konfigurieren

Jedem Host müssen Block Storage Volumes zugewiesen werden.

Bevor Sie beginnen

Sie haben die folgenden Themen behandelt, die Ihnen Informationen liefern, die Sie für diese Aufgabe benötigen:

["Storage- und Performance-Anforderungen erfüllt"](#)

["Anforderungen für die Container-Migration für Nodes"](#)

Über diese Aufgabe

Bei der Zuweisung von Block Storage Volumes (LUNs) an Hosts können Sie mithilfe der Tabellen unter „Storage-Anforderungen“ Folgendes ermitteln:

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

Sie verwenden diese Informationen sowie den permanenten Namen, der Linux jedem physischen Volume zugewiesen ist, wenn Sie StorageGRID-Nodes auf dem Host implementieren.



Sie müssen diese Volumes nicht partitionieren, formatieren oder mounten, sondern müssen nur sicherstellen, dass sie für die Hosts sichtbar sind.

Vermeiden Sie die Verwendung von „RAW“-speziellen Gerätedateien (`/dev/sdb`, Zum Beispiel) bei der Zusammenstellung Ihrer Liste von Volume-Namen. Diese Dateien können sich bei einem Neustart des Hosts ändern, was sich auf den ordnungsgemäßen Betrieb des Systems auswirkt. Wenn Sie iSCSI-LUNs und Device Mapper Multipathing verwenden, sollten Sie in der Multipath-Aliase verwenden `/dev/mapper` Verzeichnis, insbesondere wenn Ihre SAN-Topologie redundante Netzwerkpfade zu dem gemeinsam genutzten Storage umfasst. Alternativ können Sie die vom System erstellten Softlinks unter verwenden `/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 unterscheiden sich bei jeder Installation.

Zuweisung freundlicher Namen zu jedem dieser Block-Storage-Volumes zur Vereinfachung der Erstinstallation von StorageGRID und zukünftiger Wartungsarbeiten Wenn Sie den Device Mapper Multipath-Treiber für redundanten Zugriff auf gemeinsam genutzte Speicher-Volumes verwenden, können Sie das verwenden `alias` Feld in Ihrem `/etc/multipath.conf` Datei:

Beispiel:

```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

Dadurch werden die Aliase im als Blockgeräte angezeigt `/dev/mapper` Verzeichnis auf dem Host, mit dem Sie einen freundlichen, einfach validierten Namen angeben können, wenn bei einer Konfiguration oder Wartung ein Block-Speicher-Volume angegeben werden muss.



Wenn Sie gemeinsam genutzten Speicher zur Unterstützung der StorageGRID-Node-Migration einrichten und Device Mapper Multipathing verwenden, können Sie ein Common erstellen und installieren `/etc/multipath.conf` Auf allen zusammengehörige Hosts. Stellen Sie einfach sicher, dass Sie auf jedem Host einen anderen Container-Engine-Storage-Volume verwenden. Die Verwendung von Aliases und das Einschließen des Ziel-Hostnamen in den Alias für jede Container-Engine Speicher-Volume LUN wird dies leicht zu merken machen und empfohlen.

Verwandte Informationen

["Konfigurieren des Container Engine Storage Volume"](#)

Konfigurieren des Container Engine Storage Volume

Vor der Installation der Container-Engine (Docker oder Podman) müssen Sie möglicherweise das Storage-Volume formatieren und mounten.

Über diese Aufgabe

Diese Schritte können sie überspringen, wenn Sie einen lokalen Speicher für das Docker oder Podman Storage Volume verwenden möchten und genügend Speicherplatz auf der Host-Partition mit zur Verfügung steht `/var/lib/docker` Für Docker und `/var/lib/containers` Für Podman.



Podman wird nur auf Red hat Enterprise Linux (RHEL) unterstützt.

Schritte

1. Dateisystem auf dem Container-Engine-Storage-Volume erstellen:

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

2. Mounten des Container-Engine-Storage-Volumes:

- 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.

Mit diesem Schritt wird sichergestellt, dass das Storage Volume nach einem Neustart des Hosts automatisch neu eingebunden wird.

Installation Von Docker

Das StorageGRID System läuft unter Red hat Enterprise Linux oder CentOS als Sammlung von Containern. Wenn Sie sich für die Verwendung der Docker Container-Engine entschieden haben, führen Sie die folgenden Schritte aus, um Docker zu installieren. Andernfalls [Installieren Sie Podman](#).

Schritte

1. Installieren Sie Docker gemäß den Anweisungen für Ihre Linux-Distribution.



Wenn Docker nicht in Ihrer Linux Distribution enthalten ist, können Sie sie über die Docker Website herunterladen.

2. Vergewissern Sie sich, dass Docker aktiviert und gestartet wurde, indem Sie die folgenden beiden Befehle

ausführen:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

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

```
sudo docker version
```

Die Client- und Server-Versionen müssen 1.11.0 oder höher sein.

Installieren Sie Podman

Das StorageGRID-System läuft unter Red hat Enterprise Linux als eine Sammlung von Containern. Wenn Sie sich für die Verwendung der Podman Container-Engine entschieden haben, befolgen Sie diese Schritte, um Podman zu installieren. Andernfalls [Installation von Docker](#).



Podman wird nur auf Red hat Enterprise Linux (RHEL) unterstützt.

Schritte

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



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

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

```
sudo docker version
```



Das Podman-Docker Paket ermöglicht die Verwendung von Docker Befehlen.

Die Client- und Server-Versionen 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
```

Installation der StorageGRID Host Services

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

Über diese Aufgabe

In diesen Anweisungen wird beschrieben, wie die Host-Services aus den RPM-Paketen installiert werden. Alternativ können Sie die im Installationarchiv enthaltenen Yum Repository-Metadaten verwenden, um die RPM-Pakete Remote zu installieren. Weitere Informationen zu Ihrem Linux-Betriebssystem finden Sie in der Yum-Repository-Anleitung.

Schritte

1. Kopieren Sie die StorageGRID RPM-Pakete auf jeden Ihrer Hosts, oder stellen Sie sie auf Shared Storage zur Verfügung.

Legen Sie sie zum Beispiel in die `/tmp` Verzeichnis, damit 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 yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-  
version-SHA.rpm
```

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



Sie müssen zunächst das Bilderpaket und das Servicepaket als zweites installieren.



Wenn Sie die Pakete in einem anderen Verzeichnis als platziert haben `/tmp`, Ändern Sie den Befehl, um den von Ihnen verwendeten Pfad anzuzeigen.

Implementierung von virtuellen Grid-Nodes (Red hat oder CentOS)

Erstellen von Node-Konfigurationsdateien für Red hat Enterprise Linux oder CentOS Implementierungen

Konfigurationsdateien für die Nodes sind kleine Textdateien, die die Informationen liefern, die der StorageGRID-Host-Service benötigt, um einen Node zu starten und eine Verbindung zu den entsprechenden Netzwerk- und Block-Storage-Ressourcen herzustellen. Node-Konfigurationsdateien werden für virtuelle Nodes verwendet und nicht für Appliance-Nodes verwendet.

Wo lege ich die Knoten-Konfigurationsdateien ab?

Sie müssen die Konfigurationsdatei für jeden StorageGRID-Knoten im platzieren `/etc/storagegrid/nodes` Verzeichnis auf dem Host, auf dem der Knoten ausgeführt wird. Wenn Sie beispielsweise einen Admin-Node,

einen Gateway-Node und einen Storage-Node auf Hosta ausführen möchten, müssen Sie die Konfigurationsdateien mit drei Knoten in die Datei legen `/etc/storagegrid/nodes` Auf Hosta. Sie können die Konfigurationsdateien direkt auf jedem Host mit einem Texteditor, wie z. B. vim oder nano, erstellen oder sie an einem anderen Ort erstellen und auf jeden Host verschieben.

Was benenne ich die Node-Konfigurationsdateien?

Die Namen der Konfigurationsdateien sind erheblich. Das Format lautet `node-name.conf`, Wo `node-name` Ist ein Name, den Sie dem Node zuweisen. Dieser Name wird im StorageGRID Installer angezeigt und wird für Knotenwartungsvorgänge, z. B. für Node-Migration, verwendet.

Node-Namen müssen folgende Bedingungen erfüllen:

- Muss eindeutig sein
- Nur mit einem Buchstaben beginnen
- Kann die Zeichen A bis Z und a bis z enthalten
- Kann die Zahlen 0 bis 9 enthalten
- Kann eine oder mehrere Bindestriche enthalten (-)
- Darf nicht mehr als 32 Zeichen enthalten, wobei der nicht enthalten ist `.conf` Erweiterung

Alle Dateien in `/etc/storagegrid/nodes` Die diese Namenskonventionen nicht befolgen, werden vom Host Service nicht geparkt.

Wenn das Grid eine Topologie mit mehreren Standorten geplant ist, ist unter Umständen ein typisches Benennungsschema für Node möglich:

```
site-nodetype-nodenummer.conf
```

Beispielsweise können Sie verwenden `dc1-adm1.conf` Für den ersten Admin-Node in Data Center 1 und `dc2-sn3.conf` Für den dritten Storage-Node in Datacenter 2. Sie können jedoch ein beliebiges Schema verwenden, das Sie mögen, solange alle Knotennamen den Benennungsregeln folgen.

Was befindet sich in einer Node-Konfigurationsdatei?

Die Konfigurationsdateien enthalten Schlüssel-/Wertpaare mit einem Schlüssel und einem Wert pro Zeile. Für jedes Schlüssel-/Wertpaar müssen Sie folgende Regeln einhalten:

- Der Schlüssel und der Wert müssen durch ein Gleichheitszeichen getrennt werden (=) Und optional Whitespace.
- Die Schlüssel können keine Leerzeichen enthalten.
- Die Werte können eingebettete Leerzeichen enthalten.
- Führende oder nachgestellte Leerzeichen werden ignoriert.

Einige Schlüssel sind für jeden Knoten erforderlich, während andere optional sind oder nur für bestimmte Node-Typen erforderlich sind.

Die Tabelle definiert die zulässigen Werte für alle unterstützten Schlüssel. In der mittleren Spalte:

R: Erforderlich + **BP:** Best Practice + **O:** Optional

Taste	R, BP ODER O?	Wert
ADMIN_IP	BP	<p>Grid Network IPv4-Adresse des primären Admin-Knotens für das Grid, zu dem dieser Node gehört. Verwenden Sie denselben Wert, den Sie für GRID_NETWORK_IP für den Grid-Node mit NODE_TYPE = VM_Admin_Node und ADMIN_ROLE = Primary angegeben haben. Wenn Sie diesen Parameter nicht angeben, versucht der Node, einen primären Admin-Node mit mDNS zu ermitteln.</p> <p>"Ermitteln der primären Admin-Node durch Grid-Nodes"</p> <p>Hinweis: Dieser Wert wird auf dem primären Admin-Node ignoriert und kann möglicherweise nicht verwendet werden.</p>
ADMIN_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT
ADMIN_NETWORK_ESL	O	<p>Kommagetrennte Liste von Subnetzen in CIDR-Notation, mit denen dieser Knoten über das Admin-Netzwerk-Gateway kommunizieren soll.</p> <p>Beispiel: 172.16.0.0/21,172.17.0.0/21</p>
ADMIN_NETWORK_GATEWAY	O (R)	<p>IPv4-Adresse des lokalen Admin-Netzwerk-Gateways für diesen Node. Muss sich im Subnetz befinden, das von ADMIN_NETWORK_IP und ADMIN_NETWORK_MASKE definiert ist. Dieser Wert wird bei DHCP-konfigurierten Netzwerken ignoriert.</p> <p>Hinweis: Dieser Parameter ist erforderlich, wenn ADMIN_NETWORK_ESL angegeben wird.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>
ADMIN_NETWORK_IP	O	<p>IPv4-Adresse dieses Knotens im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_MAC	O	<p>Die MAC-Adresse für die Admin-Netzwerkschnittstelle im Container.</p> <p>Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert.</p> <p>Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden.</p> <p>Beispiel: b2:9c:02:c2:27:10</p>
ADMIN_NETWORK_MASKE	O	<p>IPv4-Netmask für diesen Node im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>255.255.255.0</p> <p>255.255.248.0</p>
ADMIN_NETWORK_MTU	O	<p>Die maximale Übertragungseinheit (MTU) für diesen Knoten im Admin-Netzwerk. Geben Sie nicht an, ob ADMIN_NETWORK_CONFIG = DHCP. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 verwendet.</p> <p>Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei.</p> <p>WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, an den der Knoten angeschlossen ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.</p> <p>Beispiele:</p> <p>1500</p> <p>8192</p>

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_TARGET	BP	<p>Name des Host-Geräts, das Sie für den Administratornetzwerkzugriff durch den StorageGRID-Knoten verwenden werden. Es werden nur Namen von Netzwerkschnittstellen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den für GRID_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegebenen Namen.</p> <p>Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät oder verwenden Sie ein Bridge- und virtuelles Ethernet-Paar (veth).</p> <p>Best Practice: Geben Sie einen Wert an, selbst wenn dieser Knoten zunächst keine Admin-Netzwerk-IP-Adresse hat. Anschließend können Sie später eine Admin-Netzwerk-IP-Adresse hinzufügen, ohne den Node auf dem Host neu konfigurieren zu müssen.</p> <p>Beispiele:</p> <p>bond0.1002</p> <p>ens256</p>
ADMIN_NETWORK_TARGET_TYPE	O	<p>Schnittstelle</p> <p>(Dies ist der einzige unterstützte Wert.)</p>
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	<p>Richtig oder falsch</p> <p>Setzen Sie den Schlüssel auf „true“, damit der StorageGRID-Container die MAC-Adresse der Host-Zielschnittstelle im Admin-Netzwerk verwendet.</p> <p>Best Practice: in Netzwerken, in denen der promiskuios-Modus erforderlich wäre, verwenden Sie stattdessen DEN ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel.</p> <p>Weitere Informationen zum Klonen von MAC:</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red hat Enterprise Linux oder CentOS)"</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"</p>

Taste	R, BP ODER O?	Wert
ADMIN_ROLLE	R	<p>Primärer oder nicht primärer Storage</p> <p>Dieser Schlüssel ist nur erforderlich, wenn NODE_TYPE = VM_Admin_Node; geben Sie ihn nicht für andere Node-Typen an.</p>
BLOCK_DEVICE_AUDIT_LOGS	R	<p>Pfad und Name der Sonderdatei für Blockgeräte, die dieser Node für die persistente Speicherung von Prüfprotokollen verwendet. Dieser Schlüssel ist nur für Nodes mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an.</p> <p>Beispiele:</p> <pre data-bbox="719 682 1388 924">/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</pre>

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_RANGEDB_000	R	Pfad und Name der Sonderdatei für das Blockgerät wird dieser Node für den persistenten Objekt-Storage verwenden. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Storage_Node erforderlich; geben Sie ihn nicht für andere Knotentypen an.
BLOCK_DEVICE_RANGEDB_001		
BLOCK_DEVICE_RANGEDB_002		Es ist nur BLOCK_DEVICE_RANGEDB_000 erforderlich; der Rest ist optional. Das für BLOCK_DEVICE_RANGEDB_000 angegebene Blockgerät muss mindestens 4 TB betragen; die anderen können kleiner sein.
BLOCK_DEVICE_RANGEDB_003		
BLOCK_DEVICE_RANGEDB_004		Lassen Sie keine Lücken. Wenn Sie BLOCK_DEVICE_RANGEDB_005 angeben, müssen Sie auch BLOCK_DEVICE_RANGEDB_004 angeben.
BLOCK_DEVICE_RANGEDB_005		Hinweis: Zur Kompatibilität mit bestehenden Bereitstellungen werden zweistellige Schlüssel für aktualisierte Knoten unterstützt.
BLOCK_DEVICE_RANGEDB_006		Beispiele:
BLOCK_DEVICE_RANGEDB_007		<code>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</code>
BLOCK_DEVICE_RANGEDB_008		<code>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</code>
BLOCK_DEVICE_RANGEDB_009		<code>/dev/mapper/sgws-sn1-rangedb-000</code>
BLOCK_DEVICE_RANGEDB_010		
BLOCK_DEVICE_RANGEDB_011		
BLOCK_DEVICE_RANGEDB_012		
BLOCK_DEVICE_RANGEDB_013		
BLOCK_DEVICE_RANGEDB_014		
BLOCK_DEVICE_RANGEDB_015		

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_TABLES	R	<p>Pfad und Name der Sonderdatei des Blockgerätes, die dieser Knoten für die dauerhafte Speicherung von Datenbanktabellen verwendet. Dieser Schlüssel ist nur für Nodes mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an.</p> <p>Beispiele:</p> <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adm1-tables</pre>
BLOCK_DEVICE_VAR_LOCAL	R	<p>Pfad und Name der Sonderdatei für das Blockgerät wird dieser Node für seinen persistenten Speicher /var/local verwenden.</p> <p>Beispiele:</p> <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-var-local</pre>
CLIENT_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT
CLIENT_NETWORK_GATEWAY	O	<p>IPv4-Adresse des lokalen Client-Netzwerk-Gateways für diesen Node, der sich im Subnetz befinden muss, das durch CLIENT_NETWORK_IP und CLIENT_NETWORK_MASK definiert ist. Dieser Wert wird bei DHCP-konfigurierten Netzwerken ignoriert.</p> <p>Beispiele:</p> <pre>1.1.1.1</pre> <pre>10.224.4.81</pre>

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_IP	O	<p>IPv4-Adresse dieses Knotens im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>
CLIENT_NETWORK_MAC	O	<p>Die MAC-Adresse für die Client-Netzwerkschnittstelle im Container.</p> <p>Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert.</p> <p>Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden.</p> <p>Beispiel: b2:9c:02:c2:27:20</p>
CLIENT_NETWORK_MASK	O	<p>IPv4-Netzmaske für diesen Knoten im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>255.255.255.0</p> <p>255.255.248.0</p>

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_MTU	O	<p>Die maximale Übertragungseinheit (MTU) für diesen Knoten im Client-Netzwerk. Geben Sie nicht an, ob CLIENT_NETWORK_CONFIG = DHCP. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 verwendet.</p> <p>Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei.</p> <p>WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, an den der Knoten angeschlossen ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.</p> <p>Beispiele:</p> <p>1500</p> <p>8192</p>
CLIENT_NETWORK_TARGET	BP	<p>Name des Host-Geräts, das Sie für den Zugriff auf das Client-Netzwerk durch den StorageGRID-Knoten verwenden werden. Es werden nur Namen von Netzwerkschnittstellen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als der für GRID_NETWORK_TARGET oder ADMIN_NETWORK_TARGET angegeben wurde.</p> <p>Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät oder verwenden Sie ein Bridge- und virtuelles Ethernet-Paar (veth).</p> <p>Best Practice: Geben Sie einen Wert an, auch wenn dieser Knoten zunächst keine Client Network IP Adresse hat. Anschließend können Sie später eine Client-Netzwerk-IP-Adresse hinzufügen, ohne den Node auf dem Host neu konfigurieren zu müssen.</p> <p>Beispiele:</p> <p>bond0.1003</p> <p>ens423</p>
CLIENT_NETWORK_TARGET_TYPE	O	<p>Schnittstelle</p> <p>(Dieser Wert wird nur unterstützt.)</p>

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	<p>Richtig oder falsch</p> <p>Setzen Sie den Schlüssel auf „true“, damit der StorageGRID-Container die MAC-Adresse der Host-Zielschnittstelle im Client-Netzwerk verwenden kann.</p> <p>Best Practice: in Netzwerken, in denen der promiskuios-Modus erforderlich wäre, verwenden Sie stattdessen DEN CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel.</p> <p>Weitere Informationen zum Klonen von MAC:</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red hat Enterprise Linux oder CentOS)"</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"</p>
GRID_NETWORK_CONFIG	BP	<p>STATISCH oder DHCP</p> <p>(Ist standardmäßig STATISCH, wenn nicht angegeben.)</p>
GRID_NETWORK_GATEWAY	R	<p>IPv4-Adresse des lokalen Grid-Netzwerk-Gateways für diesen Node, der sich im Subnetz befinden muss, das durch GRID_NETWORK_IP und GRID_NETWORK_MASKE definiert ist. Dieser Wert wird bei DHCP-konfigurierten Netzwerken ignoriert.</p> <p>Wenn das Grid-Netzwerk ein einzelnes Subnetz ohne Gateway ist, verwenden Sie entweder die Standard-Gateway-Adresse für das Subnetz (X.Z.1) oder den GRID_NETWORK_IP-Wert dieses Knotens; jeder Wert wird mögliche zukünftige Grid-Netzwerk-Erweiterungen vereinfachen.</p>
GRID_NETWORK_IP	R	<p>IPv4-Adresse dieses Knotens im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>

Taste	R, BP ODER O?	Wert
GRID_NETWORK_MAC	O	<p>Die MAC-Adresse für die Grid-Netzwerkschnittstelle im Container.</p> <p>Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert.</p> <p>Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden.</p> <p>Beispiel: b2 : 9c : 02 : c2 : 27 : 30</p>
GRID_NETWORK_MASKE	O	<p>IPv4-Netzmaske für diesen Knoten im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>255.255.255.0</p> <p>255.255.248.0</p>
GRID_NETWORK_MTU	O	<p>Die maximale Übertragungseinheit (MTU) für diesen Knoten im Grid-Netzwerk. Geben Sie nicht an, ob GRID_NETWORK_CONFIG = DHCP ist. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 verwendet.</p> <p>Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei.</p> <p>WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, an den der Knoten angeschlossen ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.</p> <p>WICHTIG: Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung Grid Network MTU mismatch wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.</p> <p>Beispiele:</p> <p>1500 8192</p>

Taste	R, BP ODER O?	Wert
GRID_NETWORK_TARGET	R	<p>Name des Hostgeräts, das Sie für den Netzzugang über den StorageGRID-Knoten verwenden werden. Es werden nur Namen von Netzwerkschnittstellen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den für ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegebenen.</p> <p>Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät oder verwenden Sie ein Bridge- und virtuelles Ethernet-Paar (veth).</p> <p>Beispiele:</p> <pre>bond0.1001</pre> <pre>ens192</pre>
GRID_NETWORK_TARGET_TYPE	O	<p>Schnittstelle</p> <p>(Dies ist der einzige unterstützte Wert.)</p>
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	<p>Richtig oder falsch</p> <p>Setzen Sie den Wert des Schlüssels auf „true“, um den StorageGRID-Container dazu zu bringen, die MAC-Adresse der Host-Zielschnittstelle im Grid-Netzwerk zu verwenden.</p> <p>Best Practice: in Netzwerken, in denen der promiscuius-Modus erforderlich wäre, verwenden Sie stattdessen DEN GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel.</p> <p>Weitere Informationen zum Klonen von MAC:</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red hat Enterprise Linux oder CentOS)"</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"</p>

Taste	R, BP ODER O?	Wert
INTERFACE_TARGET_nnnn	O	<p>Name und optionale Beschreibung für eine zusätzliche Schnittstelle, die Sie diesem Node hinzufügen möchten. Jeder Node kann mehrere zusätzliche Schnittstellen hinzugefügt werden.</p> <p>Geben Sie für <i>nnnn</i> eine eindeutige Nummer für jeden Eintrag INTERFACE_TARGET an, den Sie hinzufügen.</p> <p>Geben Sie für den 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 an, die auf der Seite VLAN-Schnittstellen und der Seite HA-Gruppen angezeigt wird.</p> <p>Beispiel: INTERFACE_TARGET_0001=ens256, Trunk</p> <p>Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.</p>
MAXIMUM_RAM	O	<p>Der maximale RAM-Umfang, den dieser Node nutzen darf. Wenn dieser Schlüssel nicht angegeben ist, gelten für den Node keine 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 kleiner als der gesamte RAM des Systems ist.</p> <p>Hinweis: Der RAM-Wert wirkt sich auf den tatsächlich reservierten Metadaten Speicherplatz eines Knotens aus. Siehe "beschreibung des reservierten Speicherplatzes für Metadaten".</p> <p>Das Format für dieses Feld lautet <number><unit>, Wo <unit> Kann sein b, k, m, Oder g.</p> <p>Beispiele:</p> <p>24g</p> <p>38654705664b</p> <p>Hinweis: Wenn Sie diese Option verwenden möchten, müssen Sie Kernel-Unterstützung für Speicher-cgroups aktivieren.</p>

Taste	R, BP ODER O?	Wert
NODE_TYPE	R	<p>Node-Typ:</p> <p>VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway</p>
PORT_NEU ZUORDNEN	O	<p>Ordnet alle von einem Node verwendeten Ports für interne Grid Node-Kommunikation oder externe Kommunikation neu zu. Neuzuordnungen von Ports sind erforderlich, wenn die Netzwerkrichtlinien des Unternehmens einen oder mehrere von StorageGRID verwendete Ports einschränken, wie in beschrieben "Interne Kommunikation mit Grid-Nodes" Oder "Externe Kommunikation".</p> <p>WICHTIG: Weisen Sie die Ports, die Sie für die Konfiguration von Load Balancer Endpunkten verwenden möchten, nicht neu zu.</p> <p>Hinweis: Wenn nur PORT_REMAP eingestellt ist, wird die von Ihnen angegebene Zuordnung sowohl für eingehende als auch für ausgehende Kommunikation verwendet. Wenn AUCH PORT_REMAP_INBOUND angegeben wird, gilt PORT_REMAP nur für ausgehende Kommunikation.</p> <p>Das verwendete Format ist: <network type>/<protocol>/<default port used by grid node>/<new port>, Wo <network type> Ist Grid, Administrator oder Client und das Protokoll tcp oder udp.</p> <p>Beispiel:</p> <p>PORT_REMAP = client/tcp/18082/443</p>

Taste	R, BP ODER O?	Wert
PORT_REMAP_INBOUND	O	<p>Ordnet die eingehende Kommunikation dem angegebenen Port erneut zu. Wenn SIE PORT_REMAP_INBOUND angeben, aber keinen Wert für PORT_REMAP angeben, bleiben die ausgehenden Kommunikationen für den Port unverändert.</p> <p>WICHTIG: Weisen Sie die Ports, die Sie für die Konfiguration von Load Balancer Endpunkten verwenden möchten, nicht neu zu.</p> <p>Das verwendete Format ist: <network type>/<protocol:>/<remapped port >/<default port used by grid node>, Wo <network type> Ist Grid, Administrator oder Client und das Protokoll tcp oder udp.</p> <p>Beispiel:</p> <p>PORT_REMAP_INBOUND = grid/tcp/3022/22</p>

Ermitteln der primären Admin-Node durch Grid-Nodes

Die Grid-Nodes kommunizieren mit dem primären Admin-Node zu Konfiguration und Management. Jeder Grid-Knoten muss die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk kennen.

Um sicherzustellen, dass ein Grid-Node auf den primären Admin-Node zugreifen kann, können Sie bei der Bereitstellung des Node eines der folgenden Schritte ausführen:

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

Die automatische Erkennung des primären Admin-Knotens wird über ein Multicast-Domänennamensystem (mDNS) durchgeführt. Beim ersten Start des primären Admin-Knotens veröffentlicht er seine IP-Adresse mit mDNS. Andere Knoten im selben Subnetz können dann die IP-Adresse abfragen und automatisch erfassen. Da der Multicast-IP-Datenverkehr normalerweise nicht über Subnetze routingfähig ist, können Nodes in anderen Subnetzen die IP-Adresse des primären Admin-Node nicht direkt abrufen.

Wenn Sie die automatische Erkennung verwenden:



- Sie müssen DIE ADMIN_IP-Einstellung für mindestens einen Grid-Node in allen Subnetzen, mit denen der primäre Admin-Node nicht direkt verbunden ist, enthalten. Dieser Grid-Knoten veröffentlicht dann die IP-Adresse des primären Admin-Knotens für andere Knoten im Subnetz, um mit mDNS zu ermitteln.
- Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur den Datenverkehr mehrerer gegossener IP-Daten innerhalb eines Subnetzes unterstützt.

Beispiel für die Node-Konfigurationsdateien

Sie können die Beispiel-Node-Konfigurationsdateien verwenden, die Ihnen bei der Einrichtung der Node-Konfigurationsdateien für Ihr StorageGRID System helfen. Die Beispiele zeigen Node-Konfigurationsdateien für alle Grid-Nodes.

Bei den 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-Node. Wenn Sie die Admin-Netzwerk-IP des primären Admin-Knotens durchsuchen möchten, um die Grid-Konfiguration abzuschließen (z. B. weil das Grid-Netzwerk nicht weitergeleitet wird), müssen Sie die Admin-Netzwerkverbindung für den primären Admin-Node in seiner Node-Konfigurationsdatei konfigurieren. Dies ist im Beispiel dargestellt.



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

Beispiel für primären Admin-Node

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-adm1.conf`

Beispieldateiinhalt:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-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

Beispiel Dateiname: /etc/storagegrid/nodes/dcl-sn1.conf

Beispieldateinhalt:

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dcl-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dcl-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dcl-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dcl-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 Archivknoten

Beispiel Dateiname: /etc/storagegrid/nodes/dcl-ar1.conf

Beispieldateinhalt:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-arcl-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Beispiel für Gateway-Node

Beispiel Dateiname: /etc/storagegrid/nodes/dcl-gw1.conf

Beispieldateinhalt:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-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-Node

Beispiel Dateiname: /etc/storagegrid/nodes/dcl-adm2.conf

Beispieldateinhalt:

```
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
```

StorageGRID-Konfiguration validieren

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 folgenden Befehl auf jedem Host aus:

```
sudo storagegrid node validate all
```

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

```
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 mithilfe von unterdrücken `-q` Oder `--quiet` Optionen in `storagegrid` Befehl (z. B. `storagegrid --quiet...`). Wenn Sie die Ausgabe unterdrücken, hat der Befehl einen Wert ungleich null Exit, wenn Konfigurationswarnungen oder Fehler erkannt wurden.

Wenn die Konfigurationsdateien nicht korrekt sind, werden die Probleme wie im Beispiel gezeigt als **WARNUNG** und **FEHLER** angezeigt. Wenn Konfigurationsfehler gefunden werden, müssen Sie sie korrigieren, bevor Sie mit der Installation fortfahren.

```

Checking for misnamed node configuration files...
  WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
  WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
  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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Starten Sie den StorageGRID Host Service

Um die StorageGRID Nodes zu starten und sicherzustellen, dass sie nach einem Neustart des Hosts neu gestartet werden, müssen Sie den StorageGRID Host Service aktivieren und starten.

Schritte

1. Führen Sie auf jedem Host folgende 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 „not running“ oder „` stopped“ zurückgibt, führen Sie den folgenden Befehl aus:

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

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

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

Grid Konfiguration und vollständige Installation (Red hat oder CentOS)

Navigieren Sie zum Grid Manager

Mit dem Grid Manager können Sie alle Informationen definieren, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Bevor Sie beginnen

Der primäre Admin-Node muss bereitgestellt werden und die anfängliche Startsequenz abgeschlossen haben.

Schritte

1. Öffnen Sie Ihren Webbrowser, und navigieren Sie zu einer der folgenden Adressen:

```
https://primary_admin_node_ip
```

```
client_network_ip
```

Alternativ können Sie auf den Grid Manager an Port 8443 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, je nach Ihrer Netzwerkkonfiguration, verwenden.

2. Wählen Sie **StorageGRID-System installieren**.

Die Seite zum Konfigurieren eines StorageGRID-Systems wird angezeigt.

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Geben Sie die StorageGRID Lizenzinformationen an

Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Schritte

1. Geben Sie auf der Lizenzseite einen aussagekräftigen Namen für Ihr StorageGRID-System in das Feld **Rastername** ein.

Nach der Installation wird der Name oben im Menü Nodes angezeigt.

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

Die Lizenzdatei wird validiert, und die Seriennummer wird angezeigt.



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

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Wählen Sie **Weiter**.

Fügen Sie Sites hinzu

Sie müssen mindestens einen Standort erstellen, wenn Sie StorageGRID installieren. Sie können weitere Standorte erstellen, um die Zuverlässigkeit und Storage-Kapazität Ihres StorageGRID Systems zu erhöhen.

Schritte

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

Fügen Sie so viele zusätzliche Standorte wie für Ihre Grid-Topologie hinzu. Sie können bis zu 16 Standorte hinzufügen.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there is a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a navigation bar with an 'Install' button. A progress bar below the navigation bar shows eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Step 2, 'Sites', is currently active and highlighted in blue. Below the progress bar, the 'Sites' section is displayed. It contains two paragraphs of text explaining single-site and multi-site deployments. Below the text are two input fields for site names. The first field is labeled 'Site Name 1' and contains the text 'Raleigh'. To its right is a red 'x' icon. The second field is labeled 'Site Name 2' and contains the text 'Atlanta'. To its right is a red '+ x' icon, indicating that a new site can be added.

3. Klicken Sie Auf **Weiter**.

Grid-Netzwerk-Subnetze angeben

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

Über diese Aufgabe

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

Wenn Sie mehrere Grid-Subnetze haben, 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 zusätzlichen Netzwerkeintrag hinzuzufügen.

Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf **Netzwerke-Subnetze**

ermitteln, um die Netznetzwerksubnetz-Liste automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die beim Grid Manager registriert sind.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Klicken Sie Auf **Weiter**.

Ausstehende Grid-Nodes genehmigen

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

Bevor Sie beginnen

Sie haben alle virtuellen und StorageGRID Appliance Grid-Nodes implementiert.



Es ist effizienter, eine einzelne Installation aller Nodes durchzuführen, anstatt zu einem späteren Zeitpunkt einige Nodes zu installieren.

Schritte

1. Prüfen Sie die Liste ausstehender Nodes und bestätigen Sie, dass alle von Ihnen bereitgestellten Grid-Nodes angezeigt werden.



Wenn ein Grid-Node fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

2. Aktivieren Sie das Optionsfeld neben einem Knoten, der noch nicht genehmigt werden soll.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✘ Remove		Search <input type="text"/>			
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address		
<input checked="" type="radio"/>	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21		

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

✎ Edit		🔄 Reset		✘ Remove		Search <input type="text"/>	
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
<input type="radio"/>	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21	
<input type="radio"/>	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21	
<input type="radio"/>	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21	
<input type="radio"/>	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21	
<input type="radio"/>	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21	

3. Klicken Sie Auf **Genehmigen**.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften, falls erforderlich:

Storage Node Configuration

General Settings

Site	<input type="text" value="Raleigh"/>
Name	<input type="text" value="NetApp-SGA"/>
NTP Role	<input type="text" value="Automatic"/>
ADC Service	<input type="text" value="Automatic"/>

Grid Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="172.16.5.20/21"/>
Gateway	<input type="text" value="172.16.5.20"/>

Admin Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="10.224.5.20/21"/>
Gateway	<input type="text" value="10.224.0.1"/>
Subnets (CIDR)	<input type="text" value="10.0.0.0/8"/> x
	<input type="text" value="172.19.0.0/16"/> x
	<input type="text" value="172.21.0.0/16"/> + x

Client Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="47.47.5.20/21"/>
Gateway	<input type="text" value="47.47.0.1"/>

- **Standort:** Der Systemname des Standorts für diesen Grid-Knoten.
- **Name:** Der Systemname für den Knoten. Der Name ist standardmäßig auf den Namen eingestellt, den Sie beim Konfigurieren des Nodes angegeben haben.

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

- **NTP-Rolle:** Die NTP-Rolle (Network Time Protocol) des Grid-Knotens. Die Optionen sind **Automatic**, **Primary** und **Client**. Bei Auswahl von **automatisch** wird die primäre Rolle Administratorknoten, Speicherknoten mit ADC-Diensten, Gateway-Nodes und beliebigen Grid-Nodes mit nicht statischen IP-

Adressen zugewiesen. Allen anderen Grid-Nodes wird die Client-Rolle zugewiesen.



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

- **ADC-Dienst** (nur Speicherknoten): Wählen Sie **automatisch** aus, damit das System feststellen kann, ob der Knoten den Dienst Administrative Domain Controller (ADC) benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten. Sie können den ADC-Dienst nicht zu einem Knoten hinzufügen, nachdem er bereitgestellt wurde.

5. Ändern Sie im Grid Network die Einstellungen für die folgenden Eigenschaften, falls erforderlich:

- **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Grid-Netzwerkschnittstelle (eth0 im Container). Zum Beispiel: 192.168.1.234/21
- **Gateway**: Das Grid Network Gateway. Beispiel: 192.168.0.1

Das Gateway ist erforderlich, wenn es mehrere Grid-Subnetze gibt.



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

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

Geben Sie die Zielnetze 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 Konfiguration des Admin-Netzwerks ausgewählt haben und hier den Wert ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die resultierende IP-Adresse nicht in einem DHCP-Adressenpool befindet.

Appliances: Wenn bei einer StorageGRID-Appliance das Admin-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Grid-Manager-Dialogfeld konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

- a. Starten Sie das Gerät neu: Wählen Sie im Appliance Installer die Option **Erweitert > Neustart**.

Ein Neustart kann mehrere Minuten dauern.

- b. Wählen Sie **Netzwerke konfigurieren > Link-Konfiguration** aus, und aktivieren Sie die entsprechenden Netzwerke.
- c. Wählen Sie **Netzwerke konfigurieren > IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.
- d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

- e. Entfernen Sie im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, 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. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration des Appliance Installer angegeben haben.

Weitere Informationen finden Sie in den Installationsanweisungen für Ihr Gerätemodell.

7. Wenn Sie das Client-Netzwerk für den Grid-Node 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 es wird nach der Installation zum Standard-Gateway für den Node.



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

Appliances: Wenn bei einer StorageGRID-Appliance das Client-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Grid-Manager-Dialogfeld konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

- a. Starten Sie das Gerät neu: Wählen Sie im Appliance Installer die Option **Erweitert > Neustart**.

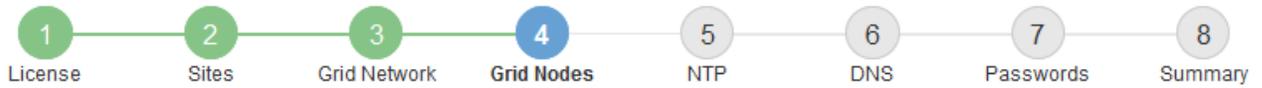
Ein Neustart kann mehrere Minuten dauern.

- b. Wählen Sie **Netzwerke konfigurieren > Link-Konfiguration** aus, und aktivieren Sie die entsprechenden Netzwerke.
- c. Wählen Sie **Netzwerke konfigurieren > IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.
- d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.
- e. Entfernen Sie im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, 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. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration des Appliance Installer angegeben haben.

Weitere Informationen finden Sie in den Installationsanweisungen für Ihr Gerät.

8. Klicken Sie Auf **Speichern**.

Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve
✖ Remove

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

◀ ▶

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

✎ Edit
🔄 Reset
✖ Remove

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
<input type="radio"/>	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
<input type="radio"/>	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
<input type="radio"/>	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
<input type="radio"/>	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
<input type="radio"/>	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
<input type="radio"/>	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

◀ ▶

9. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

Sie müssen alle Knoten genehmigen, die Sie im Raster benötigen. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Übersichtsseite auf **Installieren** klicken. Sie können die Eigenschaften eines genehmigten Grid-Knotens ändern, indem Sie das entsprechende Optionsfeld auswählen und auf **Bearbeiten** klicken.

10. Wenn Sie die Genehmigung von Gitterknoten abgeschlossen haben, klicken Sie auf **Weiter**.

Geben Sie Informationen zum Network Time Protocol-Server an

Sie müssen die NTP-Konfigurationsinformationen (Network Time Protocol) für das StorageGRID-System angeben, damit die auf separaten Servern ausgeführten Vorgänge synchronisiert bleiben können.

Über diese Aufgabe

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 Zeitdrift zu vermeiden.



Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer älteren Windows-Version als Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, unterstützt.

["Begrenzung des Supports, um Windows Time Service für hochpräzise Umgebungen zu konfigurieren"](#)

Die externen NTP-Server werden von den Nodes verwendet, denen Sie zuvor primäre NTP-Rollen zugewiesen haben.



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid 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 zusätzliche Servereinträge hinzuzufügen.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there is a blue header with "NetApp® StorageGRID®" and a "Help" dropdown. Below the header is a navigation bar with "Install" and a progress indicator. The progress indicator consists of eight numbered circles: 1 (License), 2 (Sites), 3 (Grid Network), 4 (Grid Nodes), 5 (NTP), 6 (DNS), 7 (Passwords), and 8 (Summary). Step 5, "NTP", is currently selected and highlighted in blue. Below the progress bar, the "Network Time Protocol" section is visible. It contains the instruction: "Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync." There are four input fields labeled "Server 1" through "Server 4". The values entered are: Server 1: 10.60.248.183, Server 2: 10.227.204.142, Server 3: 10.235.48.111, and Server 4: 0.0.0.0. To the right of the "Server 4" field is a plus sign (+) for adding more servers.

3. Wählen Sie **Weiter**.

Geben Sie die DNS-Serverinformationen an

Sie müssen DNS-Informationen für Ihr StorageGRID-System angeben, damit Sie mit Hostnamen anstelle von IP-Adressen auf externe Server zugreifen können.

Über diese Aufgabe

Angeben "[Informationen zum DNS-Server](#)" Ermöglicht die Verwendung von vollständig qualifizierten Domännennamen (FQDN) anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport.

Um einen ordnungsgemäßen Betrieb zu gewährleisten, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, können aufgrund bekannter Einschränkungen des Betriebssystems auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie dies tun "[Passen Sie die DNS-Serverliste an](#)" Für einzelne Knoten (in der Regel alle Knoten an einem Standort) einen anderen Satz von bis zu drei DNS-Servern verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein Inselstandort die FQDNs für externe Ziele auflösen kann.

Wenn die DNS-Serverinformationen nicht angegeben oder falsch konfiguriert sind, wird ein DNST-Alarm für den SSM-Service jedes Grid-Knotens ausgelöst. Der Alarm wird gelöscht, wenn DNS richtig konfiguriert ist und die neuen Serverinformationen alle Grid-Knoten erreicht haben.

Schritte

1. Geben Sie die IPv4-Adresse für mindestens einen DNS-Server im Textfeld **Server 1** an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um zusätzliche Servereinträge hinzuzufügen.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there is a blue header with the text "NetApp® StorageGRID®" and a "Help" dropdown menu. Below the header is a navigation bar with a tab labeled "Install". A progress indicator below the navigation bar shows eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress indicator, the "Domain Name Service" section is displayed. It contains the following text: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this text, there are two input fields for DNS servers. The first field is labeled "Server 1" and contains the IP address "10.224.223.130". To the right of this field is a red "x" icon. The second field is labeled "Server 2" and contains the IP address "10.224.223.136". To the right of this field are red "+" and "x" icons.

Als Best Practice empfehlen wir, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Geben Sie die Passwörter für das StorageGRID-System an

Im Rahmen der Installation des StorageGRID-Systems müssen Sie die Passwörter eingeben, um das System zu sichern und Wartungsarbeiten durchzuführen.

Über diese Aufgabe

Geben Sie auf der Seite Passwörter installieren die Passphrase für die Bereitstellung und das Root-Benutzerpasswort für die Grid-Verwaltung an.

- Die Provisionierungs-Passphrase wird als Verschlüsselungsschlüssel verwendet und nicht vom StorageGRID System gespeichert.
- Sie benötigen die Provisionierungs-Passphrase für Installations-, Erweiterungs- und Wartungsverfahren, einschließlich Download des Recovery-Pakets. Daher ist es wichtig, dass Sie die Provisionierungs-Passphrase an einem sicheren Ort speichern.
- Sie können die Provisionierungs-Passphrase im Grid Manager ändern, wenn Sie die aktuelle haben.
- Das Root-Benutzerpasswort für das Grid-Management kann mit dem Grid Manager geändert werden.
- Zufällig generierte Befehlszeilen-Konsole und SSH-Passwörter werden im gespeichert `passwords.txt` Datei im Wiederherstellungspaket.

Schritte

1. Geben Sie unter **Provisioning-Passphrase** das Provisioning-Passphrase ein, das für Änderungen an der Grid-Topologie Ihres StorageGRID-Systems erforderlich ist.

Speichern Sie die Provisionierungs-Passphrase an einem sicheren Ort.



Wenn Sie nach Abschluss der Installation die Provisionierungs-Passphrase später ändern möchten, können Sie das Grid Manager verwenden. Wählen Sie **KONFIGURATION > Zugangskontrolle > Grid-Passwörter**.

2. Geben Sie unter **Provisioning-Passphrase bestätigen** die Provisionierungs-Passphrase erneut ein, um sie zu bestätigen.
3. Geben Sie unter **Grid Management Root User Password** das Passwort ein, mit dem Sie auf den Grid Manager als „root“-Benutzer zugreifen können.

Speichern Sie das Passwort an einem sicheren Ort.

4. Geben Sie unter **Root-Benutzerpasswort bestätigen** das Grid Manager-Kennwort erneut ein, um es zu bestätigen.

Install



Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase	<input type="password"/>
Confirm Provisioning Passphrase	<input type="password"/>
Grid Management Root User Password	<input type="password"/>
Confirm Root User Password	<input type="password"/>

Create random command line passwords.

5. Wenn Sie ein Raster für Proof of Concept- oder Demo-Zwecke installieren, deaktivieren Sie optional das Kontrollkästchen **Random Command Line passwords**.

Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Löschen Sie **Create random command line passwords** nur für Demo-Grids, wenn Sie Standardpasswörter verwenden möchten, um über die Befehlszeile mit dem „root“- oder „admin“-Konto auf Grid-Nodes zuzugreifen.



Sie werden aufgefordert, die Recovery Package-Datei herunterzuladen (sgws-recovery-package-id-revision.zip) Nach dem Klick auf **Installieren** auf der Übersichtsseite. Unbedingt "[Laden Sie diese Datei herunter](#)" Um die Installation abzuschließen. Im werden die für den Zugriff auf das System erforderlichen Passwörter gespeichert `Passwords.txt Datei, in der Recovery Package-Datei enthalten.

6. Klicken Sie Auf **Weiter**.

Überprüfung der Konfiguration und vollständige Installation

Sie müssen die von Ihnen eingegebenen Konfigurationsinformationen sorgfältig prüfen, um sicherzustellen, dass die Installation erfolgreich abgeschlossen wurde.

Schritte

1. Öffnen Sie die Seite **Übersicht**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1 dc1-g1 dc1-s1 dc1-s2 dc1-s3 NetApp-SGA		

- Vergewissern Sie sich, dass alle Informationen zur Grid-Konfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite Zusammenfassung, um zurück zu gehen und Fehler zu beheben.
- 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 unterbrochen wird, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Siehe "[Netzwerkrichtlinien](#)" Entsprechende Details.

- Klicken Sie Auf **Download Wiederherstellungspaket**.

Wenn die Installation bis zum Punkt weiterläuft, an dem die Grid-Topologie definiert ist, werden Sie aufgefordert, die Recovery Package-Datei herunterzuladen (.zip), und bestätigen, dass Sie erfolgreich auf den Inhalt dieser Datei zugreifen können. Sie müssen die Recovery Package-Datei herunterladen, damit Sie das StorageGRID-System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Die Installation wird im Hintergrund fortgesetzt, aber Sie können die Installation nicht abschließen und erst auf das StorageGRID-System zugreifen, wenn Sie diese Datei herunterladen und überprüfen.

- Stellen Sie sicher, dass Sie den Inhalt des extrahieren können. .zip Speichern Sie die Datei an zwei sicheren und separaten Speicherorten.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

6. Aktivieren Sie das Kontrollkästchen **Ich habe die Wiederherstellungspaket-Datei erfolgreich heruntergeladen und verifiziert**, 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.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Name	Site	Grid Network IPv4 Address	Progress	Stage
dc1-adm1	Site1	172.16.4.215/21	<div style="width: 100%;"><div style="width: 100%;"></div></div>	Starting services
dc1-g1	Site1	172.16.4.216/21	<div style="width: 100%;"><div style="width: 100%;"></div></div>	Complete
dc1-s1	Site1	172.16.4.217/21	<div style="width: 50%;"><div style="width: 50%;"></div></div>	Waiting for Dynamic IP Service peers
dc1-s2	Site1	172.16.4.218/21	<div style="width: 20%;"><div style="width: 20%;"></div></div>	Downloading hotfix from primary Admin if needed
dc1-s3	Site1	172.16.4.219/21	<div style="width: 10%;"><div style="width: 10%;"></div></div>	Downloading hotfix from primary Admin if needed

Wenn die komplette Phase für alle Grid-Knoten erreicht ist, wird die Anmeldeseite für den Grid Manager angezeigt.

7. Melden Sie sich beim Grid Manager mit dem „root“-Benutzer und dem Passwort an, das Sie während der Installation angegeben haben.

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Implementierung und Konfiguration des Grid-Node die folgenden Richtlinien für DHCP-Adressen und Änderungen der Netzwerkkonfiguration.

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

Sie können DHCP nur während der Bereitstellungsphase einrichten. DHCP kann während der Konfiguration nicht eingerichtet werden.



Nodes werden neu gebootet, wenn sich ihre IP-Adressen ändern. Dies kann zu Ausfällen führen, wenn sich eine DHCP-Adresse gleichzeitig auf mehrere Nodes auswirkt.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmaske und Standard-Gateways für einen Grid-Node ändern möchten. Siehe "[Konfigurieren Sie IP-Adressen](#)".
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, geht die Client-Verbindung zum primären Admin-Node und anderen Grid-Nodes unter Umständen verloren. Je nach den vorgenommenen Änderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Automatisierung der Installation (Red hat Enterprise Linux oder CentOS)

Die Installation des StorageGRID Host Service und die Konfiguration der Grid-Nodes können automatisiert werden.

Eine Automatisierung der Implementierung kann in einem der folgenden Fälle von Nutzen sein:

- Sie verwenden bereits ein Standard-Orchestrierungs-Framework wie Ansible, Puppet oder Chef für die Implementierung und Konfiguration physischer oder virtueller Hosts.
- Sie beabsichtigen, mehrere StorageGRID Instanzen zu implementieren.
- Sie implementieren eine große, komplexe StorageGRID Instanz.

Der StorageGRID-Host-Service wird von einem Paket installiert und durch 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 vorab (oder programmatisch) auf die automatisierte Installation mithilfe von Standard-Orchestrierungs-Frameworks vor, wie in diesem Artikel beschrieben.

StorageGRID stellt optionale Python-Skripte zur Verfügung, mit denen die Konfiguration von StorageGRID Appliances und dem gesamten StorageGRID System (das „Grid“) automatisiert werden kann. Sie können diese Skripte direkt verwenden oder sie informieren, wie Sie die StorageGRID Installations-REST-API bei den von Ihnen selbst entwickelten Grid-Implementierungs- und Konfigurations-Tools verwenden.

Automatisieren Sie die Installation und Konfiguration des StorageGRID-Host-Service

Die Installation des StorageGRID-Host-Service kann mithilfe von Standard-Orchestrierungs-Frameworks wie Ansible, Puppet, Chef, Fabric oder SaltStack automatisiert werden.

Der StorageGRID-Host-Service ist eine RPM und orientiert sich an Konfigurationsdateien, die Sie für die automatisierte Installation vorab (oder programmgesteuert) vorbereiten können. Wenn Sie bereits ein Standard-Orchestrierungs-Framework für die Installation und Konfiguration von RHEL oder CentOS verwenden, sollte das Hinzufügen von StorageGRID zu Playbooks oder Rezepten unkompliziert sein.

Weitere Informationen dazu finden Sie in der Ansible-Rolle und dem Playbook `/extras` Ordner, der mit dem Installationsarchiv geliefert wird. Im Ansible-Playbook wird gezeigt, wie das funktioniert `storagegrid` Rolle bereitet den Host vor und installiert StorageGRID auf den Ziel-Servern. Die Rolle oder das Playbook können Sie nach Bedarf anpassen.



Das Beispiel-Playbook enthält nicht die Schritte, die zum Erstellen von Netzwerkgeräten vor dem Start des StorageGRID-Hostdienstes erforderlich sind. Fügen Sie diese Schritte vor der Fertigstellung und Verwendung des Playbook ein.

Sie können alle Schritte zur Vorbereitung der Hosts automatisieren und virtuelle Grid-Nodes implementieren.

Automatisieren Sie die Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Bevor Sie beginnen

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

Dateiname	Beschreibung
<code>configure-storagegrid.py</code>	Python-Skript zur Automatisierung der Konfiguration

Dateiname	Beschreibung
Configure-storagegrid.sample.json	Beispielkonfigurationsdatei für die Verwendung mit dem Skript
Configure-storagegrid.blank.json	Leere Konfigurationsdatei für die Verwendung mit dem Skript

- Sie haben ein erstellt `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`).

Über diese Aufgabe

Sie können das verwenden `configure-storagegrid.py` Python-Skript und das `configure-storagegrid.json` Konfigurationsdatei zur automatischen Konfiguration des StorageGRID Systems



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

Schritte

1. Melden Sie sich an der Linux-Maschine an, die Sie verwenden, um das Python-Skript auszuführen.
2. Wechseln Sie in das Verzeichnis, in dem 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 Recovery-Paket-Datei sichern, damit Sie das StorageGRID-System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Zum Beispiel kopieren Sie den Text auf einen sicheren, gesicherten Netzwerkstandort und an einen sicheren Cloud-Storage-Standort.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

Wenn Sie angegeben haben, dass zufällige Passwörter generiert werden, öffnen Sie die `Passwords.txt`

Datei und suchen Sie nach den Kennwörtern, 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. #####  
#####
```

Das StorageGRID System wird installiert und konfiguriert, wenn eine Bestätigungsmeldung angezeigt wird.

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

Verwandte Informationen

["Überblick über DIE REST API zur Installation"](#)

Überblick über DIE REST API zur Installation

StorageGRID stellt die StorageGRID Installations-API für die Durchführung von Installationsaufgaben bereit.

Die API verwendet die Swagger Open Source API-Plattform, um die API-Dokumentation bereitzustellen. Swagger ermöglicht Entwicklern und nicht-Entwicklern die Interaktion mit der API in einer Benutzeroberfläche, die zeigt, 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 mit der API Docs Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Jeder REST-API-Befehl umfasst die URL der API, eine HTTP-Aktion, alle erforderlichen oder optionalen URL-Parameter sowie eine erwartete API-Antwort.

StorageGRID Installations-API

Die StorageGRID Installations-API ist nur verfügbar, wenn Sie das StorageGRID-System zu Beginn konfigurieren und eine primäre Wiederherstellung des Admin-Knotens durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um auf die API-Dokumentation zuzugreifen, gehen Sie auf die Installations-Webseite des primären Admin-Knotens und wählen Sie in der Menüleiste **Hilfe > API-Dokumentation** aus.

Die StorageGRID Installations-API umfasst die folgenden Abschnitte:

- **Config** — Operationen bezogen auf die Produktversion und Versionen der API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Grid** — Konfigurationsvorgänge auf Grid-Ebene. Grid-Einstellungen erhalten und aktualisiert werden, einschließlich Grid-Details, Grid-Netzwerken, Grid-Passwörter und NTP- und DNS-Server-IP-Adressen.

- **Nodes** — Konfigurationsvorgänge auf Node-Ebene. Sie können eine Liste der Grid-Nodes abrufen, einen Grid-Node löschen, einen Grid-Node konfigurieren, einen Grid-Node anzeigen und die Konfiguration eines Grid-Node zurücksetzen.
- **Bereitstellung** — Provisioning Operationen. Sie können den Bereitstellungsverfahren starten und den Status des Bereitstellungsverfahrens anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsverfahrens anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Schemas** — API-Schemata für erweiterte Bereitstellungen
- **Standorte** — Konfigurationsvorgänge auf Standortebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.

Weitere Schritte

Führen Sie nach Abschluss einer Installation die erforderlichen Integrations- und Konfigurationsaufgaben aus. Sie können die optionalen Aufgaben nach Bedarf ausführen.

Erforderliche Aufgaben

- ["Erstellen Sie ein Mandantenkonto"](#) Für jedes Client-Protokoll (Swift oder S3), das zum Speichern von Objekten auf Ihrem StorageGRID System verwendet wird.
- ["Kontrolle des Systemzugriffs"](#) Durch das Konfigurieren von Gruppen und Benutzerkonten. Optional können Sie ["Konfigurieren Sie eine föderierte Identitätsquelle"](#) (Z. B. Active Directory oder OpenLDAP), damit Sie Verwaltungsgruppen und Benutzer importieren können. Sie können es auch ["Erstellen Sie lokale Gruppen und Benutzer"](#).
- Integration und Test der ["S3-API"](#) Oder ["Swift-API"](#) Client-Anwendungen, mit denen Sie Objekte auf Ihr StorageGRID-System hochladen.
- ["Konfigurieren Sie die Regeln für Information Lifecycle Management \(ILM\) und die ILM-Richtlinie"](#) Sie möchten zum Schutz von Objektdaten verwenden.
- Wenn Ihre Installation Storage-Nodes der Appliance umfasst, führen Sie mithilfe von SANtricity OS die folgenden Aufgaben aus:
 - Stellen Sie Verbindungen zu jeder StorageGRID Appliance her.
 - Eingang der AutoSupport-Daten überprüfen.

Siehe ["Richten Sie die Hardware ein"](#).
- Überprüfen und befolgen Sie die ["Richtlinien zur StorageGRID-Systemhärtung"](#) Zur Vermeidung von Sicherheitsrisiken.
- ["Konfigurieren Sie E-Mail-Benachrichtigungen für Systemwarnungen"](#).
- Wenn Ihr StorageGRID-System Archivknoten enthält (veraltet), konfigurieren Sie die Verbindung des Archivknotens mit dem externen Archivierungssystem des Ziels.

Optionale Aufgaben

- ["Aktualisieren der IP-Adressen des Grid-Node"](#) Wenn sie sich seit der Planung der Bereitstellung geändert

haben und das Wiederherstellungspaket erstellt haben.

- ["Konfigurieren Sie die Speicherverschlüsselung"](#), Bei Bedarf.
- ["Konfigurieren Sie die Storage-Komprimierung"](#) Um die Größe gespeicherter Objekte bei Bedarf zu reduzieren.
- ["Konfigurieren Sie den Zugriff auf das System für Überwachungszwecke"](#) Über eine NFS-Dateifreigabe

Fehlerbehebung bei Installationsproblemen

Falls bei der Installation des StorageGRID-Systems Probleme auftreten, können Sie auf die Installationsprotokolldateien zugreifen. Der technische Support muss möglicherweise auch die Installations-Log-Dateien verwenden, um Probleme zu beheben.

Die folgenden Installationsprotokolldateien sind über den Container verfügbar, auf dem jeder Node ausgeführt wird:

- `/var/local/log/install.log` (Auf allen Grid-Nodes gefunden)
- `/var/local/log/gdu-server.log` (Auf dem primären Admin-Node gefunden)

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"](#).

Verwandte Informationen

["Fehler in einem StorageGRID System beheben"](#)

Beispiel `/etc/sysconfig/Network-scripts`

Sie können die Beispieldateien verwenden, um vier physische Linux-Schnittstellen in einer einzelnen LACP-Verbindung zu aggregieren. Anschließend können Sie drei VLAN-Schnittstellen einrichten, die die Verbindung als StorageGRID-Grid-, Admin- und Client-Netzwerkschnittstellen unterteilen.

Physische Schnittstellen

Beachten Sie, dass die Switches an den anderen Enden der Links auch die vier Ports als einzelnen LACP-Trunk oder Port-Kanal behandeln müssen und mindestens drei referenzierte VLANs mit Tags übergeben werden 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 Ubuntu oder Debian

Installieren Sie Ubuntu oder Debian: Übersicht

Die Installation eines StorageGRID-Systems in einer Ubuntu- oder Debian-Umgebung umfasst drei primäre Schritte.

- 1. Vorbereitung:** Bei der Planung und Vorbereitung führen Sie folgende Aufgaben aus:
 - Erfahren Sie mehr über die Hardware- und Storage-Anforderungen für StorageGRID.
 - Erfahren Sie mehr über die Besonderheiten von "[StorageGRID Networking](#)" Damit Sie Ihr Netzwerk entsprechend konfigurieren können.
 - Ermitteln und Vorbereiten der physischen oder virtuellen Server, die Sie für das Hosten Ihrer StorageGRID Grid Nodes verwenden möchten
 - Auf den Servern, die Sie vorbereitet haben:
 - Installieren Sie Linux
 - Konfigurieren Sie das Hostnetzwerk
 - Hostspeicher konfigurieren
 - Installation Von Docker
 - Installieren Sie die StorageGRID Host Services
 - 2. * Bereitstellung*:** Bereitstellung von Grid-Knoten mit der entsprechenden Benutzeroberfläche. Wenn Sie Grid-Nodes implementieren, werden diese als Teil des StorageGRID Systems erstellt und mit einem oder mehreren Netzwerken verbunden.
 - a. Verwenden Sie die Linux-Befehlszeile und die Konfigurationsdateien der Nodes, um virtuelle Grid-Nodes auf den in Schritt 1 vorbereiteten Hosts bereitzustellen.
 - b. Verwenden Sie das Installationsprogramm für StorageGRID Appliance, um StorageGRID Appliance-Nodes bereitzustellen.
-  Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im StorageGRID Installationsverfahren enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie im "[Schnellstart für die Hardwareinstallation](#)" Anleitung für das Gerät finden.
- 3. Konfiguration:** Wenn alle Knoten bereitgestellt wurden, verwenden Sie den Grid Manager, um das Grid zu konfigurieren und die Installation abzuschließen.

Diese Anweisungen empfehlen einen Standardansatz für die Bereitstellung und Konfiguration eines StorageGRID-Systems in einer Ubuntu- oder Debian-Umgebung. Siehe auch die Informationen über folgende alternative Ansätze:

- Verwendung eines Standard-Orchestrierungs-Frameworks wie Ansible, Puppet oder Chef zur Installation von Ubuntu oder Debian, zur Konfiguration von Netzwerk und Storage, zur Installation von Docker und dem StorageGRID-Host-Service und zur Implementierung von virtuellen Grid-Nodes
- Automatisieren Sie die Implementierung und Konfiguration des StorageGRID Systems mit einem Python-Konfigurationsskript (im Installationsarchiv bereitgestellt).
- Automatisieren Sie die Implementierung und Konfiguration von Appliance-Grid-Nodes mit einem Python-Konfigurationsskript (erhältlich über das Installationsarchiv oder über das Installationsprogramm von StorageGRID Appliance).
- Als fortschrittlicher Entwickler von StorageGRID-Implementierungen sollten Sie die Installation VON REST-APIs verwenden, um die Installation von StorageGRID Grid-Nodes zu automatisieren.

Planen und bereiten Sie sich auf die Installation von Ubuntu oder Debian vor

Vor der Installation (Ubuntu oder Debian)

Bevor Sie Grid-Nodes implementieren und StorageGRID konfigurieren, müssen Sie mit den Schritten und Anforderungen für den Abschluss des Verfahrens vertraut sein.

Bei den Implementierungs- und Konfigurationsverfahren für StorageGRID ist bereits die Architektur und der Betrieb des StorageGRID Systems bekannt.

Sie können einen oder mehrere Standorte gleichzeitig implementieren. Alle Standorte müssen jedoch die Mindestanforderungen erfüllen, die für mindestens drei Storage-Nodes bestehen.

Vor dem Starten einer StorageGRID-Installation müssen folgende Schritte durchgeführt werden:

- Verstehen Sie die Computing-Anforderungen, einschließlich der minimalen CPU- und RAM-Anforderungen für jeden Node.
- Erfahren Sie, wie StorageGRID diverse Netzwerke unterstützt, um die Trennung von Datenverkehr, Sicherheit und Verwaltung zu gewährleisten, und planen Sie, welche Netzwerke Sie mit den einzelnen StorageGRID Nodes verbinden möchten.

Siehe StorageGRID "[Netzwerkrichtlinien](#)".

- Ermitteln der Storage- und Performance-Anforderungen der einzelnen Grid-Nodes
- Ermitteln Sie eine Reihe von Servern (physische, virtuelle oder beides), die als Aggregat ausreichend Ressourcen zur Unterstützung der Anzahl und des Typs der zu implementierenden StorageGRID Nodes bieten.
- Verstehen Sie die "[Anforderungen für die Node-Migration](#)", Wenn Sie planmäßige Wartungsarbeiten auf physischen Hosts ohne Serviceunterbrechung durchführen möchten.
- Sammeln Sie alle Netzwerkinformationen im Voraus. Sammeln Sie, sofern Sie kein DHCP verwenden, die IP-Adressen für die einzelnen Grid-Nodes sowie die IP-Adressen der zu verwendenden DNS- und NTP-Server.
- Installation, Anschluss und Konfiguration der gesamten erforderlichen Hardware – einschließlich aller StorageGRID Appliances – gemäß den Spezifikationen



Wenn bei der StorageGRID-Installation keine StorageGRID Appliance (Hardware) Storage Nodes verwendet werden, müssen Sie Hardware-RAID-Storage mit batteriegestütztem Schreib-Cache (BBWC) verwenden. StorageGRID unterstützt die Verwendung von Virtual Storage Area Networks (VSANs), Software-RAID oder keinen RAID-Schutz.



Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im StorageGRID Installationsverfahren enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie unter ["Appliance-Hardware installieren"](#).

- Legen Sie fest, welche der verfügbaren Implementierungs- und Konfigurationstools Sie verwenden möchten.

Erforderliche Materialien

Bevor Sie StorageGRID installieren, müssen Sie die erforderlichen Materialien erfassen und vorbereiten.

Element	Hinweise
NetApp StorageGRID Lizenz	Sie benötigen eine gültige, digital signierte NetApp Lizenz. Hinweis: Eine Non-Production-Lizenz, die für Tests und Proof of Concept Grids verwendet werden kann, ist im StorageGRID-Installationsarchiv enthalten.
StorageGRID Installationsarchiv	Unbedingt "Laden Sie das StorageGRID-Installationsarchiv herunter und extrahieren Sie die Dateien" .
Service-Laptop	Das StorageGRID System wird über einen Service-Laptop installiert. Der Service-Laptop muss Folgendes haben: <ul style="list-style-type: none"> • Netzwerkport • SSH-Client (z. B. PuTTY) • "Unterstützter Webbrowser"
StorageGRID-Dokumentation	<ul style="list-style-type: none"> • "Versionshinweise" • "Anweisungen für die Administration von StorageGRID"

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Sie müssen das StorageGRID-Installationsarchiv herunterladen und die erforderlichen

Dateien extrahieren.

Schritte

1. Wechseln Sie zum "[NetApp Download-Seite für StorageGRID](#)".
2. Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version, oder wählen Sie eine andere Version aus dem Dropdown-Menü aus und wählen Sie **Go**.
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
4. Wenn eine Vorsichtshinweis/MustRead-Anweisung angezeigt wird, lesen Sie sie und aktivieren Sie das Kontrollkästchen.



Nachdem Sie die StorageGRID Version installiert haben, müssen Sie alle erforderlichen Hotfixes anwenden. Weitere Informationen finden Sie im "[Hotfix-Verfahren in der Recovery- und Wartungsanleitung](#)".

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren** aus.

Die Download-Seite für die ausgewählte Version wird angezeigt. Die Seite enthält drei Spalten:

6. Wählen Sie in der Spalte **Install StorageGRID** die .tgz- oder .zip-Datei für Ubuntu oder Debian aus.



Wählen Sie die aus .zip Datei, wenn Windows auf dem Service-Laptop ausgeführt wird.

7. Speichern und extrahieren Sie die Archivdatei.
8. Wählen Sie aus der folgenden Liste die benötigten Dateien aus.

Welche Dateien benötigt werden, hängt von der geplanten Grid-Topologie und der Implementierung des StorageGRID Grids ab.



Die in der Tabelle aufgeführten Pfade beziehen sich auf das Verzeichnis der obersten Ebene, das vom extrahierten Installationsarchiv installiert wird.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine NetApp Lizenzdatei, die nicht in der Produktionsumgebung enthalten ist und für Tests und Proof of Concept-Implementierungen genutzt werden kann
	DEB-Paket zum Installieren der StorageGRID-Knoten-Images auf Ubuntu oder Debian-Hosts.
	MD5-Prüfsumme für die Datei /debs/storagegrid-webscale-images-version-SHA.deb.

Pfad und Dateiname	Beschreibung
	DEB-Paket zur Installation des StorageGRID-Hostdienstes auf Ubuntu oder Debian-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können. Sie können dieses Skript auch für Ping Federate verwenden.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel-Rolle und Playbook für Ansible zur Konfiguration von Ubuntu oder Debian-Hosts für die Implementierung von StorageGRID-Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure
	<p>API-Schemata für StorageGRID:</p> <p>Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.</p>

CPU- und RAM-Anforderungen erfüllt

Überprüfen und konfigurieren Sie vor dem Installieren der StorageGRID Software die Hardware so, dass sie zur Unterstützung des StorageGRID Systems bereit ist.

Informationen zu unterstützten Servern finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

Jeder StorageGRID Node benötigt die folgenden Mindestanforderungen:

- CPU-Cores: 8 pro Node
- RAM: Mindestens 24 GB pro Node und 2 bis 16 GB weniger als der gesamte System-RAM, abhängig von der verfügbaren RAM-Gesamtkapazität und der Anzahl der nicht-StorageGRID-Software, die auf dem System ausgeführt wird

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



Überwachen Sie Ihre CPU- und Arbeitsspeicherauslastung regelmäßig, um sicherzustellen, dass diese Ressourcen Ihre Workloads weiterhin erfüllen. Beispielsweise würde eine Verdoppelung der RAM- und CPU-Zuweisung für virtuelle Storage-Nodes ähnliche Ressourcen bereitstellen wie für die StorageGRID Appliance-Nodes. Wenn die Menge der Metadaten pro Node 500 GB überschreitet, sollten Sie darüber hinaus den RAM pro Node auf 48 GB oder mehr erhöhen. Informationen zum Management von Objekt-Metadaten-Storage, zum Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten und zum Monitoring der CPU- und Arbeitsspeicherauslastung finden Sie in den Anweisungen für ["Administration"](#), ["Monitoring"](#), und ["Aktualisierung"](#) StorageGRID:

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

Wenn Sie Virtual Machines als Hosts verwenden und die Größe und Anzahl der VMs kontrollieren können, sollten Sie für jeden StorageGRID Node eine einzelne VM verwenden und die Größe der VM entsprechend festlegen.

Bei Produktionsimplementierungen sollten nicht mehrere Storage-Nodes auf derselben physischen Speicherhardware oder einem virtuellen Host ausgeführt werden. Jeder Storage-Node in einer einzelnen StorageGRID-Implementierung sollte sich in einer eigenen, isolierten Ausfall-Domäne befinden. Sie können die Langlebigkeit und Verfügbarkeit von Objektdaten maximieren, wenn sichergestellt wird, dass ein einzelner Hardwareausfall nur einen einzelnen Storage-Node beeinträchtigen kann.

Siehe auch ["Storage- und Performance-Anforderungen erfüllt"](#).

Storage- und Performance-Anforderungen erfüllt

Sie müssen die Storage-Anforderungen für StorageGRID-Nodes verstehen, damit Sie ausreichend Speicherplatz für die Erstkonfiguration und die künftige Storage-Erweiterung bereitstellen können.

StorageGRID Nodes erfordern drei logische Storage-Kategorien:

- **Container Pool** — Performance-Tier (10.000 SAS oder SSD) Storage für die Node-Container, der dem Docker-Storage-Treiber zugewiesen wird, wenn Sie Docker auf den Hosts installieren und konfigurieren, die Ihre StorageGRID-Knoten unterstützen.
- **Systemdaten** — Performance-Tier (10.000 SAS oder SSD) Speicher für persistenten Speicher pro Node von Systemdaten und Transaktionsprotokollen, die die StorageGRID Host Services nutzen und einzelnen Nodes zuordnen werden.
- **Objektdaten** — Performance-Tier (10.000 SAS oder SSD) Storage und Capacity-Tier (NL-SAS/SATA) Massenspeicher für die persistente Speicherung von Objektdaten und Objekt-Metadaten.

Sie müssen RAID-gestützte Blockgeräte für alle Speicherkategorien verwenden. Nicht redundante Festplatten, SSDs oder JBODs werden nicht unterstützt. Sie können für jede der Storage-Kategorien gemeinsam genutzten oder lokalen RAID-Speicher verwenden. Wenn Sie jedoch die Funktion zur Node-Migration in StorageGRID verwenden möchten, müssen Sie sowohl System- als auch Objektdaten auf Shared Storage speichern. Weitere Informationen finden Sie unter "[Anforderungen für die Container-Migration für Nodes](#)".

Performance-Anforderungen erfüllt

Die Performance der für den Container-Pool verwendeten Volumes, Systemdaten und Objektmetadaten wirkt sich erheblich auf die Gesamt-Performance des Systems aus. Sie sollten Performance-Tier-Storage (10.000 SAS oder SSD) für diese Volumes verwenden, um eine angemessene Festplatten-Performance in Bezug auf Latenz, Input/Output Operations per Second (IOPS) und Durchsatz sicherzustellen. Sie können Capacity-Tier (NL-SAS/SATA)-Storage für den persistenten Storage von Objektdaten verwenden.

Für die Volumes, die für den Container-Pool, Systemdaten und Objektdaten verwendet werden, muss ein Write-Back-Caching aktiviert sein. Der Cache muss sich auf einem geschützten oder persistenten Medium befinden.

Anforderungen an Hosts, die NetApp ONTAP Storage nutzen

Wenn der StorageGRID-Node Storage verwendet, der einem NetApp ONTAP System zugewiesen ist, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

Anzahl der erforderlichen Hosts

Jeder StorageGRID Standort erfordert mindestens drei Storage-Nodes.



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Storage Node auf einem einzelnen physischen oder virtuellen Host aus. Die Verwendung eines dedizierten Hosts für jeden Speicherknoten stellt eine isolierte Ausfalldomäne zur Verfügung.

Andere Node-Typen wie Admin-Nodes oder Gateway-Nodes können auf denselben Hosts implementiert oder je nach Bedarf auf ihren eigenen dedizierten Hosts implementiert werden.

Anzahl der Storage-Volumes pro Host

In der folgenden Tabelle ist die Anzahl der für jeden Host erforderlichen Storage Volumes (LUNs) und die

Mindestgröße für jede LUN angegeben, basierend darauf, welche Nodes auf diesem Host implementiert werden.

Die maximale getestete LUN-Größe beträgt 39 TB.



Diese Nummern gelten für jeden Host, nicht für das gesamte Raster.

LUN-Zweck	Storage-Kategorie	Anzahl LUNs	Minimale Größe/LUN
Storage-Pool für Container-Engine	Container-Pool	1	Gesamtzahl der Nodes × 100 GB
/var/local Datenmenge	Systemdaten	1 für jeden Node auf diesem Host	90 GB
Storage-Node	Objektdaten	3 für jeden Speicherknoten auf diesem Host Hinweis: ein softwarebasierter Speicherknoten kann 1 bis 16 Speicher-Volumes haben; es werden mindestens 3 Speicher-Volumes empfohlen.	12 TB (4 TB/LUN) Weitere Informationen finden Sie unter Storage-Anforderungen für Storage-Nodes.
Prüfprotokolle für Admin-Node	Systemdaten	1 für jeden Admin-Node auf diesem Host	200 GB
Admin-Node-Tabellen	Systemdaten	1 für jeden Admin-Node auf diesem Host	200 GB



Je nach konfigurierter Audit-Ebene die Größe der Benutzereingaben wie S3-Objektschlüsselname, Und wie viele Audit-Log-Daten Sie erhalten müssen, müssen Sie möglicherweise die Größe der Audit-Log-LUN auf jedem Admin-Node erhöhen. im Allgemeinen generiert ein Grid ca. 1 KB Audit-Daten pro S3-Vorgang, Das heißt, eine 200 GB LUN würde 70 Millionen Operationen pro Tag oder 800 Operationen pro Sekunde für zwei bis drei Tage unterstützen.

Minimaler Speicherplatz für einen Host

In der folgenden Tabelle ist der erforderliche Mindestspeicherplatz für jeden Node-Typ aufgeführt. Anhand dieser Tabelle können Sie bestimmen, welcher Storage-Mindestbetrag für den Host in jeder Storage-Kategorie bereitgestellt werden muss. Dabei können Sie festlegen, welche Nodes auf diesem Host implementiert werden.



Disk Snapshots können nicht zur Wiederherstellung von Grid Nodes verwendet werden. Lesen Sie stattdessen den Abschnitt "[Recovery von Grid Nodes](#)" Verfahren für jeden Node-Typ.

Node-Typ	Container-Pool	Systemdaten	Objektdaten
Storage-Node	100 GB	90 GB	4,000 GB
Admin-Node	100 GB	490 GB (3 LUNs)	<i>Nicht zutreffend</i>
Gateway-Node	100 GB	90 GB	<i>Nicht zutreffend</i>
Archiv-Node	100 GB	90 GB	<i>Nicht zutreffend</i>

Beispiel: Berechnung der Storage-Anforderungen für einen Host

Angenommen, Sie planen, drei Nodes auf demselben Host zu implementieren: Einen Storage-Node, einen Admin-Node und einen Gateway-Node. Sie sollten dem Host mindestens neun Storage Volumes zur Verfügung stellen. Es sind mindestens 300 GB Performance-Tier-Storage für die Node-Container, 670 GB Performance-Tier-Storage für Systemdaten und Transaktionsprotokolle und 12 TB Kapazitäts-Tier Storage für Objektdaten erforderlich.

Node-Typ	LUN-Zweck	Anzahl LUNs	Die LUN-Größe
Storage-Node	Docker Storage-Pool	1	300 GB (100 GB/Node)
Storage-Node	/var/local Datenmenge	1	90 GB
Storage-Node	Objektdaten	3	12 TB (4 TB/LUN)
Admin-Node	/var/local Datenmenge	1	90 GB
Admin-Node	Prüfprotokolle für Admin- Node	1	200 GB
Admin-Node	Admin-Node-Tabellen	1	200 GB
Gateway-Node	/var/local Datenmenge	1	90 GB
Gesamt		9	Container-Pool: 300 GB Systemdaten: 670 GB Objektdaten: 12,000 GB

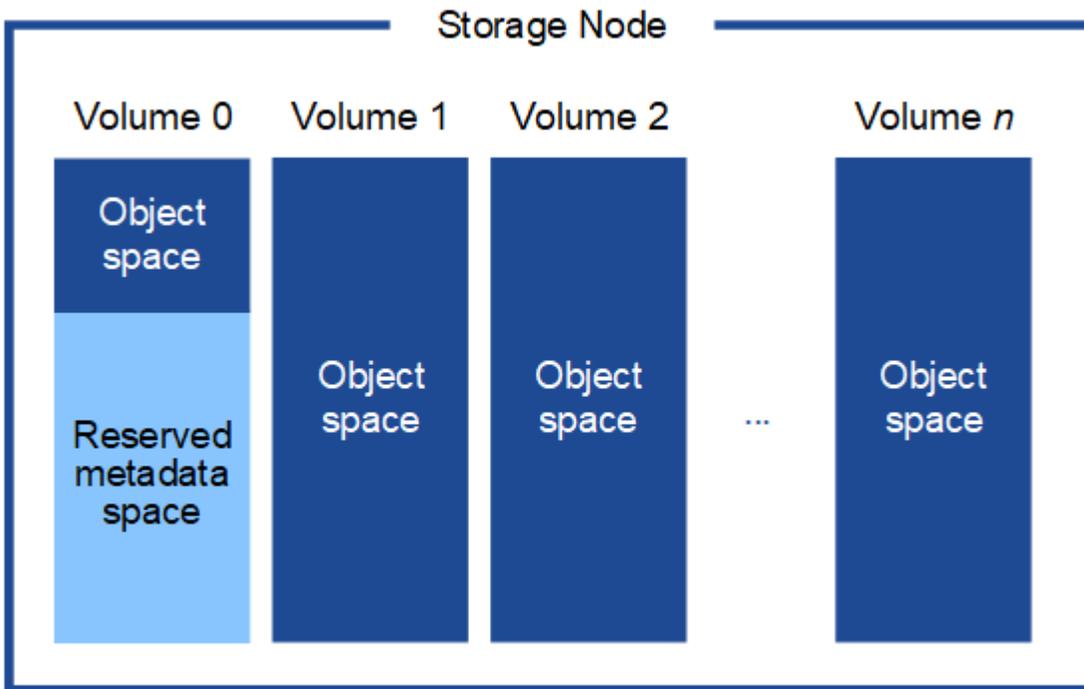
Storage-Anforderungen für Storage-Nodes

Ein softwarebasierter Speicher-Node kann 1 bis 16 Speicher-Volumes haben - 3 oder mehr Speicher-Volumes werden empfohlen. Jedes Storage-Volume sollte 4 TB oder größer sein.



Ein Appliance-Speicherknoten kann bis zu 48 Speicher-Volumes haben.

Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objekt-Metadaten auf dem Storage Volume 0 jedes Storage-Nodes. Alle verbleibenden Speicherplatz auf dem Storage-Volume 0 und anderen Storage-Volumes im Storage-Node werden ausschließlich für Objektdaten verwendet.



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

Wenn Sie Volume 0 eines neuen Storage-Node Speicherplatz zuweisen, müssen Sie sicherstellen, dass für den Anteil aller Objekt-Metadaten des Node ausreichend Speicherplatz vorhanden ist.

- Mindestens müssen Sie Volume 0 mindestens 4 TB zuweisen.



Wenn Sie nur ein Storage-Volume für einen Storage-Node verwenden und dem Volume 4 TB oder weniger zuweisen, hat der Storage-Node beim Start möglicherweise den Schreibgeschützten Storage-Status und speichert nur Objekt-Metadaten.



Wenn Sie Volume 0 weniger als 500 GB zuweisen (nur für den nicht-produktiven Einsatz), sind 10 % der Kapazität des Speicher-Volumes für Metadaten reserviert.

- Wenn Sie ein neues System installieren (StorageGRID 11.6 oder höher) und jeder Speicherknoten mindestens 128 GB RAM hat, weisen Sie Volume 0 mindestens 8 TB zu. Bei Verwendung eines größeren Werts für Volume 0 kann der zulässige Speicherplatz für Metadaten auf jedem Storage Node erhöht werden.
- Verwenden Sie bei der Konfiguration verschiedener Storage-Nodes für einen Standort, falls möglich, die gleiche Einstellung für Volume 0. Wenn ein Standort Storage-Nodes unterschiedlicher Größe enthält, bestimmt der Storage-Node mit dem kleinsten Volume 0 die Metadaten-Kapazität dieses Standorts.

Weitere Informationen finden Sie unter ["Management von Objekt-Metadaten-Storage"](#).

Anforderungen für die Container-Migration für Nodes

Mit der Funktion zur Node-Migration können Sie einen Node manuell von einem Host auf einen anderen verschieben. Normalerweise befinden sich beide Hosts im selben physischen Datacenter.

Dank der Node-Migration können Sie physische Host-Wartungsarbeiten durchführen, ohne Grid-Vorgänge zu unterbrechen. Sie verschieben alle StorageGRID-Nodes nacheinander auf einen anderen Host, bevor Sie den physischen Host in den Offline-Modus versetzen. Die Migration von Nodes erfordert nur kurze Ausfallzeiten für jeden Node. Der Betrieb und die Verfügbarkeit von Grid-Services sollte dabei nicht beeinträchtigt werden.

Wenn Sie die StorageGRID-Node-Migrationsfunktion nutzen möchten, muss Ihre Implementierung zusätzliche Anforderungen erfüllen:

- Konsistente Netzwerkschnittstellennamen über Hosts in einem einzigen physischen Datacenter hinweg
- Shared Storage für StorageGRID Metadaten und Objekt-Repository-Volumes, auf die alle Hosts in einem einzigen physischen Datacenter zugreifen können. So können Sie beispielsweise ein NetApp E-Series Storage-Array verwenden.

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

Bevor Sie eine Migration oder eine Hypervisor-Wartung durchführen, müssen Sie die Nodes ordnungsgemäß herunterfahren. Siehe Anweisungen für ["Herunterfahren eines Grid-Node"](#).

VMware Live Migration wird nicht unterstützt

OpenStack Live Migration und VMware Live vMotion sorgen dafür, dass die Uhr der Virtual Machine sprunghaft anzeigt und werden für Grid-Nodes unabhängig vom Typ nicht unterstützt. Obwohl selten, falsche Uhrzeiten können zum Verlust von Daten oder Konfigurations-Updates führen.

Cold-Migration wird unterstützt. Bei der „Cold“-Migration sollten Sie die StorageGRID Nodes herunterfahren, bevor Sie sie zwischen Hosts migrieren. Siehe Anweisungen für ["Herunterfahren eines Grid-Node"](#).

Konsistente Namen von Netzwerkschnittstellen

Um einen Knoten von einem Host auf einen anderen zu verschieben, muss der StorageGRID-Hostdienst darauf vertrauen können, dass die externe Netzwerkverbindung, die der Knoten am aktuellen Standort hat, am neuen Standort dupliziert werden kann. Dies schafft Vertrauen durch die Verwendung konsistenter Netzwerk-Interface-Namen in den Hosts.

Angenommen, beispielsweise, dass StorageGRID NodeA, der auf Host1 ausgeführt wird, mit den folgenden Schnittstellenzuordnungen konfiguriert wurde:

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

Die linke Seite der Pfeile entspricht den traditionellen Schnittstellen, die aus einem StorageGRID-Container betrachtet werden (das sind die Grid-, Administrator- und Client-Netzwerk-Schnittstellen). Die rechte Seite der Pfeile entspricht den tatsächlichen Host-Schnittstellen, die diese Netzwerke bereitstellen. Dabei handelt es sich um drei VLAN-Schnittstellen, die derselben physischen Interface-Verbindung untergeordnet sind.

Nehmen Sie an, Sie möchten NodeA zu Host2 migrieren. Wenn Host2 auch Schnittstellen mit den Namen bond0.1001, bond0.1002 und bond0.1003 besitzt, ermöglicht das System die Verschiebung, vorausgesetzt, dass die „Gefällt mir“-Schnittstellen auf Host2 die gleiche Konnektivität wie auf Host1 bereitstellen. Wenn Host2 keine Schnittstellen mit demselben Namen hat, ist die Verschiebung nicht zulässig.

Es gibt viele Möglichkeiten, eine konsistente Netzwerkschnittstelle über mehrere Hosts hinweg zu benennen; siehe ["Konfigurieren Sie das Hostnetzwerk"](#) Für einige Beispiele.

Shared Storage

Für schnelle Node-Migrationen mit geringem Overhead werden Node-Daten mit der StorageGRID Node-Migrationsfunktion nicht physisch verschoben. Stattdessen werden die Node-Migration als Export- und Importpaar durchgeführt:

Schritte

1. Während des Vorgangs „Node Export“ wird eine kleine Menge von persistenten Zustandsdaten aus dem Node-Container extrahiert, der auf HostA ausgeführt wird und auf dem Systemdatenvolume dieses Node zwischengespeichert wird. Anschließend wird der Knoten-Container auf HostA deaktiviert.
2. Während des Vorgangs „Node Import“ wird der Node-Container auf HostB, der die gleiche Netzwerkschnittstelle und die Blockspeicherzuordnungen verwendet, die auf HostA wirksam waren, instanziiert. Anschließend werden die im Cache gespeicherten Persistent State-Daten in die neue Instanz eingefügt.

In Anbetracht dieses Betriebsmodus müssen alle Systemdaten und Objekt-Storage-Volumes des Node sowohl von HostA als auch von HostB aus zugänglich sein, damit die Migration erlaubt und ausgeführt werden kann. Außerdem müssen sie auf dem Knoten mit Namen abgebildet worden sein, die garantiert auf die gleichen LUNs auf HostA und HostB verweisen.

Das folgende Beispiel zeigt eine Lösung für die Zuordnung von Blockgeräten für einen StorageGRID-Speicherknoten, bei dem auf den Hosts DM-Multipathing verwendet wird und in das Alias-Feld verwendet wurde `/etc/multipath.conf` Um konsistente, freundliche Blockgerätenamen zu liefern, die auf allen Hosts verfügbar sind.

```
/var/local  ───>  /dev/mapper/sgws-sn1-var-local
rangedb0   ───>  /dev/mapper/sgws-sn1-rangedb0
rangedb1   ───>  /dev/mapper/sgws-sn1-rangedb1
rangedb2   ───>  /dev/mapper/sgws-sn1-rangedb2
rangedb3   ───>  /dev/mapper/sgws-sn1-rangedb3
```

Implementierungstools

Sie profitieren möglicherweise von der Automatisierung der gesamten StorageGRID Installation oder eines Teils.

Eine Automatisierung der Implementierung kann in einem der folgenden Fälle von Nutzen sein:

- Sie verwenden bereits ein Standard-Orchestrierungs-Framework wie Ansible, Puppet oder Chef für die Implementierung und Konfiguration physischer oder virtueller Hosts.
- Sie beabsichtigen, mehrere StorageGRID Instanzen zu implementieren.
- Sie implementieren eine große, komplexe StorageGRID Instanz.

Der StorageGRID Host Service wird durch ein Paket installiert und unterstützt durch Konfigurationsdateien, die während einer manuellen Installation interaktiv erstellt oder vorab (oder programmgesteuert) vorbereitet werden können, um eine automatisierte Installation mithilfe von Standard-Orchestrierungs-Frameworks zu ermöglichen. StorageGRID bietet optionale Python-Skripte zur Automatisierung der Konfiguration von StorageGRID Appliances und dem gesamten StorageGRID-System (das „Grid“). Sie können diese Skripte direkt verwenden oder sie informieren, wie Sie die StorageGRID Installations-REST-API bei den von Ihnen selbst entwickelten Grid-Implementierungs- und Konfigurations-Tools verwenden.

Wenn Sie an der Automatisierung Ihrer gesamten StorageGRID-Implementierung oder eines Teils interessiert sind, lesen Sie die Seite ["Automatisieren Sie die Installation"](#) Vor Beginn des Installationsprozesses.

Vorbereiten der Hosts (Ubuntu oder Debian)

Wie sich die Host-weiten Einstellungen während der Installation ändern

Auf Bare Metal-Systemen nimmt StorageGRID einige Änderungen am gesamten Host vor `sysctl` Einstellungen.

Folgende Änderungen wurden 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 Linux auf allen Grid-Hosts installieren. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um eine Liste der unterstützten Versionen zu erhalten.



Stellen Sie sicher, dass Ihr Betriebssystem auf Linux Kernel 4.15 oder höher aktualisiert wird.

Schritte

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



Installieren Sie keine grafischen Desktop-Umgebungen. Bei der Installation von Ubuntu müssen Sie **Standard-Systemdienstprogramme** auswählen. Die Auswahl von **OpenSSH-Server** wird empfohlen, um SSH-Zugriff auf Ihre Ubuntu-Hosts zu aktivieren. Alle anderen Optionen können gelöscht bleiben.

2. Stellen Sie sicher, dass alle Hosts Zugriff auf Ubuntu- oder Debian-Paket-Repositorys 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 zu erhalten.



Wenn Sie den Auslagerungsaustausch nicht vollständig deaktivieren, kann die Leistung erheblich gesenkt werden.

AppArmor-Profilinstallation verstehen

Wenn Sie in einer selbst bereitgestellten Ubuntu-Umgebung arbeiten und das obligatorische Zutrittskontrollsystem AppArmor verwenden, werden die AppArmor-Profile, die mit Paketen verknüpft sind, die Sie auf dem Basissystem installieren, möglicherweise durch die entsprechenden Pakete blockiert, die mit StorageGRID installiert sind.

Standardmäßig werden AppArmor-Profile für Pakete installiert, die auf dem Basisbetriebssystem installiert sind. Wenn Sie diese Pakete aus dem StorageGRID-Systemcontainer ausführen, werden die AppArmor-Profile blockiert. Die Basispakete DHCP, MySQL, NTP und tcdump stehen in Konflikt mit AppArmor und anderen Basispaketen können ebenfalls kollidieren.

Für die Handhabung von AppArmor-Profilen stehen Ihnen zwei Optionen zur Verfügung:

- Deaktivieren Sie einzelne Profile für die im 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 folgende 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 ganz. Für Ubuntu 9.10 oder höher, folgen Sie den Anweisungen in der Ubuntu Online-Community: "[Deaktivieren Sie AppArmor](#)". Die Deaktivierung von AppArmor ist unter neueren Ubuntu-Versionen möglicherweise nicht möglich.

Wenn Sie AppArmor deaktivieren, werden in den StorageGRID-Protokolldateien keine Einträge angezeigt, die darauf hinweisen, dass AppArmor aktiviert ist.

Konfigurieren des Hostnetzwerks (Ubuntu oder Debian)

Nach dem Abschluss der Linux-Installation auf Ihren Hosts müssen Sie möglicherweise eine zusätzliche Konfiguration durchführen, um auf jedem Host eine Reihe von Netzwerkschnittstellen vorzubereiten, die sich für die Zuordnung zu den später zu implementierenden StorageGRID Nodes eignen.

Bevor Sie beginnen

- Sie haben die geprüft "[StorageGRID Netzwerkrichtlinien](#)".
- Sie haben die Informationen zu überprüft "[Anforderungen für die Container-Migration für Nodes](#)".
- Wenn Sie virtuelle Hosts verwenden, haben Sie die gelesen [Überlegungen und Empfehlungen zum Klonen von MAC-Adressen](#) Vor dem Konfigurieren des Hostnetzwerks.



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

Über diese Aufgabe

Grid-Nodes müssen auf das Grid-Netzwerk und optional auf Admin- und Client-Netzwerke zugreifen können. Sie ermöglichen diesen Zugriff, indem Sie Zuordnungen erstellen, die die physische Schnittstelle des Hosts den virtuellen Schnittstellen für jeden Grid-Node zuordnen. Verwenden Sie bei der Erstellung von Host-Schnittstellen benutzerfreundliche Namen, um die Implementierung über alle Hosts hinweg zu vereinfachen und die Migration zu ermöglichen.

Die gleiche Schnittstelle kann von dem Host und einem oder mehreren Nodes gemeinsam genutzt werden.

Beispielsweise können Sie für den Hostzugriff und den Netzwerkzugriff von Node-Admin dieselbe Schnittstelle verwenden, um die Wartung von Hosts und Nodes zu vereinfachen. Obwohl dieselbe Schnittstelle zwischen dem Host und den einzelnen Nodes gemeinsam genutzt werden kann, müssen alle unterschiedliche IP-Adressen haben. IP-Adressen können nicht zwischen Nodes oder zwischen dem Host und einem beliebigen Node gemeinsam genutzt 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 etwas dazwischen tun. Normalerweise würden Sie jedoch nicht die gleiche Hostnetzwerkschnittstelle bereitstellen wie die Grid- und Admin-Netzwerkschnittstellen für einen einzelnen Knoten oder als Grid-Netzwerkschnittstelle für einen Knoten und die Client-Netzwerkschnittstelle für einen anderen.

Sie können diese Aufgabe auf unterschiedliche Weise ausführen. Wenn es sich bei Ihren Hosts beispielsweise um virtuelle Maschinen handelt und Sie für jeden Host einen oder zwei StorageGRID-Nodes bereitstellen, können Sie die korrekte Anzahl an Netzwerkschnittstellen im Hypervisor erstellen und eine 1:1-Zuordnung verwenden. Wenn Sie mehrere Nodes auf Bare-Metal-Hosts für die Produktion implementieren, können Sie die Unterstützung des Linux-Netzwerk-Stacks für VLAN und LACP nutzen, um Fehlertoleranz und Bandbreitenfreigabe zu erhalten. Die folgenden Abschnitte enthalten detaillierte Ansätze für beide Beispiele. Sie müssen keines dieser Beispiele verwenden; Sie können jeden Ansatz verwenden, der Ihren Anforderungen entspricht.



Verwenden Sie keine Bond- oder Bridge-Geräte direkt als Container-Netzwerkschnittstelle. Dies könnte den Anlauf eines Knotens verhindern, der durch ein Kernel-Problem verursacht wurde, indem MACLAN mit Bond- und Bridge-Geräten im Container-Namespace verwendet wird. Verwenden Sie stattdessen ein Gerät ohne Bindung, z. B. ein VLAN- oder ein virtuelles Ethernet-Paar (veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Node-Konfigurationsdatei an.

Überlegungen und Empfehlungen zum Klonen von MAC-Adressen

Das Klonen VON MAC-Adressen bewirkt, dass der Container die MAC-Adresse des Hosts verwendet und der Host die MAC-Adresse entweder einer von Ihnen angegebenen oder einer zufällig generierten Adresse verwendet. Verwenden Sie das Klonen von MAC-Adressen, um Netzwerkkonfigurationen im einfach zu vermeiden.

Aktivieren des MAC-Klonens

In bestimmten Umgebungen kann die Sicherheit durch das Klonen von MAC-Adressen erhöht werden, da es Ihnen ermöglicht, eine dedizierte virtuelle NIC für das Admin-Netzwerk, das Grid-Netzwerk und das Client-Netzwerk zu verwenden. Wenn der Container die MAC-Adresse der dedizierten NIC auf dem Host nutzen soll, können Sie keine Kompromissmodus-Netzwerkkonfigurationen mehr verwenden.



Das Klonen DER MAC-Adresse wurde für Installationen virtueller Server entwickelt und funktioniert möglicherweise nicht ordnungsgemäß bei allen Konfigurationen der physischen Appliance.



Wenn ein Knoten nicht gestartet werden kann, weil eine gezielte Schnittstelle für das MAC-Klonen belegt ist, müssen Sie die Verbindung möglicherweise auf „down“ setzen, bevor Sie den Knoten starten. Darüber hinaus kann es vorkommen, dass die virtuelle Umgebung das Klonen von MAC auf einer Netzwerkschnittstelle verhindert, während der Link aktiv ist. Wenn ein Knoten die MAC-Adresse nicht einstellt und aufgrund einer überlasteten Schnittstelle gestartet wird, kann das Problem durch Setzen des Links auf „down“ vor dem Starten des Knotens behoben werden.

Das Klonen VON MAC-Adressen ist standardmäßig deaktiviert und muss durch Knoten-Konfigurationsschlüssel festgelegt werden. Sie sollten die Aktivierung bei der Installation von StorageGRID aktivieren.

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 NIC des Hosts. Außerdem verwendet der Host dann die MAC-Adresse des angegebenen Containernetzwerks. Standardmäßig ist die Container-Adresse eine zufällig generierte Adresse, jedoch wenn Sie mithilfe des eine Adresse festgelegt haben `_NETWORK_MAC` Der Node-Konfigurationsschlüssel, diese Adresse wird stattdessen verwendet. Host und Container haben immer unterschiedliche MAC-Adressen.



Wenn das MAC-Klonen auf einem virtuellen Host aktiviert wird, ohne dass gleichzeitig der einfach austauschbare Modus auf dem Hypervisor aktiviert werden muss, kann dies dazu führen, dass Linux-Host-Netzwerke, die die Host-Schnittstelle verwenden, nicht mehr funktionieren.

Anwendungsfälle für DAS Klonen VON MAC

Es gibt zwei Anwendungsfälle, die beim Klonen von MAC berücksichtigt werden müssen:

- MAC-Klonen nicht aktiviert: Wenn der `_CLONE_MAC` Der Schlüssel in der Node-Konfigurationsdatei ist nicht festgelegt oder auf „false“ gesetzt. Der Host verwendet die Host-NIC-MAC und der Container verfügt über eine von StorageGRID generierte MAC, sofern im keine MAC angegeben ist `_NETWORK_MAC` Taste. Wenn im eine Adresse festgelegt ist `_NETWORK_MAC` Schlüssel, der Container wird die Adresse im angegeben `_NETWORK_MAC` Taste. Diese Schlüsselkonfiguration erfordert den Einsatz des promiskuitiven Modus.
- MAC-Klonen aktiviert: Wenn der `_CLONE_MAC` Schlüssel in der Node-Konfigurationsdatei ist auf „true“ gesetzt, der Container verwendet die Host-NIC MAC und der Host verwendet eine von StorageGRID generierte MAC, es sei denn, eine MAC wird im angegeben `_NETWORK_MAC` Taste. Wenn im eine Adresse festgelegt ist `_NETWORK_MAC` Schlüssel, der Host verwendet die angegebene Adresse anstelle einer generierten. In dieser Konfiguration von Schlüsseln sollten Sie nicht den promiskuous Modus verwenden.



Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen erlauben möchten, Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen zu empfangen und zu übertragen, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppen für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen auf **Accept** gesetzt sind. Die auf dem virtuellen Switch eingestellten Werte können von den Werten auf der Portgruppenebene außer Kraft gesetzt werden. Stellen Sie also sicher, dass die Einstellungen an beiden Stellen identisch sind.

Informationen zum Aktivieren des MAC-Klonens finden Sie im ["Anweisungen zum Erstellen von Node-Konfigurationsdateien"](#).

BEISPIEL FÜR DAS Klonen VON MAC

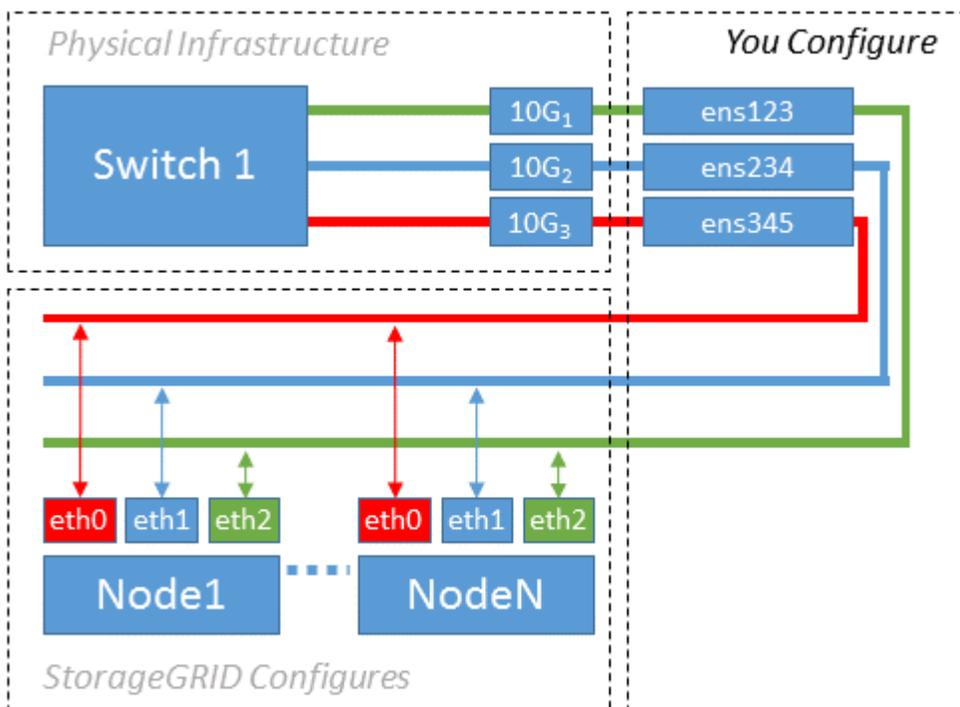
Beispiel für das MAC-Klonen bei einem Host mit einer MAC-Adresse von 11:22:33:44:55:66 für die Schnittstelle ens256 und die folgenden Schlüssel in der Node-Konfigurationsdatei:

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

Ergebnis: Der 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

In Beispiel 1 wird eine einfache Zuordnung von physischen Schnittstellen beschrieben, wofür nur wenig oder keine Host-seitige Konfiguration erforderlich ist.



Das Linux-Betriebssystem erstellt die ensXYZ-Schnittstellen automatisch während der Installation oder beim Start oder beim Hot-Added-Hinzufügen der Schnittstellen. Es ist keine andere Konfiguration erforderlich als sicherzustellen, dass die Schnittstellen nach dem Booten automatisch eingerichtet werden. Sie müssen

ermitteln, welcher enXYZ dem StorageGRID-Netzwerk (Raster, Administrator oder Client) entspricht, damit Sie später im Konfigurationsprozess die korrekten Zuordnungen bereitstellen können.

Beachten Sie, dass in der Abbildung mehrere StorageGRID Nodes angezeigt werden. Normalerweise werden diese Konfigurationen jedoch für VMs mit einem Node verwendet.

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

Beispiel 2: LACP Bond mit VLANs

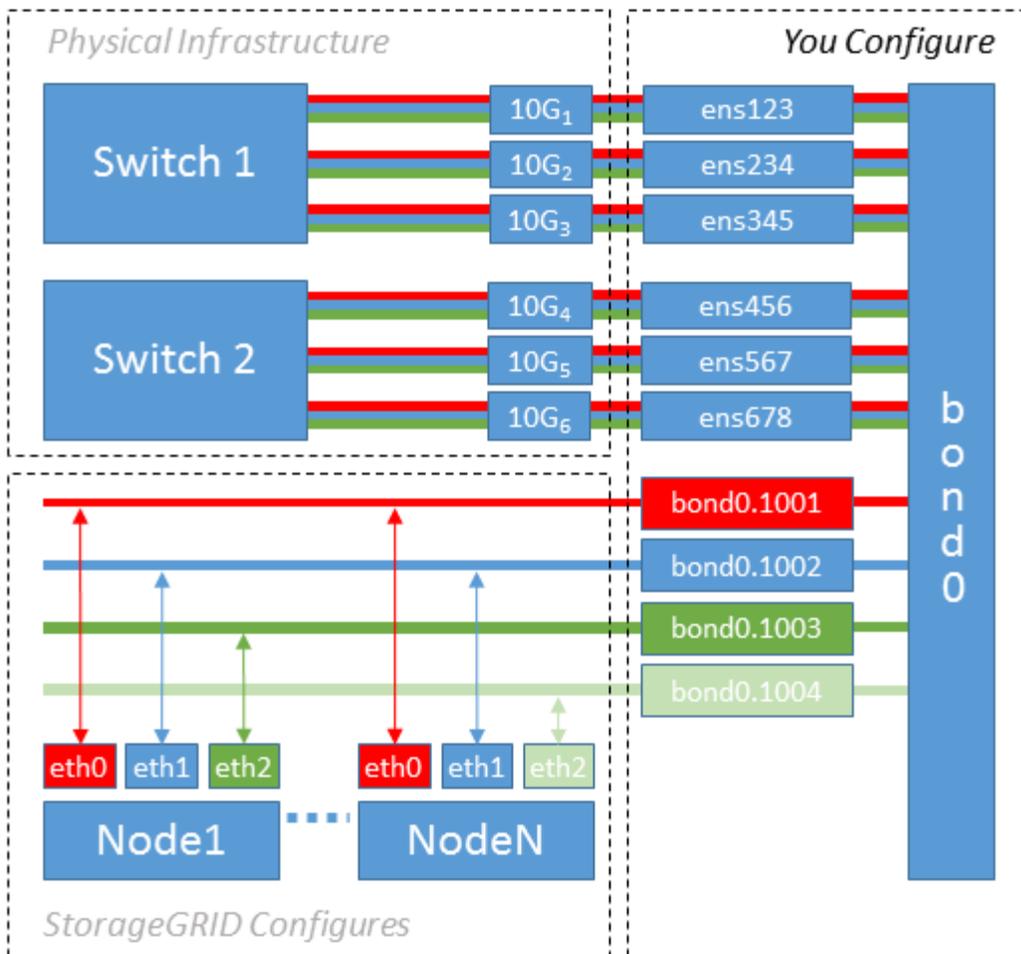
Beispiel 2 geht davon aus, dass Sie mit der Verbindung von Netzwerkschnittstellen und der Erstellung von VLAN-Schnittstellen auf der von Ihnen verwendeten Linux-Distribution vertraut sind.

Über diese Aufgabe

Beispiel 2 beschreibt ein generisches, flexibles, VLAN-basiertes Schema, das die gemeinsame Nutzung aller verfügbaren Netzwerkbandbreite über alle Nodes auf einem einzelnen Host ermöglicht. Dieses Beispiel gilt insbesondere für Bare-Metal-Hosts.

Um dieses Beispiel zu verstehen, stellen Sie vor, Sie verfügen über drei separate Subnetze für Grid, Admin und Client-Netzwerke in jedem Rechenzentrum. Die Subnetze sind in getrennten VLANs (1001, 1002 und 1003) angesiedelt und werden dem Host auf einem LACP-gebundenen Trunk-Port (bond0) präsentiert. Sie würden drei VLAN-Schnittstellen auf der Verbindung konfigurieren: Bond0.1001, bond0.1002 und bond0.1003.

Wenn für Node-Netzwerke auf demselben Host separate VLANs und Subnetze erforderlich sind, können Sie auf der Verbindung VLAN-Schnittstellen hinzufügen und sie dem Host zuordnen (in der Abbildung als bond0.1004 dargestellt).



Schritte

1. Aggregieren Sie alle physischen Netzwerkschnittstellen, die für die StorageGRID-Netzwerkverbindung in einer einzigen LACP-Verbindung verwendet werden.

Verwenden Sie denselben Namen für die Verbindung auf jedem Host, z. B. bond0.

2. Erstellen Sie VLAN-Schnittstellen, die diese Verbindung als ihr zugehöriges „physisches Gerät verwenden,“ using the standard VLAN interface naming convention ``physdev-name.VLAN ID`.

Beachten Sie, dass für die Schritte 1 und 2 eine entsprechende Konfiguration an den Edge-Switches erforderlich ist, die die anderen Enden der Netzwerkverbindungen beenden. Die Edge-Switch-Ports müssen auch zu LACP-Port-Kanälen aggregiert, als Trunk konfiguriert und alle erforderlichen VLANs übergeben werden können.

Beispiele für Schnittstellenkonfigurationsdateien für dieses Netzwerkkonfigurationsschema pro Host werden bereitgestellt.

Verwandte Informationen

["Beispiel /etc/Netzwerk/Schnittstellen"](#)

Hostspeicher konfigurieren

Jedem Host müssen Block Storage Volumes zugewiesen werden.

Bevor Sie beginnen

Sie haben die folgenden Themen behandelt, die Ihnen Informationen liefern, die Sie für diese Aufgabe benötigen:

["Storage- und Performance-Anforderungen erfüllt"](#)

["Anforderungen für die Container-Migration für Nodes"](#)

Über diese Aufgabe

Bei der Zuweisung von Block Storage Volumes (LUNs) an Hosts können Sie mithilfe der Tabellen unter „Storage-Anforderungen“ Folgendes ermitteln:

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

Sie verwenden diese Informationen sowie den permanenten Namen, der Linux jedem physischen Volume zugewiesen ist, wenn Sie StorageGRID-Nodes auf dem Host implementieren.



Sie müssen diese Volumes nicht partitionieren, formatieren oder mounten, sondern müssen nur sicherstellen, dass sie für die Hosts sichtbar sind.

Vermeiden Sie die Verwendung von „RAW“-speziellen Gerätedateien (`/dev/sdb`, Zum Beispiel) bei der Zusammenstellung Ihrer Liste von Volume-Namen. Diese Dateien können sich bei einem Neustart des Hosts ändern, was sich auf den ordnungsgemäßen Betrieb des Systems auswirkt. Wenn Sie iSCSI-LUNs und Device Mapper Multipathing verwenden, sollten Sie in der Multipath-Aliase verwenden `/dev/mapper` Verzeichnis, insbesondere wenn Ihre SAN-Topologie redundante Netzwerkpfade zu dem gemeinsam genutzten Storage umfasst. Alternativ können Sie die vom System erstellten Softlinks unter verwenden `/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 unterscheiden sich bei jeder Installation.

Zuweisung freundlicher Namen zu jedem dieser Block-Storage-Volumes zur Vereinfachung der Erstinstallation von StorageGRID und zukünftiger Wartungsarbeiten Wenn Sie den Device Mapper Multipath-Treiber für redundanten Zugriff auf gemeinsam genutzte Speicher-Volumes verwenden, können Sie das verwenden `alias` Feld in Ihrem `/etc/multipath.conf` Datei:

Beispiel:

```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

Dadurch werden die Aliase im als Blockgeräte angezeigt `/dev/mapper` Verzeichnis auf dem Host, mit dem Sie einen freundlichen, einfach validierten Namen angeben können, wenn bei einer Konfiguration oder Wartung ein Block-Speicher-Volume angegeben werden muss.



Wenn Sie gemeinsam genutzten Speicher zur Unterstützung der StorageGRID-Node-Migration einrichten und Device Mapper Multipathing verwenden, können Sie ein Common erstellen und installieren `/etc/multipath.conf` Auf allen zusammengehörige Hosts. Stellen Sie einfach sicher, dass auf jedem Host ein anderes Docker Storage Volume verwendet wird. Die Verwendung von Alias und die Angabe des Ziel-Hostnamen im Alias für jede Docker Storage-Volume-LUN macht dies leicht zu merken und wird empfohlen.

Verwandte Informationen

["Storage- und Performance-Anforderungen erfüllt"](#)

["Anforderungen für die Container-Migration für Nodes"](#)

Konfigurieren des Docker Storage-Volumes

Vor der Installation von Docker muss möglicherweise das Docker Storage Volume formatiert und gemountet werden `/var/lib/docker`.

Über diese Aufgabe

Sie können diese Schritte überspringen, wenn Sie planen, lokalen Speicher für das Docker-Speicher-Volumen zu verwenden und über genügend Speicherplatz auf der Host-Partition mit verfügen `/var/lib`.

Schritte

1. Dateisystem auf dem Docker-Storage-Volumen erstellen:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Mounten des Docker-Storage-Volumens:

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

3. Fügen Sie einen Eintrag für Docker-Storage-Volumen-Gerät zu `/etc/fstab` hinzu.

Mit diesem Schritt wird sichergestellt, dass das Storage Volume nach einem Neustart des Hosts automatisch neu eingebunden wird.

Installation Von Docker

Das StorageGRID System wird unter Linux als Sammlung von Docker Containern ausgeführt. Bevor Sie StorageGRID installieren können, müssen Sie Docker installieren.

Schritte

1. Installieren Sie Docker gemäß den Anweisungen für Ihre Linux-Distribution.



Wenn Docker nicht in Ihrer Linux Distribution enthalten ist, können Sie sie über die Docker Website herunterladen.

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

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

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

```
sudo docker version
```

Die Client- und Server-Versionen müssen 1.11.0 oder höher sein.

Verwandte Informationen

["Hostspeicher konfigurieren"](#)

Installation der StorageGRID Host Services

Sie verwenden das DEB-Paket von StorageGRID, um die StorageGRID-Host-Dienste zu installieren.

Über diese Aufgabe

In diesen Anweisungen wird beschrieben, wie die Host-Services aus den DEB-Paketen installiert werden. Alternativ können Sie die im Installationarchiv enthaltenen APT-Repository-Metadaten verwenden, um die DEB-Pakete Remote zu installieren. Lesen Sie die APT-Repository-Anweisungen für Ihr Linux-Betriebssystem.

Schritte

1. Kopieren Sie die StorageGRID DEB-Pakete auf jeden Ihrer Hosts oder stellen Sie sie auf gemeinsam genutztem Storage bereit.

Legen Sie sie zum Beispiel in die `/tmp` Verzeichnis, damit Sie den Beispielbefehl im nächsten Schritt verwenden können.

2. Melden Sie sich bei jedem Host als Root an oder verwenden Sie ein Konto mit sudo-Berechtigung, und führen Sie die folgenden Befehle aus.

Sie müssen das installieren `images` Paket zuerst, und das `service` Paket 2. Wenn Sie die Pakete in einem anderen Verzeichnis als platziert haben `/tmp`, Ändern Sie den Befehl, um den von Ihnen verwendeten Pfad anzuzeigen.

```
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.

Virtuelle Grid-Nodes implementieren (Ubuntu oder Debian)

Erstellen Sie Knoten-Konfigurationsdateien für Ubuntu oder Debian-Bereitstellungen

Konfigurationsdateien für die Nodes sind kleine Textdateien, die die Informationen liefern, die der StorageGRID-Host-Service benötigt, um einen Node zu starten und eine

Verbindung zu den entsprechenden Netzwerk- und Block-Storage-Ressourcen herzustellen. Node-Konfigurationsdateien werden für virtuelle Nodes verwendet und nicht für Appliance-Nodes verwendet.

Wo lege ich die Knoten-Konfigurationsdateien ab?

Sie müssen die Konfigurationsdatei für jeden StorageGRID-Knoten im platzieren `/etc/storagegrid/nodes` Verzeichnis auf dem Host, auf dem der Knoten ausgeführt wird. Wenn Sie beispielsweise einen Admin-Node, einen Gateway-Node und einen Storage-Node auf Hosta ausführen möchten, müssen Sie die Konfigurationsdateien mit drei Knoten in die Datei legen `/etc/storagegrid/nodes` Auf Hosta. Sie können die Konfigurationsdateien direkt auf jedem Host mit einem Texteditor, wie z. B. vim oder nano, erstellen oder sie an einem anderen Ort erstellen und auf jeden Host verschieben.

Was benenne ich die Node-Konfigurationsdateien?

Die Namen der Konfigurationsdateien sind erheblich. Das Format lautet `node-name.conf`, Wo `node-name` Ist ein Name, den Sie dem Node zuweisen. Dieser Name wird im StorageGRID Installer angezeigt und wird für Knotenwartungsvorgänge, z. B. für Node-Migration, verwendet.

Node-Namen müssen folgende Bedingungen erfüllen:

- Muss eindeutig sein
- Nur mit einem Buchstaben beginnen
- Kann die Zeichen A bis Z und a bis z enthalten
- Kann die Zahlen 0 bis 9 enthalten
- Kann eine oder mehrere Bindestriche enthalten (-)
- Darf nicht mehr als 32 Zeichen enthalten, wobei der nicht enthalten ist `.conf` Erweiterung

Alle Dateien in `/etc/storagegrid/nodes` Die diese Namenskonventionen nicht befolgen, werden vom Host Service nicht geparkt.

Wenn das Grid eine Topologie mit mehreren Standorten geplant ist, ist unter Umständen ein typisches Benennungsschema für Node möglich:

```
site-nodetype-nodenummer.conf
```

Beispielsweise können Sie verwenden `dc1-adm1.conf` Für den ersten Admin-Node in Data Center 1 und `dc2-sn3.conf` Für den dritten Storage-Node in Datacenter 2. Sie können jedoch ein beliebiges Schema verwenden, das Sie mögen, solange alle Knotennamen den Benennungsregeln folgen.

Was befindet sich in einer Node-Konfigurationsdatei?

Die Konfigurationsdateien enthalten Schlüssel-/Wertpaare mit einem Schlüssel und einem Wert pro Zeile. Für jedes Schlüssel-/Wertpaar müssen Sie folgende Regeln einhalten:

- Der Schlüssel und der Wert müssen durch ein Gleichheitszeichen getrennt werden (=) Und optional Whitespace.
- Die Schlüssel können keine Leerzeichen enthalten.
- Die Werte können eingebettete Leerzeichen enthalten.

- Führende oder nachgestellte Leerzeichen werden ignoriert.

Einige Schlüssel sind für jeden Knoten erforderlich, während andere optional sind oder nur für bestimmte Node-Typen erforderlich sind.

Die Tabelle definiert die zulässigen Werte für alle unterstützten Schlüssel. In der mittleren Spalte:

R: Erforderlich + BP: Best Practice + O: Optional

Taste	R, BP ODER O?	Wert
ADMIN_IP	BP	<p>Grid Network IPv4-Adresse des primären Admin-Knotens für das Grid, zu dem dieser Node gehört. Verwenden Sie denselben Wert, den Sie für GRID_NETWORK_IP für den Grid-Node mit NODE_TYPE = VM_Admin_Node und ADMIN_ROLE = Primary angegeben haben. Wenn Sie diesen Parameter nicht angeben, versucht der Node, einen primären Admin-Node mit mDNS zu ermitteln.</p> <p>"Ermitteln der primären Admin-Node durch Grid-Nodes"</p> <p>Hinweis: Dieser Wert wird auf dem primären Admin-Node ignoriert und kann möglicherweise nicht verwendet werden.</p>
ADMIN_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT
ADMIN_NETWORK_ESL	O	<p>Kommagetrennte Liste von Subnetzen in CIDR-Notation, mit denen dieser Knoten über das Admin-Netzwerk-Gateway kommunizieren soll.</p> <p>Beispiel: 172.16.0.0/21,172.17.0.0/21</p>
ADMIN_NETWORK_GATEWAY	O (R)	<p>IPv4-Adresse des lokalen Admin-Netzwerk-Gateways für diesen Node. Muss sich im Subnetz befinden, das von ADMIN_NETWORK_IP und ADMIN_NETWORK_MASKE definiert ist. Dieser Wert wird bei DHCP-konfigurierten Netzwerken ignoriert.</p> <p>Hinweis: Dieser Parameter ist erforderlich, wenn ADMIN_NETWORK_ESL angegeben wird.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_IP	O	<p>IPv4-Adresse dieses Knotens im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>
ADMIN_NETWORK_MAC	O	<p>Die MAC-Adresse für die Admin-Netzwerkschnittstelle im Container.</p> <p>Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert.</p> <p>Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden.</p> <p>Beispiel: b2:9c:02:c2:27:10</p>
ADMIN_NETWORK_MASKE	O	<p>IPv4-Netmask für diesen Node im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>255.255.255.0</p> <p>255.255.248.0</p>

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_MTU	O	<p>Die maximale Übertragungseinheit (MTU) für diesen Knoten im Admin-Netzwerk. Geben Sie nicht an, ob ADMIN_NETWORK_CONFIG = DHCP. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 verwendet.</p> <p>Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei.</p> <p>WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, an den der Knoten angeschlossen ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.</p> <p>Beispiele:</p> <p>1500</p> <p>8192</p>
ADMIN_NETWORK_TARGET	BP	<p>Name des Host-Geräts, das Sie für den Administratornetzwerkzugriff durch den StorageGRID-Knoten verwenden werden. Es werden nur Namen von Netzwerkschnittstellen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den für GRID_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegebenen Namen.</p> <p>Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät oder verwenden Sie ein Bridge- und virtuelles Ethernet-Paar (veth).</p> <p>Best Practice: Geben Sie einen Wert an, selbst wenn dieser Knoten zunächst keine Admin-Netzwerk-IP-Adresse hat. Anschließend können Sie später eine Admin-Netzwerk-IP-Adresse hinzufügen, ohne den Node auf dem Host neu konfigurieren zu müssen.</p> <p>Beispiele:</p> <p>bond0.1002</p> <p>ens256</p>

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_TARGET_TYPE	O	Schnittstelle (Dies ist der einzige unterstützte Wert.)
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	Richtig oder falsch Setzen Sie den Schlüssel auf „true“, damit der StorageGRID-Container die MAC-Adresse der Host-Zielschnittstelle im Admin-Netzwerk verwendet. Best Practice: in Netzwerken, in denen der promiskuios-Modus erforderlich wäre, verwenden Sie stattdessen DEN ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel. Weitere Informationen zum Klonen von MAC: "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red hat Enterprise Linux oder CentOS)" "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"
ADMIN_ROLLE	R	Primärer oder nicht primärer Storage Dieser Schlüssel ist nur erforderlich, wenn NODE_TYPE = VM_Admin_Node; geben Sie ihn nicht für andere Node-Typen an.
BLOCK_DEVICE_AUDIT_LOGS	R	Pfad und Name der Sonderdatei für Blockgeräte, die dieser Node für die persistente Speicherung von Prüfprotokollen verwendet. Dieser Schlüssel ist nur für Nodes mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an. Beispiele: <code>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</code> <code>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</code> <code>/dev/mapper/sgws-adm1-audit-logs</code>

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_RANGEDB_000	R	<p>Pfad und Name der Sonderdatei für das Blockgerät wird dieser Node für den persistenten Objekt-Storage verwenden. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Storage_Node erforderlich; geben Sie ihn nicht für andere Knotentypen an.</p>
BLOCK_DEVICE_RANGEDB_001		
BLOCK_DEVICE_RANGEDB_002		<p>Es ist nur BLOCK_DEVICE_RANGEDB_000 erforderlich; der Rest ist optional. Das für BLOCK_DEVICE_RANGEDB_000 angegebene Blockgerät muss mindestens 4 TB betragen; die anderen können kleiner sein.</p>
BLOCK_DEVICE_RANGEDB_003		
BLOCK_DEVICE_RANGEDB_004		<p>Lassen Sie keine Lücken. Wenn Sie BLOCK_DEVICE_RANGEDB_005 angeben, müssen Sie auch BLOCK_DEVICE_RANGEDB_004 angeben.</p>
BLOCK_DEVICE_RANGEDB_005		<p>Hinweis: Zur Kompatibilität mit bestehenden Bereitstellungen werden zweistellige Schlüssel für aktualisierte Knoten unterstützt.</p>
BLOCK_DEVICE_RANGEDB_006		<p>Beispiele:</p>
BLOCK_DEVICE_RANGEDB_007		<pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre>
BLOCK_DEVICE_RANGEDB_008		<pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre>
BLOCK_DEVICE_RANGEDB_009		<pre>/dev/mapper/sgws-sn1-rangedb-000</pre>
BLOCK_DEVICE_RANGEDB_010		
BLOCK_DEVICE_RANGEDB_011		
BLOCK_DEVICE_RANGEDB_012		
BLOCK_DEVICE_RANGEDB_013		
BLOCK_DEVICE_RANGEDB_014		
BLOCK_DEVICE_RANGEDB_015		

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_TABLES	R	<p>Pfad und Name der Sonderdatei des Blockgerätes, die dieser Knoten für die dauerhafte Speicherung von Datenbanktabellen verwendet. Dieser Schlüssel ist nur für Nodes mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an.</p> <p>Beispiele:</p> <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adm1-tables</pre>
BLOCK_DEVICE_VAR_LOCAL	R	<p>Pfad und Name der Sonderdatei für das Blockgerät wird dieser Node für seinen persistenten Speicher /var/local verwenden.</p> <p>Beispiele:</p> <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-var-local</pre>
CLIENT_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT
CLIENT_NETWORK_GATEWAY	O	<p>IPv4-Adresse des lokalen Client-Netzwerk-Gateways für diesen Node, der sich im Subnetz befinden muss, das durch CLIENT_NETWORK_IP und CLIENT_NETWORK_MASK definiert ist. Dieser Wert wird bei DHCP-konfigurierten Netzwerken ignoriert.</p> <p>Beispiele:</p> <pre>1.1.1.1</pre> <pre>10.224.4.81</pre>

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_IP	O	<p>IPv4-Adresse dieses Knotens im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>
CLIENT_NETWORK_MAC	O	<p>Die MAC-Adresse für die Client-Netzwerkschnittstelle im Container.</p> <p>Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert.</p> <p>Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden.</p> <p>Beispiel: b2:9c:02:c2:27:20</p>
CLIENT_NETWORK_MASK	O	<p>IPv4-Netzmaske für diesen Knoten im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>255.255.255.0</p> <p>255.255.248.0</p>

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_MTU	O	<p>Die maximale Übertragungseinheit (MTU) für diesen Knoten im Client-Netzwerk. Geben Sie nicht an, ob CLIENT_NETWORK_CONFIG = DHCP. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 verwendet.</p> <p>Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei.</p> <p>WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, an den der Knoten angeschlossen ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.</p> <p>Beispiele:</p> <p>1500</p> <p>8192</p>
CLIENT_NETWORK_TARGET	BP	<p>Name des Host-Geräts, das Sie für den Zugriff auf das Client-Netzwerk durch den StorageGRID-Knoten verwenden werden. Es werden nur Namen von Netzwerkschnittstellen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als der für GRID_NETWORK_TARGET oder ADMIN_NETWORK_TARGET angegeben wurde.</p> <p>Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät oder verwenden Sie ein Bridge- und virtuelles Ethernet-Paar (veth).</p> <p>Best Practice: Geben Sie einen Wert an, auch wenn dieser Knoten zunächst keine Client Network IP Adresse hat. Anschließend können Sie später eine Client-Netzwerk-IP-Adresse hinzufügen, ohne den Node auf dem Host neu konfigurieren zu müssen.</p> <p>Beispiele:</p> <p>bond0.1003</p> <p>ens423</p>
CLIENT_NETWORK_TARGET_TYPE	O	<p>Schnittstelle</p> <p>(Dieser Wert wird nur unterstützt.)</p>

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	<p>Richtig oder falsch</p> <p>Setzen Sie den Schlüssel auf „true“, damit der StorageGRID-Container die MAC-Adresse der Host-Zielschnittstelle im Client-Netzwerk verwenden kann.</p> <p>Best Practice: in Netzwerken, in denen der promiskuios-Modus erforderlich wäre, verwenden Sie stattdessen DEN CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel.</p> <p>Weitere Informationen zum Klonen von MAC:</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red hat Enterprise Linux oder CentOS)"</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"</p>
GRID_NETWORK_CONFIG	BP	<p>STATISCH oder DHCP</p> <p>(Ist standardmäßig STATISCH, wenn nicht angegeben.)</p>
GRID_NETWORK_GATEWAY	R	<p>IPv4-Adresse des lokalen Grid-Netzwerk-Gateways für diesen Node, der sich im Subnetz befinden muss, das durch GRID_NETWORK_IP und GRID_NETWORK_MASKE definiert ist. Dieser Wert wird bei DHCP-konfigurierten Netzwerken ignoriert.</p> <p>Wenn das Grid-Netzwerk ein einzelnes Subnetz ohne Gateway ist, verwenden Sie entweder die Standard-Gateway-Adresse für das Subnetz (X.Z.1) oder den GRID_NETWORK_IP-Wert dieses Knotens; jeder Wert wird mögliche zukünftige Grid-Netzwerk-Erweiterungen vereinfachen.</p>
GRID_NETWORK_IP	R	<p>IPv4-Adresse dieses Knotens im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>1.1.1.1</p> <p>10.224.4.81</p>

Taste	R, BP ODER O?	Wert
GRID_NETWORK_MAC	O	<p>Die MAC-Adresse für die Grid-Netzwerkschnittstelle im Container.</p> <p>Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert.</p> <p>Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden.</p> <p>Beispiel: b2 : 9c : 02 : c2 : 27 : 30</p>
GRID_NETWORK_MASKE	O	<p>IPv4-Netzmaske für diesen Knoten im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATIC; geben Sie ihn nicht für andere Werte an.</p> <p>Beispiele:</p> <p>255.255.255.0</p> <p>255.255.248.0</p>
GRID_NETWORK_MTU	O	<p>Die maximale Übertragungseinheit (MTU) für diesen Knoten im Grid-Netzwerk. Geben Sie nicht an, ob GRID_NETWORK_CONFIG = DHCP ist. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 verwendet.</p> <p>Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei.</p> <p>WICHTIG: Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, an den der Knoten angeschlossen ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.</p> <p>WICHTIG: Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung Grid Network MTU mismatch wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.</p> <p>Beispiele:</p> <p>1500 8192</p>

Taste	R, BP ODER O?	Wert
GRID_NETWORK_TARGET	R	<p>Name des Hostgeräts, das Sie für den Netzzugang über den StorageGRID-Knoten verwenden werden. Es werden nur Namen von Netzwerkschnittstellen unterstützt. Normalerweise verwenden Sie einen anderen Schnittstellennamen als den für ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET angegebenen.</p> <p>Hinweis: Verwenden Sie keine Bond- oder Bridge-Geräte als Netzwerkziel. Konfigurieren Sie entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät oder verwenden Sie ein Bridge- und virtuelles Ethernet-Paar (veth).</p> <p>Beispiele:</p> <pre>bond0.1001</pre> <pre>ens192</pre>
GRID_NETWORK_TARGET_TYPE	O	<p>Schnittstelle</p> <p>(Dies ist der einzige unterstützte Wert.)</p>
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	<p>Richtig oder falsch</p> <p>Setzen Sie den Wert des Schlüssels auf „true“, um den StorageGRID-Container dazu zu bringen, die MAC-Adresse der Host-Zielschnittstelle im Grid-Netzwerk zu verwenden.</p> <p>Best Practice: in Netzwerken, in denen der promiscuous-Modus erforderlich wäre, verwenden Sie stattdessen DEN GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel.</p> <p>Weitere Informationen zum Klonen von MAC:</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Red hat Enterprise Linux oder CentOS)"</p> <p>"Überlegungen und Empfehlungen zum Klonen von MAC-Adressen (Ubuntu oder Debian)"</p>

Taste	R, BP ODER O?	Wert
INTERFACE_TARGET_nnnn	O	<p>Name und optionale Beschreibung für eine zusätzliche Schnittstelle, die Sie diesem Node hinzufügen möchten. Jeder Node kann mehrere zusätzliche Schnittstellen hinzugefügt werden.</p> <p>Geben Sie für <i>nnnn</i> eine eindeutige Nummer für jeden Eintrag INTERFACE_TARGET an, den Sie hinzufügen.</p> <p>Geben Sie für den 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 an, die auf der Seite VLAN-Schnittstellen und der Seite HA-Gruppen angezeigt wird.</p> <p>Beispiel: INTERFACE_TARGET_0001=ens256, Trunk</p> <p>Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.</p>
MAXIMUM_RAM	O	<p>Der maximale RAM-Umfang, den dieser Node nutzen darf. Wenn dieser Schlüssel nicht angegeben ist, gelten für den Node keine 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 kleiner als der gesamte RAM des Systems ist.</p> <p>Hinweis: Der RAM-Wert wirkt sich auf den tatsächlich reservierten Metadaten Speicherplatz eines Knotens aus. Siehe "beschreibung des reservierten Speicherplatzes für Metadaten".</p> <p>Das Format für dieses Feld lautet <number><unit>, Wo <unit> Kann sein b, k, m, Oder g.</p> <p>Beispiele:</p> <p>24g</p> <p>38654705664b</p> <p>Hinweis: Wenn Sie diese Option verwenden möchten, müssen Sie Kernel-Unterstützung für Speicher-cgroups aktivieren.</p>

Taste	R, BP ODER O?	Wert
NODE_TYPE	R	<p>Node-Typ:</p> <p>VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway</p>
PORT_NEU ZUORDNEN	O	<p>Ordnet alle von einem Node verwendeten Ports für interne Grid Node-Kommunikation oder externe Kommunikation neu zu. Neuzuordnungen von Ports sind erforderlich, wenn die Netzwerkrichtlinien des Unternehmens einen oder mehrere von StorageGRID verwendete Ports einschränken, wie in beschrieben "Interne Kommunikation mit Grid-Nodes" Oder "Externe Kommunikation".</p> <p>WICHTIG: Weisen Sie die Ports, die Sie für die Konfiguration von Load Balancer Endpunkten verwenden möchten, nicht neu zu.</p> <p>Hinweis: Wenn nur PORT_REMAP eingestellt ist, wird die von Ihnen angegebene Zuordnung sowohl für eingehende als auch für ausgehende Kommunikation verwendet. Wenn AUCH PORT_REMAP_INBOUND angegeben wird, gilt PORT_REMAP nur für ausgehende Kommunikation.</p> <p>Das verwendete Format ist: <network type>/<protocol>/<default port used by grid node>/<new port>, Wo <network type> Ist Grid, Administrator oder Client und das Protokoll tcp oder udp.</p> <p>Beispiel:</p> <p>PORT_REMAP = client/tcp/18082/443</p>

Taste	R, BP ODER O?	Wert
PORT_REMAP_INBOUND	O	<p>Ordnet die eingehende Kommunikation dem angegebenen Port erneut zu. Wenn SIE PORT_REMAP_INBOUND angeben, aber keinen Wert für PORT_REMAP angeben, bleiben die ausgehenden Kommunikationen für den Port unverändert.</p> <p>WICHTIG: Weisen Sie die Ports, die Sie für die Konfiguration von Load Balancer Endpunkten verwenden möchten, nicht neu zu.</p> <p>Das verwendete Format ist: <network type>/<protocol:>/<remapped port >/<default port used by grid node>, Wo <network type> Ist Grid, Administrator oder Client und das Protokoll tcp oder udp.</p> <p>Beispiel:</p> <p>PORT_REMAP_INBOUND = grid/tcp/3022/22</p>

Ermitteln der primären Admin-Node durch Grid-Nodes

Die Grid-Nodes kommunizieren mit dem primären Admin-Node zu Konfiguration und Management. Jeder Grid-Knoten muss die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk kennen.

Um sicherzustellen, dass ein Grid-Node auf den primären Admin-Node zugreifen kann, können Sie bei der Bereitstellung des Node eines der folgenden Schritte ausführen:

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

Die automatische Erkennung des primären Admin-Knotens wird über ein Multicast-Domänennamensystem (mDNS) durchgeführt. Beim ersten Start des primären Admin-Knotens veröffentlicht er seine IP-Adresse mit mDNS. Andere Knoten im selben Subnetz können dann die IP-Adresse abfragen und automatisch erfassen. Da der Multicast-IP-Datenverkehr normalerweise nicht über Subnetze routingfähig ist, können Nodes in anderen Subnetzen die IP-Adresse des primären Admin-Node nicht direkt abrufen.

Wenn Sie die automatische Erkennung verwenden:



- Sie müssen DIE ADMIN_IP-Einstellung für mindestens einen Grid-Node in allen Subnetzen, mit denen der primäre Admin-Node nicht direkt verbunden ist, enthalten. Dieser Grid-Knoten veröffentlicht dann die IP-Adresse des primären Admin-Knotens für andere Knoten im Subnetz, um mit mDNS zu ermitteln.
- Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur den Datenverkehr mehrerer gegossener IP-Daten innerhalb eines Subnetzes unterstützt.

Beispiel für die Node-Konfigurationsdateien

Sie können die Beispiel-Node-Konfigurationsdateien verwenden, die Ihnen bei der Einrichtung der Node-Konfigurationsdateien für Ihr StorageGRID System helfen. Die Beispiele zeigen Node-Konfigurationsdateien für alle Grid-Nodes.

Bei den 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-Node. Wenn Sie die Admin-Netzwerk-IP des primären Admin-Knotens durchsuchen möchten, um die Grid-Konfiguration abzuschließen (z. B. weil das Grid-Netzwerk nicht weitergeleitet wird), müssen Sie die Admin-Netzwerkverbindung für den primären Admin-Node in seiner Node-Konfigurationsdatei konfigurieren. Dies ist im Beispiel dargestellt.



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

Beispiel für primären Admin-Node

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-adm1.conf`

Beispieldateiinhalt:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-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

Beispiel Dateiname: /etc/storagegrid/nodes/dcl-sn1.conf

Beispieldateinhalt:

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dcl-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dcl-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dcl-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dcl-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 Archivknoten

Beispiel Dateiname: /etc/storagegrid/nodes/dcl-ar1.conf

Beispieldateinhalt:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arcl-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Beispiel für Gateway-Node

Beispiel Dateiname: /etc/storagegrid/nodes/dc1-gw1.conf

Beispieldateinhalt:

```
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-Node

Beispiel Dateiname: /etc/storagegrid/nodes/dc1-adm2.conf

Beispieldateinhalt:

```
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
```

StorageGRID-Konfiguration validieren

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 folgenden Befehl auf jedem Host aus:

```
sudo storagegrid node validate all
```

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

```
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 mithilfe von unterdrücken `-q` Oder `--quiet` Optionen in `storagegrid` Befehl (z. B. `storagegrid --quiet...`). Wenn Sie die Ausgabe unterdrücken, hat der Befehl einen Wert ungleich null Exit, wenn Konfigurationswarnungen oder Fehler erkannt wurden.

Wenn die Konfigurationsdateien nicht korrekt sind, werden die Probleme wie im Beispiel gezeigt als **WARNUNG** und **FEHLER** angezeigt. Wenn Konfigurationsfehler gefunden werden, müssen Sie sie korrigieren, bevor Sie mit der Installation fortfahren.

```

Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Starten Sie den StorageGRID Host Service

Um die StorageGRID Nodes zu starten und sicherzustellen, dass sie nach einem Neustart des Hosts neu gestartet werden, müssen Sie den StorageGRID Host Service aktivieren und starten.

Schritte

1. Führen Sie auf jedem Host folgende 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 „not running“ oder „` stopped“ zurückgibt, führen Sie den folgenden Befehl aus:

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

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

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

Grid und vollständige Installation konfigurieren (Ubuntu oder Debian)

Navigieren Sie zum Grid Manager

Mit dem Grid Manager können Sie alle Informationen definieren, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Bevor Sie beginnen

Der primäre Admin-Node muss bereitgestellt werden und die anfängliche Startsequenz abgeschlossen haben.

Schritte

1. Öffnen Sie Ihren Webbrowser, und navigieren Sie zu einer der folgenden Adressen:

```
https://primary_admin_node_ip
```

```
client_network_ip
```

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

```
https://primary_admin_node_ip:8443
```

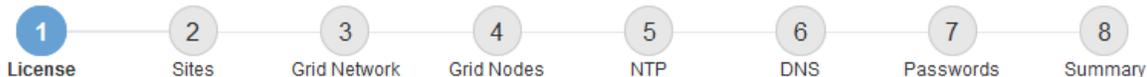


Sie können die IP-Adresse für die primäre Admin-Knoten-IP im Grid-Netzwerk oder im Admin-Netzwerk, je nach Ihrer Netzwerkkonfiguration, verwenden.

2. Wählen Sie **StorageGRID-System installieren**.

Die Seite zum Konfigurieren eines StorageGRID-Systems wird angezeigt.

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Geben Sie die StorageGRID Lizenzinformationen an

Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Schritte

1. Geben Sie auf der Lizenzseite einen aussagekräftigen Namen für Ihr StorageGRID-System in das Feld **Rastername** ein.

Nach der Installation wird der Name oben im Menü Nodes angezeigt.

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

Die Lizenzdatei wird validiert, und die Seriennummer wird angezeigt.



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

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

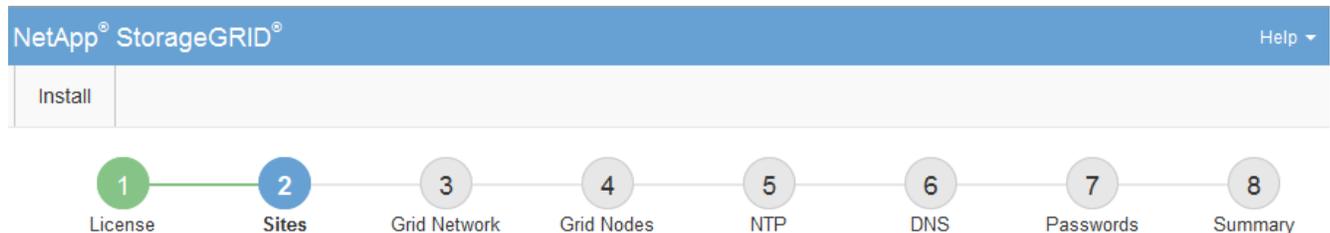
3. Wählen Sie **Weiter**.

Fügen Sie Sites hinzu

Sie müssen mindestens einen Standort erstellen, wenn Sie StorageGRID installieren. Sie können weitere Standorte erstellen, um die Zuverlässigkeit und Storage-Kapazität Ihres StorageGRID Systems zu erhöhen.

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

Fügen Sie so viele zusätzliche Standorte wie für Ihre Grid-Topologie hinzu. Sie können bis zu 16 Standorte hinzufügen.



Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1	<input type="text" value="Raleigh"/>	✕
Site Name 2	<input type="text" value="Atlanta"/>	+ ✕

3. Klicken Sie Auf **Weiter**.

Grid-Netzwerk-Subnetze angeben

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

Über diese Aufgabe

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

Wenn Sie mehrere Grid-Subnetze haben, 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 zusätzlichen Netzwerkeintrag hinzuzufügen.

Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf **Netzwerke-Subnetze ermitteln**, um die Netzwerke-Subnetz-Liste automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die beim Grid Manager registriert sind.

Install



Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1



3. Klicken Sie Auf **Weiter**.

Ausstehende Grid-Nodes genehmigen

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

Bevor Sie beginnen

Sie haben alle virtuellen und StorageGRID Appliance Grid-Nodes implementiert.



Es ist effizienter, eine einzelne Installation aller Nodes durchzuführen, anstatt zu einem späteren Zeitpunkt einige Nodes zu installieren.

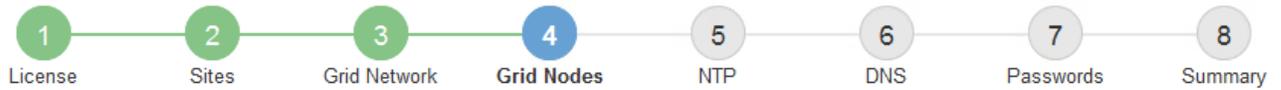
Schritte

1. Prüfen Sie die Liste ausstehender Nodes und bestätigen Sie, dass alle von Ihnen bereitgestellten Grid-Nodes angezeigt werden.



Wenn ein Grid-Node fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

2. Aktivieren Sie das Optionsfeld neben einem Knoten, der noch nicht genehmigt werden soll.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✘ Remove		Search <input type="text"/>		
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
<input checked="" type="radio"/>	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

✎ Edit		🔄 Reset		✘ Remove		Search <input type="text"/>		
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address		
<input type="radio"/>	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21		
<input type="radio"/>	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21		
<input type="radio"/>	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21		
<input type="radio"/>	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21		
<input type="radio"/>	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21		

3. Klicken Sie Auf **Genehmigen**.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften, falls erforderlich:

Storage Node Configuration

General Settings

Site	<input type="text" value="Raleigh"/>
Name	<input type="text" value="NetApp-SGA"/>
NTP Role	<input type="text" value="Automatic"/>
ADC Service	<input type="text" value="Automatic"/>

Grid Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="172.16.5.20/21"/>
Gateway	<input type="text" value="172.16.5.20"/>

Admin Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="10.224.5.20/21"/>
Gateway	<input type="text" value="10.224.0.1"/>
Subnets (CIDR)	<input type="text" value="10.0.0.0/8"/> x
	<input type="text" value="172.19.0.0/16"/> x
	<input type="text" value="172.21.0.0/16"/> + x

Client Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="47.47.5.20/21"/>
Gateway	<input type="text" value="47.47.0.1"/>

- **Standort:** Der Systemname des Standorts für diesen Grid-Knoten.
- **Name:** Der Systemname für den Knoten. Der Name ist standardmäßig auf den Namen eingestellt, den Sie beim Konfigurieren des Nodes angegeben haben.

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

- **NTP-Rolle:** Die NTP-Rolle (Network Time Protocol) des Grid-Knotens. Die Optionen sind **Automatic**, **Primary** und **Client**. Bei Auswahl von **automatisch** wird die primäre Rolle Administratorknoten, Speicherknoten mit ADC-Diensten, Gateway-Nodes und beliebigen Grid-Nodes mit nicht statischen IP-

Adressen zugewiesen. Allen anderen Grid-Nodes wird die Client-Rolle zugewiesen.



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

- **ADC-Dienst** (nur Speicherknoten): Wählen Sie **automatisch** aus, damit das System feststellen kann, ob der Knoten den Dienst Administrative Domain Controller (ADC) benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten. Sie können den ADC-Dienst nicht zu einem Knoten hinzufügen, nachdem er bereitgestellt wurde.

5. Ändern Sie im Grid Network die Einstellungen für die folgenden Eigenschaften, falls erforderlich:

- **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Grid-Netzwerkschnittstelle (eth0 im Container). Zum Beispiel: 192.168.1.234/21
- **Gateway**: Das Grid Network Gateway. Beispiel: 192.168.0.1

Das Gateway ist erforderlich, wenn es mehrere Grid-Subnetze gibt.



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

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

Geben Sie die Zielnetze 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 Konfiguration des Admin-Netzwerks ausgewählt haben und hier den Wert ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die resultierende IP-Adresse nicht in einem DHCP-Adressenpool befindet.

Appliances: Wenn bei einer StorageGRID-Appliance das Admin-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Grid-Manager-Dialogfeld konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

- a. Starten Sie das Gerät neu: Wählen Sie im Appliance Installer die Option **Erweitert > Neustart**.

Ein Neustart kann mehrere Minuten dauern.

- b. Wählen Sie **Netzwerke konfigurieren > Link-Konfiguration** aus, und aktivieren Sie die entsprechenden Netzwerke.
- c. Wählen Sie **Netzwerke konfigurieren > IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.
- d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.

- e. Entfernen Sie im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, 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. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration des Appliance Installer angegeben haben.

Weitere Informationen finden Sie im "[Schnellstart für die Hardwareinstallation](#)" Anleitung für das Gerät finden.

7. Wenn Sie das Client-Netzwerk für den Grid-Node 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 es wird nach der Installation zum Standard-Gateway für den Node.



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

Appliances: Wenn bei einer StorageGRID-Appliance das Client-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Grid-Manager-Dialogfeld konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

- a. Starten Sie das Gerät neu: Wählen Sie im Appliance Installer die Option **Erweitert > Neustart**.

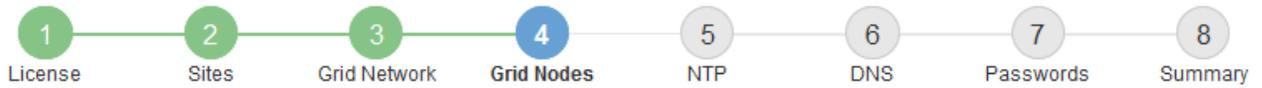
Ein Neustart kann mehrere Minuten dauern.

- b. Wählen Sie **Netzwerke konfigurieren > Link-Konfiguration** aus, und aktivieren Sie die entsprechenden Netzwerke.
- c. Wählen Sie **Netzwerke konfigurieren > IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.
- d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.
- e. Entfernen Sie im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, 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. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration des Appliance Installer angegeben haben.

Informationen zur Installation von StorageGRID Appliances finden Sie im "[Schnellstart für die Hardwareinstallation](#)" Anleitung für das Gerät finden.

8. Klicken Sie Auf **Speichern**.

Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve
✕ Remove

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

◀ ▶

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

✎ Edit
🔄 Reset
✕ Remove

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
<input type="radio"/>	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
<input type="radio"/>	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
<input type="radio"/>	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
<input type="radio"/>	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
<input type="radio"/>	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
<input type="radio"/>	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

◀ ▶

9. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

Sie müssen alle Knoten genehmigen, die Sie im Raster benötigen. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Übersichtsseite auf **Installieren** klicken. Sie können die Eigenschaften eines genehmigten Grid-Knotens ändern, indem Sie das entsprechende Optionsfeld auswählen und auf **Bearbeiten** klicken.

10. Wenn Sie die Genehmigung von Gitterknoten abgeschlossen haben, klicken Sie auf **Weiter**.

Geben Sie Informationen zum Network Time Protocol-Server an

Sie müssen die NTP-Konfigurationsinformationen (Network Time Protocol) für das StorageGRID-System angeben, damit die auf separaten Servern ausgeführten Vorgänge synchronisiert bleiben können.

Über diese Aufgabe

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 Zeitdrift zu vermeiden.



Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer älteren Windows-Version als Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, unterstützt.

["Begrenzung des Supports, um Windows Time Service für hochpräzise Umgebungen zu konfigurieren"](#)

Die externen NTP-Server werden von den Nodes verwendet, denen Sie zuvor primäre NTP-Rollen zugewiesen haben.



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid 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 zusätzliche Servereinträge hinzuzufügen.

The screenshot shows the NetApp StorageGRID installation wizard. The progress bar indicates that step 5, 'NTP', is the current step. Below the progress bar, the 'Network Time Protocol' section is visible. It contains the instruction: 'Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.' There are four input fields labeled 'Server 1' through 'Server 4'. The IP addresses entered are: Server 1: 10.60.248.183, Server 2: 10.227.204.142, Server 3: 10.235.48.111, and Server 4: 0.0.0.0. A plus sign (+) is located to the right of the Server 4 field, indicating that more servers can be added.

3. Wählen Sie **Weiter**.

Verwandte Informationen

["Netzwerkrichtlinien"](#)

Geben Sie die DNS-Serverinformationen an

Sie müssen DNS-Informationen für Ihr StorageGRID-System angeben, damit Sie mit Hostnamen anstelle von IP-Adressen auf externe Server zugreifen können.

Über diese Aufgabe

Angaben "[Informationen zum DNS-Server](#)" Ermöglicht die Verwendung von vollständig qualifizierten Domännennamen (FQDN) anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport.

Um einen ordnungsgemäßen Betrieb zu gewährleisten, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, können aufgrund bekannter Einschränkungen des Betriebssystems auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie dies tun "[Passen Sie die DNS-Serverliste an](#)" Für einzelne Knoten (in der Regel alle Knoten an einem Standort) einen anderen Satz von bis zu drei DNS-Servern verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein Inselstandort die FQDNs für externe Ziele auflösen kann.

Wenn die DNS-Serverinformationen nicht angegeben oder falsch konfiguriert sind, wird ein DNST-Alarm für den SSM-Service jedes Grid-Knotens ausgelöst. Der Alarm wird gelöscht, wenn DNS richtig konfiguriert ist und die neuen Serverinformationen alle Grid-Knoten erreicht haben.

Schritte

1. Geben Sie die IPv4-Adresse für mindestens einen DNS-Server im Textfeld **Server 1** an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um zusätzliche Servereinträge hinzuzufügen.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there is a blue header with the text "NetApp® StorageGRID®" and a "Help" dropdown menu. Below the header is a navigation bar with a tab labeled "Install". A progress indicator consists of eight numbered circles: 1 (License), 2 (Sites), 3 (Grid Network), 4 (Grid Nodes), 5 (NTP), 6 (DNS), 7 (Passwords), and 8 (Summary). The "DNS" step (6) is currently active and highlighted in blue. Below the progress indicator, the section is titled "Domain Name Service". The instructions read: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." There are two input fields for DNS servers. The first field, labeled "Server 1", contains the IP address "10.224.223.130" and has a red "x" icon to its right. The second field, labeled "Server 2", contains the IP address "10.224.223.136" and has a red "+" icon to its right.

Als Best Practice empfehlen wir, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Geben Sie die Passwörter für das StorageGRID-System an

Im Rahmen der Installation des StorageGRID-Systems müssen Sie die Passwörter eingeben, um das System zu sichern und Wartungsarbeiten durchzuführen.

Über diese Aufgabe

Geben Sie auf der Seite Passwörter installieren die Passphrase für die Bereitstellung und das Root-Benutzerpasswort für die Grid-Verwaltung an.

- Die Provisionierungs-Passphrase wird als Verschlüsselungsschlüssel verwendet und nicht vom StorageGRID System gespeichert.
- Sie benötigen die Provisionierungs-Passphrase für Installations-, Erweiterungs- und Wartungsverfahren, einschließlich Download des Recovery-Pakets. Daher ist es wichtig, dass Sie die Provisionierungs-Passphrase an einem sicheren Ort speichern.
- Sie können die Provisionierungs-Passphrase im Grid Manager ändern, wenn Sie die aktuelle haben.
- Das Root-Benutzerpasswort für das Grid-Management kann mit dem Grid Manager geändert werden.
- Zufällig generierte Befehlszeilen-Konsole und SSH-Passwörter werden im gespeichert `passwords.txt` Datei im Wiederherstellungspaket.

Schritte

1. Geben Sie unter **Provisioning-Passphrase** das Provisioning-Passphrase ein, das für Änderungen an der Grid-Topologie Ihres StorageGRID-Systems erforderlich ist.

Speichern Sie die Provisionierungs-Passphrase an einem sicheren Ort.



Wenn Sie nach Abschluss der Installation die Provisionierungs-Passphrase später ändern möchten, können Sie das Grid Manager verwenden. Wählen Sie **KONFIGURATION > Zugangskontrolle > Grid-Passwörter**.

2. Geben Sie unter **Provisioning-Passphrase bestätigen** die Provisionierungs-Passphrase erneut ein, um sie zu bestätigen.
3. Geben Sie unter **Grid Management Root User Password** das Passwort ein, mit dem Sie auf den Grid Manager als „root“-Benutzer zugreifen können.

Speichern Sie das Passwort an einem sicheren Ort.

4. Geben Sie unter **Root-Benutzerpasswort bestätigen** das Grid Manager-Kennwort erneut ein, um es zu bestätigen.

Install



Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase	<input type="password" value="....."/>
Confirm Provisioning Passphrase	<input type="password" value="....."/>
Grid Management Root User Password	<input type="password" value="....."/>
Confirm Root User Password	<input type="password" value="....."/>

Create random command line passwords.

5. Wenn Sie ein Raster für Proof of Concept- oder Demo-Zwecke installieren, deaktivieren Sie optional das Kontrollkästchen **Random Command Line passwords**.

Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Löschen Sie **Create random command line passwords** nur für Demo-Grids, wenn Sie Standardpasswörter verwenden möchten, um über die Befehlszeile mit dem „root“- oder „admin“-Konto auf Grid-Nodes zuzugreifen.



Sie werden aufgefordert, die Recovery Package-Datei herunterzuladen (sgws-recovery-package-id-revision.zip) Nach dem Klick auf **Installieren** auf der Übersichtsseite. Unbedingt "[Laden Sie diese Datei herunter](#)" Um die Installation abzuschließen. Im werden die für den Zugriff auf das System erforderlichen Passwörter gespeichert `Passwords.txt Datei, in der Recovery Package-Datei enthalten.

6. Klicken Sie Auf **Weiter**.

Überprüfung der Konfiguration und vollständige Installation

Sie müssen die von Ihnen eingegebenen Konfigurationsinformationen sorgfältig prüfen, um sicherzustellen, dass die Installation erfolgreich abgeschlossen wurde.

Schritte

1. Öffnen Sie die Seite **Übersicht**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1 dc1-g1 dc1-s1 dc1-s2 dc1-s3 NetApp-SGA		

- Vergewissern Sie sich, dass alle Informationen zur Grid-Konfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite Zusammenfassung, um zurück zu gehen und Fehler zu beheben.
- 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 unterbrochen wird, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Siehe "[Netzwerkrichtlinien](#)" Entsprechende Details.

- Klicken Sie Auf **Download Wiederherstellungspaket**.

Wenn die Installation bis zum Punkt weiterläuft, an dem die Grid-Topologie definiert ist, werden Sie aufgefordert, die Recovery Package-Datei herunterzuladen (.zip), und bestätigen, dass Sie erfolgreich auf den Inhalt dieser Datei zugreifen können. Sie müssen die Recovery Package-Datei herunterladen, damit Sie das StorageGRID-System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Die Installation wird im Hintergrund fortgesetzt, aber Sie können die Installation nicht abschließen und erst auf das StorageGRID-System zugreifen, wenn Sie diese Datei herunterladen und überprüfen.

- Stellen Sie sicher, dass Sie den Inhalt extrahieren können. .zip Speichern Sie die Datei an zwei sicheren und separaten Speicherorten.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

6. Aktivieren Sie das Kontrollkästchen **Ich habe die Wiederherstellungspaket-Datei erfolgreich heruntergeladen und verifiziert**, 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.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Name	Site	Grid Network IPv4 Address	Progress	Stage
dc1-adm1	Site1	172.16.4.215/21	<div style="width: 100%;"><div style="width: 100%;"></div></div>	Starting services
dc1-g1	Site1	172.16.4.216/21	<div style="width: 100%;"><div style="width: 100%;"></div></div>	Complete
dc1-s1	Site1	172.16.4.217/21	<div style="width: 50%;"><div style="width: 50%;"></div></div>	Waiting for Dynamic IP Service peers
dc1-s2	Site1	172.16.4.218/21	<div style="width: 20%;"><div style="width: 20%;"></div></div>	Downloading hotfix from primary Admin if needed
dc1-s3	Site1	172.16.4.219/21	<div style="width: 20%;"><div style="width: 20%;"></div></div>	Downloading hotfix from primary Admin if needed

Wenn die komplette Phase für alle Grid-Knoten erreicht ist, wird die Anmeldeseite für den Grid Manager angezeigt.

7. Melden Sie sich beim Grid Manager mit dem „root“-Benutzer und dem Passwort an, das Sie während der Installation angegeben haben.

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Implementierung und Konfiguration des Grid-Node die folgenden Richtlinien für DHCP-Adressen und Änderungen der Netzwerkkonfiguration.

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

Sie können DHCP nur während der Bereitstellungsphase einrichten. DHCP kann während der Konfiguration nicht eingerichtet werden.



Nodes werden neu gebootet, wenn sich ihre IP-Adressen ändern. Dies kann zu Ausfällen führen, wenn sich eine DHCP-Adresse gleichzeitig auf mehrere Nodes auswirkt.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmaske und Standard-Gateways für einen Grid-Node ändern möchten. Siehe "[Konfigurieren Sie IP-Adressen](#)".
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, geht die Client-Verbindung zum primären Admin-Node und anderen Grid-Nodes unter Umständen verloren. Je nach den vorgenommenen Änderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Automatisieren der Installation (Ubuntu oder Debian)

Die Installation des StorageGRID Host Service und die Konfiguration der Grid-Nodes können automatisiert werden.

Über diese Aufgabe

Eine Automatisierung der Implementierung kann in einem der folgenden Fälle von Nutzen sein:

- Sie verwenden bereits ein Standard-Orchestrierungs-Framework wie Ansible, Puppet oder Chef für die Implementierung und Konfiguration physischer oder virtueller Hosts.
- Sie beabsichtigen, mehrere StorageGRID Instanzen zu implementieren.
- Sie implementieren eine große, komplexe StorageGRID Instanz.

Der StorageGRID Host Service wird durch ein Paket installiert und unterstützt durch Konfigurationsdateien, die während einer manuellen Installation interaktiv erstellt oder vorab (oder programmgesteuert) vorbereitet werden können, um eine automatisierte Installation mithilfe von Standard-Orchestrierungs-Frameworks zu ermöglichen. StorageGRID bietet optionale Python-Skripte zur Automatisierung der Konfiguration von StorageGRID Appliances und dem gesamten StorageGRID-System (das „Grid“). Sie können diese Skripte direkt verwenden oder sie informieren, wie Sie die StorageGRID Installations-REST-API bei den von Ihnen selbst entwickelten Grid-Implementierungs- und Konfigurations-Tools verwenden.

Automatisieren Sie die Installation und Konfiguration des StorageGRID-Host-Service

Die Installation des StorageGRID-Host-Service kann mithilfe von Standard-Orchestrierungs-Frameworks wie Ansible, Puppet, Chef, Fabric oder SaltStack automatisiert werden.

Der StorageGRID-Host-Service befindet sich in einer DEB-Paket und wird durch Konfigurationsdateien bestimmt, die vorab (oder programmgesteuert) für eine automatisierte Installation vorbereitet werden können. Wenn Sie bereits ein Standard-Orchestrierungs-Framework zur Installation und Konfiguration von Ubuntu oder Debian verwenden, sollte das Hinzufügen von StorageGRID zu Playbooks oder Rezepten einfach sein.

Sie können diese Aufgaben automatisieren:

1. Linux Wird Installiert
2. Linux Wird Konfiguriert
3. Konfiguration von Host-Netzwerkschnittstellen zur Erfüllung der StorageGRID Anforderungen
4. Konfiguration von Host-Storage zur Erfüllung von StorageGRID-Anforderungen
5. Installation Von Docker
6. Installation des StorageGRID-Hostservice
7. Konfigurationsdateien für StorageGRID-Knoten werden in erstellt `/etc/storagegrid/nodes`
8. Validieren der StorageGRID-Node-Konfigurationsdateien
9. Starten des StorageGRID Host Service

Beispiel: Ansible-Rolle und Playbook

Beispiel-Rolle und Playbook für Ansible werden im Ordner `/Extras` mit dem Installationsarchiv geliefert. Im Ansible-Playbook wird gezeigt, wie das funktioniert `storagegrid` Rolle bereitet die Hosts vor und installiert StorageGRID auf den Ziel-Servern. Die Rolle oder das Playbook können Sie nach Bedarf anpassen.

Automatisieren Sie die Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Bevor Sie beginnen

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

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

- Sie haben ein erstellt `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`).

Über diese Aufgabe

Sie können das verwenden `configure-storagegrid.py` Python-Skript und das `configure-storagegrid.json` Konfigurationsdatei zur automatischen Konfiguration des StorageGRID Systems



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

Schritte

1. Melden Sie sich an der Linux-Maschine an, die Sie verwenden, um das Python-Skript auszuführen.
2. Wechseln Sie in das Verzeichnis, in dem 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 Recovery-Paket-Datei sichern, damit Sie das StorageGRID-System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Zum Beispiel kopieren Sie den Text auf einen sicheren, gesicherten Netzwerkstandort und an einen sicheren Cloud-Storage-Standort.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

Wenn Sie angegeben haben, dass zufällige Passwörter generiert werden sollen, öffnen Sie die `Passwords.txt` Datei und suchen Sie nach den Kennwörtern, 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.      #####
#####
```

Das StorageGRID System wird installiert und konfiguriert, wenn eine Bestätigungsmeldung angezeigt wird.

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

Verwandte Informationen

["Überblick über DIE REST API zur Installation"](#)

Überblick über DIE REST API zur Installation

StorageGRID stellt die StorageGRID Installations-API für die Durchführung von Installationsaufgaben bereit.

Die API verwendet die Swagger Open Source API-Plattform, um die API-Dokumentation bereitzustellen. Swagger ermöglicht Entwicklern und nicht-Entwicklern die Interaktion mit der API in einer Benutzeroberfläche, die zeigt, 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 mit der API Docs Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Jeder REST-API-Befehl umfasst die URL der API, eine HTTP-Aktion, alle erforderlichen oder optionalen URL-Parameter sowie eine erwartete API-Antwort.

StorageGRID Installations-API

Die StorageGRID Installations-API ist nur verfügbar, wenn Sie das StorageGRID-System zu Beginn konfigurieren und eine primäre Wiederherstellung des Admin-Knotens durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um auf die API-Dokumentation zuzugreifen, gehen Sie auf die Installations-Webseite des primären Admin-Knotens und wählen Sie in der Menüleiste **Hilfe > API-Dokumentation** aus.

Die StorageGRID Installations-API umfasst die folgenden Abschnitte:

- **Config** — Operationen bezogen auf die Produktversion und Versionen der API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Grid** — Konfigurationsvorgänge auf Grid-Ebene. Grid-Einstellungen erhalten und aktualisiert werden, einschließlich Grid-Details, Grid-Netzwerknetzen, Grid-Passwörter und NTP- und DNS-Server-IP-Adressen.
- **Nodes** — Konfigurationsvorgänge auf Node-Ebene. Sie können eine Liste der Grid-Nodes abrufen, einen Grid-Node löschen, einen Grid-Node konfigurieren, einen Grid-Node anzeigen und die Konfiguration eines Grid-Node zurücksetzen.
- **Bereitstellung** — Provisioning Operationen. Sie können den Bereitstellungsverfahren starten und den Status des Bereitstellungsverfahrens anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsverfahrens anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Schemas** — API-Schemata für erweiterte Bereitstellungen
- **Standorte** — Konfigurationsvorgänge auf Standortebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.

Verwandte Informationen

["Automatisierung der Installation"](#)

Weitere Schritte

Führen Sie nach Abschluss einer Installation die erforderlichen Integrations- und Konfigurationsaufgaben aus. Sie können die optionalen Aufgaben nach Bedarf ausführen.

Erforderliche Aufgaben

- ["Erstellen Sie ein Mandantenkonto"](#) Für jedes Client-Protokoll (Swift oder S3), das zum Speichern von Objekten auf Ihrem StorageGRID System verwendet wird.
- ["Kontrolle des Systemzugriffs"](#) Durch das Konfigurieren von Gruppen und Benutzerkonten. Optional können Sie ["Konfigurieren Sie eine föderierte Identitätsquelle"](#) (Z. B. Active Directory oder OpenLDAP), damit Sie Verwaltungsgruppen und Benutzer importieren können. Sie können es auch ["Erstellen Sie lokale Gruppen und Benutzer"](#).
- Integration und Test der ["S3-API"](#) Oder ["Swift-API"](#) Client-Anwendungen, mit denen Sie Objekte auf Ihr StorageGRID-System hochladen.
- ["Konfigurieren Sie die Regeln für Information Lifecycle Management \(ILM\) und die ILM-Richtlinie"](#) Sie möchten zum Schutz von Objektdaten verwenden.
- Wenn Ihre Installation Storage-Nodes der Appliance umfasst, führen Sie mithilfe von SANtricity OS die folgenden Aufgaben aus:
 - Stellen Sie Verbindungen zu jeder StorageGRID Appliance her.
 - Eingang der AutoSupport-Daten überprüfen.

Siehe ["Richten Sie die Hardware ein"](#).

- Überprüfen und befolgen Sie die ["Richtlinien zur StorageGRID-Systemhärtung"](#) Zur Vermeidung von Sicherheitsrisiken.
- ["Konfigurieren Sie E-Mail-Benachrichtigungen für Systemwarnungen"](#).
- Wenn Ihr StorageGRID-System Archivknoten enthält (veraltet), konfigurieren Sie die Verbindung des Archivknotens mit dem externen Archivierungssystem des Ziels.

Optionale Aufgaben

- ["Aktualisieren der IP-Adressen des Grid-Node"](#) Wenn sie sich seit der Planung der Bereitstellung geändert haben und das Wiederherstellungspaket erstellt haben.
- ["Konfigurieren Sie die Speicherverschlüsselung"](#), Bei Bedarf.
- ["Konfigurieren Sie die Storage-Komprimierung"](#) Um die Größe gespeicherter Objekte bei Bedarf zu reduzieren.
- ["Konfigurieren Sie den Zugriff auf das System für Überwachungszwecke"](#) Über eine NFS-Dateifreigabe

Fehlerbehebung bei Installationsproblemen

Falls bei der Installation des StorageGRID-Systems Probleme auftreten, können Sie auf die Installationsprotokolldateien zugreifen. Der technische Support muss möglicherweise auch die Installations-Log-Dateien verwenden, um Probleme zu beheben.

Die folgenden Installationsprotokolldateien sind über den Container verfügbar, auf dem jeder Node ausgeführt wird:

- `/var/local/log/install.log` (Auf allen Grid-Nodes gefunden)
- `/var/local/log/gdu-server.log` (Auf dem primären Admin-Node gefunden)

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"](#).

Verwandte Informationen

["Fehler in einem StorageGRID System beheben"](#)

Beispiel `/etc/Netzwerk/Schnittstellen`

Der `/etc/network/interfaces` Die Datei enthält drei Abschnitte, in denen die physischen Schnittstellen, die Bond-Schnittstelle und die VLAN-Schnittstellen definiert werden. Sie können die drei Beispielabschnitte in einer einzelnen Datei kombinieren, die vier physische Linux-Schnittstellen in einer einzelnen LACP-Verbindung aggregieren wird. Anschließend können Sie drei VLAN-Schnittstellen einrichten, die die Verbindung als StorageGRID Grid, Administrator und Client-Netzwerk-Schnittstellen verwenden.

Physische Schnittstellen

Beachten Sie, dass die Switches an den anderen Enden der Links auch die vier Ports als einzelnen LACP-Trunk oder Port-Kanal behandeln müssen und mindestens drei referenzierte VLANs mit Tags übergeben werden 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
```

VMware installieren

Installieren von VMware: Übersicht

Die Installation eines StorageGRID Systems in einer VMware Umgebung umfasst drei Hauptschritte.

1. **Vorbereitung:** Bei der Planung und Vorbereitung führen Sie folgende Aufgaben aus:
 - Erfahren Sie mehr über die Hardware-, Software-, Virtual Machine-, Storage- und Performance-Anforderungen für StorageGRID.
 - Erfahren Sie mehr über die Besonderheiten von ["StorageGRID Networking"](#) Damit Sie Ihr Netzwerk entsprechend konfigurieren können.
 - Ermitteln und Vorbereiten der physischen Server, die Sie für das Hosten Ihrer StorageGRID Grid Nodes verwenden möchten
 - Auf den Servern, die Sie vorbereitet haben:
 - Installation von VMware vSphere Hypervisor
 - Konfigurieren Sie die ESX Hosts
 - Installation und Konfiguration von VMware vSphere und vCenter
2. **Bereitstellung:** Grid-Knoten mit dem VMware vSphere Web Client bereitstellen. Wenn Sie Grid-Nodes implementieren, werden diese als Teil des StorageGRID Systems erstellt und mit einem oder mehreren Netzwerken verbunden.
 - a. Verwenden Sie den VMware vSphere Web Client, eine VMDK-Datei und eine Reihe von .ovf-Dateivorlagen, um die softwarebasierten Nodes als Virtual Machines (VMs) auf den Servern bereitzustellen, die Sie in Schritt 1 vorbereitet haben.
 - b. Verwenden Sie das Installationsprogramm für StorageGRID Appliance, um StorageGRID Appliance-Nodes bereitzustellen.



Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im StorageGRID Installationsverfahren enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie im ["Schnellstart für die Hardwareinstallation"](#) Anleitung für das Gerät finden.

3. **Konfiguration:** Wenn alle Knoten bereitgestellt wurden, verwenden Sie den Grid Manager, um das Grid zu konfigurieren und die Installation abzuschließen.

Diese Anweisungen empfehlen einen Standardansatz für die Implementierung und Konfiguration eines StorageGRID Systems in einer VMware Umgebung. Siehe auch die Informationen über folgende alternative Ansätze:

- Grid-Nodes in VMware vSphere implementieren – mit dem `deploy-vsphere-ovftool.sh` Bash-Skript (erhältlich im Installationsarchiv)
- Automatisieren Sie die Implementierung und Konfiguration des StorageGRID Systems mit einem Python-Konfigurationsskript (im Installationsarchiv bereitgestellt).
- Automatisieren Sie die Implementierung und Konfiguration von Appliance-Grid-Nodes mit einem Python-Konfigurationsskript (erhältlich über das Installationsarchiv oder über das Installationsprogramm von StorageGRID Appliance).
- Als fortschrittlicher Entwickler von StorageGRID-Implementierungen sollten Sie die Installation VON REST-APIs verwenden, um die Installation von StorageGRID Grid-Nodes zu automatisieren.

Planung und Vorbereitung der VMware Installation

Vor der Installation (VMware)

Bevor Sie Grid-Nodes implementieren und das StorageGRID Grid konfigurieren, müssen Sie die Schritte und Anforderungen für das Durchführen des Verfahrens kennen.

Bei den Implementierungs- und Konfigurationsverfahren für StorageGRID ist bereits die Architektur und die betrieblichen Funktionen des StorageGRID Systems bekannt.

Sie können einen oder mehrere Standorte gleichzeitig implementieren. Alle Standorte müssen jedoch die Mindestanforderungen erfüllen, die für mindestens drei Storage-Nodes bestehen.

Bevor Sie mit der Implementierung eines Node und der Grid-Konfiguration beginnen, müssen Sie:

- Planung der StorageGRID Implementierung
- Installation, Anschluss und Konfiguration der gesamten erforderlichen Hardware – einschließlich aller StorageGRID Appliances – gemäß den Spezifikationen



Wenn bei der StorageGRID-Installation keine StorageGRID Appliance (Hardware) Storage Nodes verwendet werden, müssen Sie Hardware-RAID-Storage mit batteriegestütztem Schreib-Cache (BBWC) verwenden. StorageGRID unterstützt die Verwendung von Virtual Storage Area Networks (VSANs), Software-RAID oder keinen RAID-Schutz.



Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im StorageGRID Installationsverfahren enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie unter ["Appliance-Hardware installieren"](#).

- Verstehen Sie die "[Verfügbare Netzwerkooptionen und wie die einzelnen Netzwerkooptionen in Grid-Nodes implementiert werden sollen](#)".
- Sammeln Sie alle Netzwerkinformationen im Voraus. Sammeln Sie, sofern Sie kein DHCP verwenden, die IP-Adressen für die einzelnen Grid-Nodes sowie die IP-Adressen der zu verwendenden DNS- und NTP-Server.
- Legen Sie fest, welche der verfügbaren Implementierungs- und Konfigurationstools Sie verwenden möchten.

Erforderliche Materialien

Bevor Sie StorageGRID installieren, müssen Sie die erforderlichen Materialien erfassen und vorbereiten.

Element	Hinweise
NetApp StorageGRID Lizenz	Sie benötigen eine gültige, digital signierte NetApp Lizenz. Hinweis: Das StorageGRID Installationsarchiv enthält eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
StorageGRID Installationsarchiv	Unbedingt " Laden Sie das StorageGRID-Installationsarchiv herunter und extrahieren Sie die Dateien ".
VMware Software und Dokumentation	Während der Installation verwenden Sie VMware vSphere Web Client, um virtuelle Grid-Knoten auf Virtual Machines zu implementieren. Informationen zu unterstützten Versionen finden Sie im " NetApp Interoperabilitäts-Matrix-Tool ".
Service-Laptop	Das StorageGRID System wird über einen Service-Laptop installiert. Der Service-Laptop muss Folgendes haben: <ul style="list-style-type: none"> • Netzwerkport • SSH-Client (z. B. PuTTY) • "Unterstützter Webbrowser"
StorageGRID-Dokumentation	<ul style="list-style-type: none"> • "Versionshinweise" • "Anweisungen für die Administration von StorageGRID"

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Sie müssen die StorageGRID-Installationsarchive herunterladen und die Dateien extrahieren.

Schritte

1. Wechseln Sie zum "[NetApp Download-Seite für StorageGRID](#)".
2. Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version, oder wählen Sie eine andere Version aus dem Dropdown-Menü aus und wählen Sie **Go**.

- Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
- Wenn eine Vorsichtshinweis/MustRead-Anweisung angezeigt wird, lesen Sie sie und aktivieren Sie das Kontrollkästchen.



Nachdem Sie die StorageGRID Version installiert haben, müssen Sie alle erforderlichen Hotfixes anwenden. Weitere Informationen finden Sie im ["Hotfix-Verfahren in der Recovery- und Wartungsanleitung"](#)

- Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren** aus.
- Wählen Sie in der Spalte **Install StorageGRID** die .tgz- oder .zip-Datei für VMware aus.



Verwenden Sie die .zip Datei, wenn Windows auf dem Service-Laptop ausgeführt wird.

- Speichern und extrahieren Sie die Archivdatei.
- Wählen Sie aus der folgenden Liste die benötigten Dateien aus.

Die benötigten Dateien hängen von der geplanten Grid-Topologie und der Implementierung des StorageGRID Systems ab.



Die in der Tabelle aufgeführten Pfade beziehen sich auf das Verzeichnis der obersten Ebene, das vom extrahierten Installationsarchiv installiert wird.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	Die Festplattendatei für Virtual Machines, die als Vorlage für die Erstellung von Grid-Node-Virtual Machines verwendet wird.
	Die Vorlagendatei „Open Virtualization Format“ (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung des primären Admin-Knotens.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von nicht-primären Admin-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Archiv-Knoten.

Pfad und Dateiname	Beschreibung
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Gateway-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Zur Bereitstellung von virtuellen Maschinen-basierten Speicher-knoten.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Bash Shell-Skript, das zur Automatisierung der Implementierung virtueller Grid-Nodes verwendet wird.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>deploy-vsphere-ovftool.sh</code> Skript:
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) aktiviert ist. Sie können dieses Skript auch für Ping Federate verwenden.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure

Pfad und Dateiname	Beschreibung
	<p>API-Schemata für StorageGRID:</p> <p>Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.</p>

Softwareanforderungen

Sie können eine Virtual Machine zum Hosten jedes beliebigen Typs des StorageGRID Grid Node verwenden. Für jeden Grid-Node, der auf dem VMware-Server installiert ist, ist eine Virtual Machine erforderlich.

VMware vSphere Hypervisor

Sie müssen VMware vSphere Hypervisor auf einem vorbereiteten physischen Server installieren. Die Hardware muss vor der Installation der VMware Software korrekt konfiguriert sein (einschließlich Firmware-Versionen und BIOS-Einstellungen).

- Zur Unterstützung des Netzwerkes für das zu installierende StorageGRID-System konfigurieren Sie das Netzwerk im Hypervisor nach Bedarf.

"Netzwerkrichtlinien"

- Stellen Sie sicher, dass der Datastore groß genug für die virtuellen Maschinen und virtuellen Festplatten ist, die zum Hosten der Grid-Nodes benötigt werden.
- Wenn Sie mehr als einen Datenspeicher erstellen, benennen Sie jeden Datenspeicher. So können Sie bei der Erstellung von Virtual Machines leicht ermitteln, welchen Datenspeicher für die einzelnen Grid-Nodes verwendet werden soll.

Konfigurationsanforderungen für den ESX Host



Sie müssen das Network Time Protocol (NTP) auf jedem ESX-Host ordnungsgemäß konfigurieren. Wenn die Host-Zeit falsch ist, können negative Auswirkungen, einschließlich Datenverlust, auftreten.

Konfigurationsanforderungen für VMware

Vor der Implementierung von StorageGRID Grid-Nodes müssen Sie VMware vSphere und vCenter installieren und konfigurieren.

Informationen zu unterstützten Versionen von VMware vSphere Hypervisor und VMware vCenter Server-Software finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

Die Schritte zur Installation dieser VMware-Produkte finden Sie in der VMware-Dokumentation.

CPU- und RAM-Anforderungen erfüllt

Überprüfen und konfigurieren Sie vor dem Installieren der StorageGRID Software die Hardware so, dass sie zur Unterstützung des StorageGRID Systems bereit ist.

Informationen zu unterstützten Servern finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

Jeder StorageGRID Node benötigt die folgenden Mindestanforderungen:

- CPU-Cores: 8 pro Node
- RAM: Mindestens 24 GB pro Node und 2 bis 16 GB weniger als der gesamte System-RAM, abhängig von der verfügbaren RAM-Gesamtkapazität und der Anzahl der nicht-StorageGRID-Software, die auf dem System ausgeführt wird

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



Überwachen Sie Ihre CPU- und Arbeitsspeicherauslastung regelmäßig, um sicherzustellen, dass diese Ressourcen Ihre Workloads weiterhin erfüllen. Beispielsweise würde eine Verdoppelung der RAM- und CPU-Zuweisung für virtuelle Storage-Nodes ähnliche Ressourcen bereitstellen wie für die StorageGRID Appliance-Nodes. Wenn die Menge der Metadaten pro Node 500 GB überschreitet, sollten Sie darüber hinaus den RAM pro Node auf 48 GB oder mehr erhöhen. Informationen zum Management von Objekt-Metadaten-Storage, zum Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten und zum Monitoring der CPU- und Arbeitsspeicherauslastung finden Sie in den Anweisungen für ["Administration"](#), ["Monitoring"](#), und ["Aktualisierung"](#) StorageGRID:

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

Wenn Sie Virtual Machines als Hosts verwenden und die Größe und Anzahl der VMs kontrollieren können, sollten Sie für jeden StorageGRID Node eine einzelne VM verwenden und die Größe der VM entsprechend festlegen.

Bei Produktionsimplementierungen sollten nicht mehrere Storage-Nodes auf derselben physischen Speicherhardware oder einem virtuellen Host ausgeführt werden. Jeder Storage-Node in einer einzelnen StorageGRID-Implementierung sollte sich in einer eigenen, isolierten Ausfall-Domäne befinden. Sie können die Langlebigkeit und Verfügbarkeit von Objektdaten maximieren, wenn sichergestellt wird, dass ein einzelner Hardwareausfall nur einen einzelnen Storage-Node beeinträchtigen kann.

Siehe auch ["Storage- und Performance-Anforderungen erfüllt"](#).

Storage- und Performance-Anforderungen erfüllt

Sie müssen die Storage- und Performance-Anforderungen für StorageGRID Nodes kennen, die von Virtual Machines gehostet werden. So können Sie ausreichend Speicherplatz für die anfängliche Konfiguration und die zukünftige Storage-Erweiterung bereitstellen.

Performance-Anforderungen erfüllt

Die Performance des Betriebssystem-Volumes und des ersten Storage Volumes wirkt sich erheblich auf die Gesamt-Performance des Systems aus. Vergewissern Sie sich, dass diese eine ausreichende Festplatten-Performance in Bezug auf Latenz, IOPS (Input/Output Operations per Second) und Durchsatz bieten.

Für alle StorageGRID Nodes ist das BS-Laufwerk und alle Storage Volumes ein Write Back-Caching aktiviert. Der Cache muss sich auf einem geschützten oder persistenten Medium befinden.

Anforderungen für Virtual Machines, die NetApp ONTAP Storage nutzen

Wenn Sie einen StorageGRID-Knoten als Virtual Machine mit Speicher von 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 Datastore für den Node sichert, keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

Anzahl der erforderlichen Virtual Machines

Jeder StorageGRID Standort erfordert mindestens drei Storage-Nodes.



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Storage Node auf einem einzelnen Virtual Machine-Server aus. Die Verwendung eines dedizierten Virtual Machine-Hosts für jeden Storage Node stellt eine isolierte Ausfall-Domäne bereit.

Andere Node-Typen, wie beispielsweise Admin-Nodes oder Gateway-Nodes, können auf demselben Virtual-Machine-Host oder je nach Bedarf auf ihren eigenen dedizierten Virtual-Machine-Hosts implementiert werden. Wenn Sie jedoch mehrere Knoten desselben Typs (z. B. zwei Gateway-Nodes) haben, installieren Sie nicht alle Instanzen auf demselben Host der virtuellen Maschine.

Storage-Anforderungen nach Node-Typ

In einer Produktionsumgebung müssen die Virtual Machines für StorageGRID Grid-Nodes je nach Node-Typ unterschiedliche Anforderungen erfüllen.



Disk Snapshots können nicht zur Wiederherstellung von Grid Nodes verwendet werden. Lesen Sie stattdessen den Abschnitt "[Recovery von Grid Nodes](#)" Verfahren für jeden Node-Typ.

Node-Typ	Storage
Admin-Node	100 GB LUN FÜR OS 200 GB LUN für Admin-Node-Tabellen 200 GB LUN für Admin Node Audit-Protokoll

Node-Typ	Storage
Storage-Node	<p>100 GB LUN FÜR OS</p> <p>3 LUNs für jeden Speicherknoten auf diesem Host</p> <p>Hinweis: Ein Speicherknoten kann 1 bis 16 Speicher-LUNs haben; mindestens 3 Speicher-LUNs werden empfohlen.</p> <p>Mindestgröße pro LUN: 4 TB</p> <p>Maximale getestete LUN-Größe: 39 TB.</p>
Gateway-Node	100 GB LUN FÜR OS
Archiv-Node	100 GB LUN FÜR OS



Je nach konfigurierter Audit-Ebene die Größe der Benutzereingaben wie S3-Objektschlüsselname, Und wie viele Audit-Log-Daten Sie erhalten müssen, müssen Sie möglicherweise die Größe der Audit-Log-LUN auf jedem Admin-Node erhöhen. Im Allgemeinen generiert ein Grid ca. 1 KB Audit-Daten pro S3-Vorgang, Das heißt, eine 200 GB LUN würde 70 Millionen Operationen pro Tag oder 800 Operationen pro Sekunde für zwei bis drei Tage unterstützen.

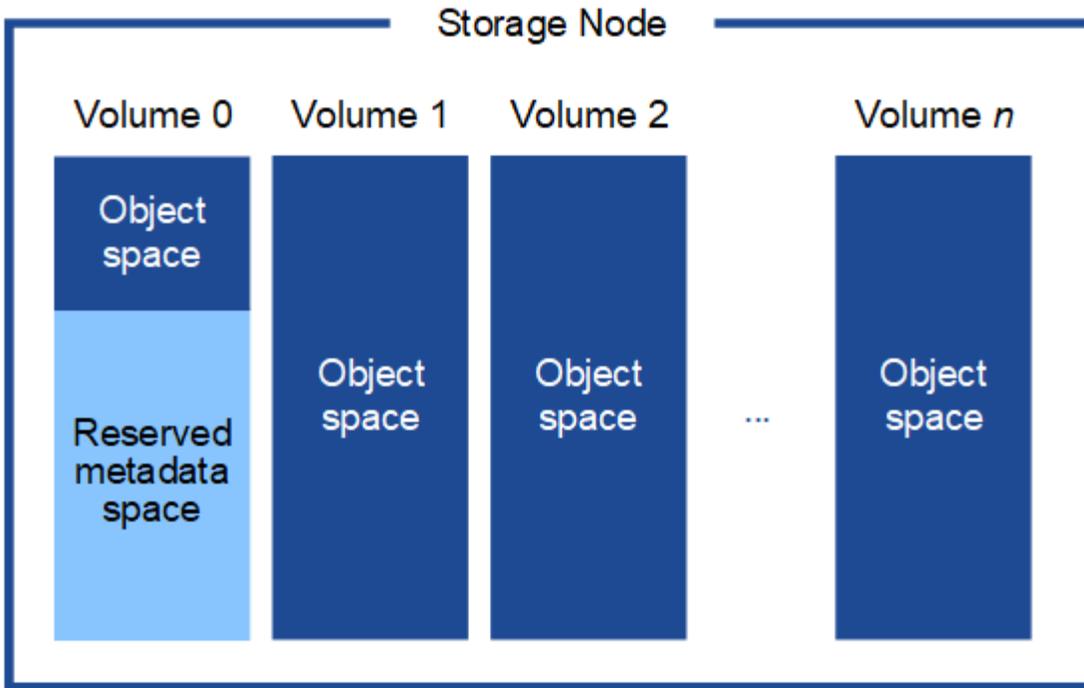
Storage-Anforderungen für Storage-Nodes

Ein softwarebasierter Speicher-Node kann 1 bis 16 Speicher-Volumes haben - -3 oder mehr Speicher-Volumes werden empfohlen. Jedes Storage-Volume sollte 4 TB oder größer sein.



Ein Appliance-Speicherknoten kann bis zu 48 Speicher-Volumes haben.

Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objekt-Metadaten auf dem Storage Volume 0 jedes Storage-Nodes. Alle verbleibenden Speicherplatz auf dem Storage-Volume 0 und anderen Storage-Volumes im Storage-Node werden ausschließlich für Objektdaten verwendet.



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

Wenn Sie Volume 0 eines neuen Storage-Node Speicherplatz zuweisen, müssen Sie sicherstellen, dass für den Anteil aller Objekt-Metadaten des Node ausreichend Speicherplatz vorhanden ist.

- Mindestens müssen Sie Volume 0 mindestens 4 TB zuweisen.



Wenn Sie nur ein Storage-Volume für einen Storage-Node verwenden und dem Volume 4 TB oder weniger zuweisen, hat der Storage-Node beim Start möglicherweise den Schreibgeschützten Storage-Status und speichert nur Objekt-Metadaten.



Wenn Sie Volume 0 weniger als 500 GB zuweisen (nur für den nicht-produktiven Einsatz), sind 10 % der Kapazität des Speicher-Volumes für Metadaten reserviert.

- Wenn Sie ein neues System installieren (StorageGRID 11.6 oder höher) und jeder Speicherknoten mindestens 128 GB RAM hat, weisen Sie Volume 0 mindestens 8 TB zu. Bei Verwendung eines größeren Werts für Volume 0 kann der zulässige Speicherplatz für Metadaten auf jedem Storage Node erhöht werden.
- Verwenden Sie bei der Konfiguration verschiedener Storage-Nodes für einen Standort, falls möglich, die gleiche Einstellung für Volume 0. Wenn ein Standort Storage-Nodes unterschiedlicher Größe enthält, bestimmt der Storage-Node mit dem kleinsten Volume 0 die Metadaten-Kapazität dieses Standorts.

Weitere Informationen finden Sie unter ["Management von Objekt-Metadaten-Storage"](#).

Virtual Machine Grid-Nodes (VMware) implementieren

Erfassen von Informationen über die Bereitstellungsumgebung

Bevor Sie Grid-Nodes bereitstellen, müssen Sie Informationen über Ihre

Netzwerkkonfiguration und die VMware Umgebung erfassen.



Es ist effizienter, eine einzelne Installation aller Nodes durchzuführen, anstatt zu einem späteren Zeitpunkt einige Nodes zu installieren.

VMware Informationen

Sie müssen in die Bereitstellungsumgebung zugreifen und Informationen über die VMware Umgebung, die für Grid, Administrator und Client-Netzwerke erstellten Netzwerke und die Storage-Volume-Typen, die Sie für Storage-Nodes verwenden möchten, sammeln.

Sie müssen Informationen über Ihre VMware Umgebung erfassen. Dazu gehören folgende:

- Benutzername und Passwort für ein VMware vSphere-Konto mit entsprechenden Berechtigungen zum Abschließen der Bereitstellung.
- Informationen zu Host-, Datastore- und Netzwerkkonfiguration für jede StorageGRID Grid-Node Virtual Machine.



VMware Live vMotion bewirkt, dass die Taktzeit der Virtual Machine zu springen und nicht für Grid-Nodes jeglicher Art unterstützt wird. Obwohl selten, falsche Uhrzeiten können zum Verlust von Daten oder Konfigurations-Updates führen.

Informationen zum Grid-Netzwerk

Sie müssen Informationen über das für das StorageGRID Grid-Netzwerk erstellte VMware-Netzwerk erfassen (erforderlich), darunter:

- Der Netzwerkname.
- Wenn Sie kein DHCP verwenden, müssen Sie die erforderlichen Netzwerkdetails für jeden Grid-Node (IP-Adresse, Gateway und Netzwerkmaske) angeben.
- Wenn Sie DHCP nicht verwenden, wird die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk verwendet. Weitere Informationen finden Sie unter „How Grid Nodes discover the primary Admin Node“.

Informationen zum Admin-Netzwerk

Bei Nodes, die mit dem optionalen StorageGRID-Admin-Netzwerk verbunden werden sollen, müssen Sie Informationen über das für dieses Netzwerk erstellte VMware-Netzwerk erfassen. Dazu gehören:

- Der Netzwerkname.
- Die Methode zum Zuweisen von IP-Adressen entweder statisch oder DHCP.
- Wenn Sie statische IP-Adressen verwenden, sind die erforderlichen Netzwerkdetails für jeden Grid-Node (IP-Adresse, Gateway, Netzwerkmaske) erforderlich.
- Die externe Subnetz-Liste (ESL) für das Admin-Netzwerk.

Informationen zum Client-Netzwerk

Bei Nodes, die mit dem optionalen StorageGRID-Clientnetzwerk verbunden werden sollen, müssen Sie Informationen über das für dieses Netzwerk erstellte VMware-Netzwerk erfassen. Dazu gehören:

- Der Netzwerkname.

- Die Methode zum Zuweisen von IP-Adressen entweder statisch oder DHCP.
- Wenn Sie statische IP-Adressen verwenden, sind die erforderlichen Netzwerkdetails für jeden Grid-Node (IP-Adresse, Gateway, Netzwerkmaske) erforderlich.

Informationen zu zusätzlichen Schnittstellen

Nach der Installation des Node können Sie optional Trunk oder Zugriffsschnittstellen zur VM in vCenter hinzufügen. Beispielsweise möchten Sie einem Admin oder Gateway Node eine Trunk-Schnittstelle hinzufügen, sodass Sie den Datenverkehr zwischen verschiedenen Applikationen oder Mandanten über VLAN-Schnittstellen trennen können. Oder auch, wenn Sie eine Access-Schnittstelle hinzufügen möchten, um sie in einer HA-Gruppe (High Availability, Hochverfügbarkeit) zu verwenden.

Die Schnittstellen, die Sie hinzufügen, werden auf der Seite VLAN-Schnittstellen und auf der Seite HA-Gruppen im Grid Manager angezeigt.

- Wenn Sie eine Trunk-Schnittstelle hinzufügen, konfigurieren Sie eine oder mehrere VLAN-Schnittstellen für jede neue übergeordnete Schnittstelle. Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)".
- Wenn Sie eine Zugriffsoberfläche hinzufügen, müssen Sie sie direkt HA-Gruppen hinzufügen. Siehe "[Konfigurieren Sie Hochverfügbarkeitsgruppen](#)".

Storage Volumes für virtuelle Storage-Nodes

Sie müssen die folgenden Informationen für virtuelle Maschinen-basierte Speicherknoten sammeln:

- Die Anzahl und Größe der Storage Volumes (Storage LUNs), die Sie hinzufügen möchten. Siehe „[Storage- und Performance-Anforderungen](#).“

Informationen zur Grid-Konfiguration

Sie müssen Informationen erfassen, um Ihr Raster zu konfigurieren:

- Grid-Lizenz
- IP-Adressen des Network Time Protocol-Servers (NTP)
- IP-Adressen des DNS-Servers

Verwandte Informationen

["Ermitteln der primären Admin-Node durch Grid-Nodes"](#)

["Storage- und Performance-Anforderungen erfüllt"](#)

Ermitteln der primären Admin-Node durch Grid-Nodes

Die Grid-Nodes kommunizieren mit dem primären Admin-Node zu Konfiguration und Management. Jeder Grid-Knoten muss die IP-Adresse des primären Admin-Knotens im Grid-Netzwerk kennen.

Um sicherzustellen, dass ein Grid-Node auf den primären Admin-Node zugreifen kann, können Sie bei der Bereitstellung des Node eines der folgenden Schritte ausführen:

- Sie können den ADMIN_IP-Parameter verwenden, um die IP-Adresse des primären Admin-Knotens manuell einzugeben.
- Sie können den ADMIN_IP-Parameter weglassen, damit der Grid-Node den Wert automatisch ermittelt.

Die automatische Erkennung ist besonders nützlich, wenn das Grid-Netzwerk DHCP verwendet, um die IP-Adresse dem primären Admin-Node zuzuweisen.

Die automatische Erkennung des primären Admin-Knotens wird über ein Multicast-Domänennamensystem (mDNS) durchgeführt. Beim ersten Start des primären Admin-Knotens veröffentlicht er seine IP-Adresse mit mDNS. Andere Knoten im selben Subnetz können dann die IP-Adresse abfragen und automatisch erfassen. Da der Multicast-IP-Datenverkehr normalerweise nicht über Subnetze routingfähig ist, können Nodes in anderen Subnetzen die IP-Adresse des primären Admin-Node nicht direkt abrufen.

Wenn Sie die automatische Erkennung verwenden:



- Sie müssen DIE ADMIN_IP-Einstellung für mindestens einen Grid-Node in allen Subnetzen, mit denen der primäre Admin-Node nicht direkt verbunden ist, enthalten. Dieser Grid-Knoten veröffentlicht dann die IP-Adresse des primären Admin-Knotens für andere Knoten im Subnetz, um mit mDNS zu ermitteln.
- Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur den Datenverkehr mehrerer gegossener IP-Daten innerhalb eines Subnetzes unterstützt.

Implementieren Sie einen StorageGRID Node als Virtual Machine

Sie verwenden VMware vSphere Web Client, um jeden Grid-Knoten als virtuelle Maschine bereitzustellen. Während der Implementierung wird jeder Grid-Node erstellt und mit einem oder mehreren StorageGRID-Netzwerken verbunden.

Wenn Sie Speicherknoten einer StorageGRID-Appliance bereitstellen müssen, finden Sie weitere Informationen unter "[Appliance-Storage-Node implementieren](#)".

Optional können Sie Node-Ports neu zuordnen oder die CPU- oder Speichereinstellungen für den Node erhöhen, bevor Sie den Node einschalten.

Bevor Sie beginnen

- Sie haben die Vorgehensweise überprüft "[Installation planen und vorbereiten](#)" und Sie verstehen die Anforderungen an Software, CPU und RAM sowie Storage und Performance.
- Sie sind mit VMware vSphere Hypervisor vertraut und verfügen über Erfahrung mit der Bereitstellung von Virtual Machines in dieser Umgebung.



Der `open-vm-tools` Paket, eine Open-Source-Implementierung ähnlich wie VMware Tools, ist in der virtuellen StorageGRID-Maschine enthalten. Sie müssen VMware Tools nicht manuell installieren.

- Sie haben die korrekte Version des StorageGRID-Installationsarchivs für VMware heruntergeladen und extrahiert.



Wenn Sie den neuen Node im Rahmen eines Erweiterungs- oder Recovery-Vorgangs implementieren, müssen Sie die Version von StorageGRID verwenden, die derzeit im Grid ausgeführt wird.

- Sie haben das Laufwerk der virtuellen StorageGRID-Maschine (`.vmdk`) Datei:

- Sie haben die `.ovf` Und `.mf` Dateien für jeden Typ von Grid-Node, den Sie implementieren:

Dateiname	Beschreibung
vsphere-Primary-admin.ovf vsphere-Primary-admin.mf	Die Vorlagendatei und die Manifestdatei für den primären Admin-Knoten.
vsphere-nicht-Primary-admin.ovf vsphere-nicht-Primary-admin.mf	Die Vorlagendatei und die Manifestdatei für einen nicht-primären Admin-Knoten.
vsphere-Archive.ovf vsphere-Archive.mf	Die Vorlagendatei und die Manifestdatei für einen Archiv-Knoten.
vsphere-Gateway.ovf vsphere-Gateway.mf	Die Vorlagendatei und die Manifestdatei für einen Gateway-Knoten.
vsphere-Storage.ovf vsphere-Storage.mf	Vorlagendatei und Manifestdatei für einen Speicher-knoten.

- Der `.vdmk`, `.ovf`, und `.mf` Alle Dateien befinden sich im selben Verzeichnis.
- Sie verfügen über einen Plan, um Ausfall-Domains zu minimieren. Sie sollten beispielsweise nicht alle Gateway-Knoten auf einem einzelnen virtuellen Maschinenserver bereitstellen.



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Storage Node auf einem einzelnen Virtual Machine-Server aus. Die Verwendung eines dedizierten Virtual Machine-Hosts für jeden Storage Node stellt eine isolierte Ausfall-Domäne bereit.

- Wenn Sie einen Node im Rahmen eines Erweiterungs- oder Recovery-Vorgangs implementieren, steht Ihnen die zur Verfügung "[Anweisungen zum erweitern eines StorageGRID-Systems](#)" Oder im "[Anweisungen zur Wiederherstellung und Wartung](#)".
- Wenn Sie einen StorageGRID-Knoten als Virtual Machine mit Speicher von 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 Datastore für den Node sichert, keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

Über diese Aufgabe

Befolgen Sie diese Anweisungen, um zunächst VMware Nodes zu implementieren, einen neuen VMware Node in einer Erweiterung hinzuzufügen oder einen VMware Node im Rahmen eines Recovery-Vorgangs zu

ersetzen. Sofern in den Schritten nicht anders angegeben, ist das Verfahren zur Node-Implementierung für alle Node-Typen, einschließlich Admin-Nodes, Storage-Nodes, Gateway-Nodes und Archiv-Nodes, identisch.

Wenn Sie ein neues StorageGRID System installieren:

- Sie müssen den primären Admin-Node bereitstellen, bevor Sie einen anderen Grid-Node bereitstellen.
- Sie müssen sicherstellen, dass jede virtuelle Maschine über das Grid-Netzwerk eine Verbindung zum primären Admin-Node herstellen kann.
- Vor der Konfiguration des Grid müssen Sie alle Grid-Nodes implementieren.

Wenn Sie eine Erweiterung oder Wiederherstellung durchführen:

- Sie müssen sicherstellen, dass die neue virtuelle Maschine über das Grid-Netzwerk eine Verbindung zum primären Admin-Node herstellen kann.

Wenn Sie einen der Node-Ports neu zuordnen müssen, schalten Sie den neuen Node erst ein, wenn die Konfiguration der Port-Neuzuordnung abgeschlossen ist.

Schritte

1. Implementieren Sie mit vCenter eine OVF-Vorlage.

Wenn Sie eine URL angeben, zeigen Sie auf einen Ordner mit den folgenden Dateien. Wählen Sie andernfalls jede dieser Dateien aus einem lokalen Verzeichnis aus.

```
NetApp-SG-version-SHA.vmdk  
vsphere-node.ovf  
vsphere-node.mf
```

Wenn dies beispielsweise der erste Node ist, den Sie bereitstellen, verwenden Sie diese Dateien, um den primären Admin-Node für Ihr StorageGRID-System bereitzustellen:

```
NetApp-SG-version-SHA.vmdk  
sphere-primary-admin.ovf  
sphere-primary-admin.mf
```

2. Geben Sie einen Namen für die virtuelle Maschine ein.

Als Standard-Practice wird derselbe Name sowohl für die Virtual Machine als auch für den Grid-Node verwendet.

3. Platzieren Sie die virtuelle Maschine in die entsprechende vApp oder den entsprechenden Ressourcen-Pool.
4. Wenn Sie den primären Admin-Knoten bereitstellen, lesen Sie die Endbenutzer-Lizenzvereinbarung und akzeptieren Sie diese.

Je nach Ihrer Version von vCenter variieren die Schritte in der Reihenfolge, in der sie die Endbenutzer-Lizenzvereinbarung akzeptieren, den Namen der virtuellen Maschine angeben und einen Datastore auswählen.

5. Wählen Sie Speicher für die virtuelle Maschine aus.

Wenn Sie einen Node im Rahmen der Recovery implementieren, führen Sie die Anweisungen im aus [Storage Recovery-Schritt](#) Um neue virtuelle Festplatten hinzuzufügen, fügen Sie virtuelle Festplatten vom ausgefallenen Grid-Node oder beiden wieder an.

Verwenden Sie bei der Bereitstellung eines Storage-Nodes 3 oder mehr Storage-Volumes, wobei jedes Storage-Volume mindestens 4 TB betragen kann. Sie müssen Volume 0 mindestens 4 TB zuweisen.



Die ovf-Datei Storage Node definiert mehrere VMDKs für den Speicher. Sofern diese VMDKs Ihre Storage-Anforderungen nicht erfüllen, sollten Sie sie entfernen und vor dem Einschalten des Knotens entsprechende VMDKs oder RDMs für den Storage zuweisen. VMDKs sind in VMware-Umgebungen häufiger und einfacher zu managen, während RDMs über 100 MB/s bessere Performance für Workloads mit größeren Objektgrößen bieten können (z. B. über 8 MB).



Einige Installationen von StorageGRID können größere, aktivere Storage Volumes als typische virtualisierte Workloads nutzen. Möglicherweise müssen Sie einige Hypervisor-Parameter einstellen, wie z. B. `MaxAddressableSpaceTB`, Optimale Leistung zu erzielen. Falls die Performance nicht beeinträchtigt wird, wenden Sie sich an Ihre Virtualisierungs-Support-Ressource, um zu ermitteln, ob Ihre Umgebung von Workload-spezifischem KonfigurationTuning profitieren kann.

6. Wählen Sie Netzwerke aus.

Legen Sie fest, welche StorageGRID-Netzwerke der Knoten verwendet, indem Sie ein Zielnetzwerk für jedes Quellnetzwerk auswählen.

- Das Grid-Netzwerk ist erforderlich. Sie müssen ein Zielnetzwerk in der vSphere Umgebung auswählen.
- 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.

7. Konfigurieren Sie unter **Vorlage anpassen** die erforderlichen Eigenschaften für den StorageGRID-Knoten.

a. Geben Sie den **Knotennamen** ein.



Wenn Sie einen Grid-Node wiederherstellen, müssen Sie den Namen des Node eingeben, den Sie wiederherstellen.

b. Wählen Sie im Abschnitt **Grid Network (eth0)** DIE Option STATISCH oder DHCP für die **Grid-Netzwerk-IP-Konfiguration** aus.

- Wenn SIE STATISCH wählen, geben Sie **Grid-Netzwerk-IP**, **Grid-Netzwerkmaske**, **Grid-Netzwerk-Gateway** und **Grid-Netzwerk-MTU** ein.
- Wenn Sie DHCP auswählen, werden die **Grid-Netzwerk-IP**, **Grid-Netzwerkmaske** und **Grid-Netzwerk-Gateway** automatisch zugewiesen.

c. Geben Sie im Feld **Primary Admin IP** die IP-Adresse des primären Admin-Knotens für das Grid Network ein.



Dieser Schritt gilt nicht, wenn der Knoten, den Sie bereitstellen, der primäre Admin-Node ist.

Wenn Sie die IP-Adresse des primären Admin-Knotens auslassen, wird die IP-Adresse automatisch erkannt, wenn der primäre Admin-Node oder mindestens ein anderer Grid-Node mit konfigurierter ADMIN_IP im selben Subnetz vorhanden ist. Es wird jedoch empfohlen, hier die IP-Adresse des primären Admin-Knotens festzulegen.

- a. Wählen Sie im Abschnitt **Admin-Netzwerk (eth1)** DIE Option STATISCH, DHCP oder DEAKTIVIERT für die **Admin-Netzwerk-IP-Konfiguration** aus.
 - Wenn Sie das Admin-Netzwerk nicht verwenden möchten, wählen SIE DEAKTIVIERT aus, und geben Sie **0.0.0.0** für die Admin-Netzwerk-IP ein. Sie können die anderen Felder leer lassen.
 - Wenn SIE STATISCH wählen, geben Sie die Option **Admin-Netzwerk-IP, Admin-Netzwerkmaske, Admin-Netzwerk-Gateway** und **Admin-Netzwerk-MTU** ein.
 - Wenn SIE STATISCH wählen, geben Sie die Liste * Admin Netzwerk External Subnetz list* ein. Außerdem müssen Sie ein Gateway konfigurieren.
 - Wenn Sie DHCP auswählen, werden die **Admin-Netzwerk-IP, Admin-Netzwerkmaske** und **Admin-Netzwerk-Gateway** automatisch zugewiesen.
 - b. Wählen Sie im Abschnitt **Client Network (eth2)** DIE Option STATISCH, DHCP oder DEAKTIVIERT für die **Client-Netzwerk-IP-Konfiguration** aus.
 - Wenn Sie das Client-Netzwerk nicht verwenden möchten, wählen SIE DEAKTIVIERT aus, und geben Sie **0.0.0.0** für die Client-Netzwerk-IP ein. Sie können die anderen Felder leer lassen.
 - Wenn SIE STATISCH wählen, geben Sie **Client-Netzwerk-IP, Client-Netzwerkmaske, Client-Netzwerk-Gateway** und **Client-Netzwerk-MTU** ein.
 - Wenn Sie DHCP auswählen, werden die **Client-Netzwerk-IP, Client-Netzwerkmaske** und **Client-Netzwerk-Gateway** automatisch zugewiesen.
8. Überprüfen Sie die Virtual Machine-Konfiguration und nehmen Sie alle erforderlichen Änderungen vor.
 9. Wenn Sie fertig sind, wählen Sie **Fertig stellen**, um den Upload der virtuellen Maschine zu starten.
 10. Wenn Sie diesen Node im Rahmen des Wiederherstellungsvorgangs bereitgestellt haben und es sich dabei nicht um eine Wiederherstellung mit einem kompletten Node 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 den Speicher bestimmt wurde, und wählen Sie **Entfernen**.
 - c. Je nach Ihren Bedingungen bei der Datenwiederherstellung fügen Sie je nach Ihren Storage-Anforderungen neue virtuelle Festplatten hinzu. Fügen Sie alle virtuellen Festplatten wieder an, die aus dem zuvor entfernten ausgefallenen Grid-Node oder beiden Festplatten erhalten bleiben.

Beachten Sie die folgenden wichtigen Richtlinien:

- Wenn Sie neue Festplatten hinzufügen, sollten Sie denselben Speichertyp verwenden, der vor der Wiederherstellung des Nodes verwendet wurde.
- Die ovf-Datei Storage Node definiert mehrere VMDKs für den Speicher. Sofern diese VMDKs Ihre Storage-Anforderungen nicht erfüllen, sollten Sie sie entfernen und vor dem Einschalten des Knotens entsprechende VMDKs oder RDMs für den Storage zuweisen. VMDKs sind in VMware-Umgebungen häufiger und einfacher zu managen, während RDMs über 100 MB/s bessere

Performance für Workloads mit größeren Objektgrößen bieten können (z. B. über 8 MB).

11. Wenn Sie die von diesem Node verwendeten Ports neu zuordnen müssen, führen Sie die folgenden Schritte aus.

Möglicherweise müssen Sie einen Port neu zuordnen, wenn Ihre Unternehmensrichtlinien den Zugriff auf einen oder mehrere von StorageGRID verwendete Ports einschränken. Siehe "[Netzwerkrichtlinien](#)". Für die von StorageGRID verwendeten Ports.



Weisen Sie die in den Endpunkten des Load Balancer verwendeten Ports nicht neu zu.

- a. Wählen Sie die neue VM aus.
- b. Wählen Sie auf der Registerkarte Konfigurieren die Option **Einstellungen > vApp Optionen**. Der Standort von **vApp Optionen** hängt von der Version von vCenter ab.
- c. Suchen Sie in der Tabelle **Properties** DIE Option PORT_REMAP_INBOUND und PORT_REMAP.
- d. Wenn Sie für einen Port ein- und ausgehende Kommunikation symmetrisch zuordnen möchten, 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 wird, gilt PORT_REMAP nur für ausgehende Kommunikation.

- i. Scrollen Sie zurück nach oben in der Tabelle und wählen Sie **Bearbeiten**.
- ii. Wählen Sie auf der Registerkarte Typ die Option **Benutzer konfigurierbar** aus, und wählen Sie **Speichern**.
- iii. Wählen Sie **Wert Festlegen**.
- iv. Geben Sie die Port-Zuordnung ein:

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type> Ist Grid, Administrator oder Client und <protocol> Ist tcp oder udp.

Um z. B. ssh-Datenverkehr von Port 22 nach Port 3022 neu zuzuweisen, geben Sie Folgendes ein:

```
client/tcp/22/3022
```

- i. Wählen Sie **OK**.

- e. Wählen Sie **PORT_REMAP_INBOUND** aus, um den Port anzugeben, der für die eingehende Kommunikation an den Knoten verwendet wird.



Wenn SIE PORT_REMAP_INBOUND angeben und keinen Wert für PORT_REMAP angeben, bleibt die ausgehende Kommunikation für den Port unverändert.

- i. Scrollen Sie zurück nach oben in der Tabelle und wählen Sie **Bearbeiten**.
- ii. Wählen Sie auf der Registerkarte Typ die Option **Benutzer konfigurierbar** aus, und wählen Sie **Speichern**.
- iii. Wählen Sie **Wert Festlegen**.
- iv. Geben Sie die Port-Zuordnung ein:

`<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>`

`<network type>` Ist Grid, Administrator oder Client und `<protocol>` Ist tcp oder udp.

Um z. B. eingehenden SSH-Datenverkehr neu zuzuweisen, der an Port 3022 gesendet wird, damit er vom Grid-Node an Port 22 empfangen wird, geben Sie Folgendes ein:

```
client/tcp/3022/22
```

i. Wählen Sie **OK**

12. Wenn Sie die CPU oder den Arbeitsspeicher für den Knoten aus den Standardeinstellungen erhöhen möchten:

a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

b. Ändern Sie je nach Bedarf die Anzahl der CPUs oder die Speichergröße.

Stellen Sie die **Speicherreservierung** auf die gleiche Größe wie der **Speicher** ein, der der virtuellen Maschine zugewiesen wurde.

c. Wählen Sie **OK**.

13. Schalten Sie die Virtual Machine ein.

Nachdem Sie fertig sind

Wenn Sie diesen Node im Rahmen eines Erweiterungs- oder Recovery-Verfahrens implementiert haben, kehren Sie zu diesen Anweisungen zurück, um das Verfahren durchzuführen.

Grid-Konfiguration und vollständige Installation (VMware)

Navigieren Sie zum Grid Manager

Mit dem Grid Manager können Sie alle Informationen definieren, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Bevor Sie beginnen

Der primäre Admin-Node muss bereitgestellt werden und die anfängliche Startsequenz abgeschlossen haben.

Schritte

1. Öffnen Sie Ihren Webbrowser, und navigieren Sie zu einer der folgenden Adressen:

```
https://primary_admin_node_ip
```

```
https://client_network_ip
```

Alternativ können Sie auf den Grid Manager an Port 8443 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, je nach Ihrer Netzwerkkonfiguration, verwenden. Möglicherweise müssen Sie die Sicherheits-/erweiterte Option in Ihrem Browser verwenden, um zu einem nicht vertrauenswürdigen Zertifikat zu navigieren.

2. Wählen Sie **StorageGRID-System installieren**.

Die Seite zum Konfigurieren eines StorageGRID-Rasters wird angezeigt.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Geben Sie die StorageGRID Lizenzinformationen an

Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Schritte

1. Geben Sie auf der Lizenzseite einen aussagekräftigen Namen für Ihr StorageGRID-System in das Feld **Rastername** ein.

Nach der Installation wird der Name oben im Menü Nodes angezeigt.

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

Die Lizenzdatei wird validiert, und die Seriennummer wird angezeigt.



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

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name:

License File: NLF-959007-Internal.txt

License Serial Number:

3. Wählen Sie **Weiter**.

Fügen Sie Sites hinzu

Sie müssen mindestens einen Standort erstellen, wenn Sie StorageGRID installieren. Sie können weitere Standorte erstellen, um die Zuverlässigkeit und Storage-Kapazität Ihres StorageGRID Systems zu erhöhen.

Schritte

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

Fügen Sie so viele zusätzliche Standorte wie für Ihre Grid-Topologie hinzu. Sie können bis zu 16 Standorte hinzufügen.

NetApp® StorageGRID® Help ▾

Install

1 License **2** Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1: **x**

Site Name 2: **+ x**

3. Klicken Sie Auf **Weiter**.

Grid-Netzwerk-Subnetze angeben

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

Über diese Aufgabe

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

Wenn Sie mehrere Grid-Subnetze haben, 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 zusätzlichen Netzwerkeintrag hinzuzufügen.

Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf **Netzwerke-Subnetze ermitteln**, um die Netzwerke-Subnetz-Liste automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die beim Grid Manager registriert sind.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there is a blue header with the text 'NetApp® StorageGRID®' and a 'Help' dropdown menu. Below the header is a navigation bar with an 'Install' button. A progress indicator consists of eight numbered circles: 1 (License), 2 (Sites), 3 (Grid Network), 4 (Grid Nodes), 5 (NTP), 6 (DNS), 7 (Passwords), and 8 (Summary). The 'Grid Network' step (3) is currently active and highlighted in blue. Below the progress indicator, the 'Grid Network' section is displayed. It contains the following text: 'You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.' Below this text is a note: 'Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.' The main content area shows a form with a label 'Subnet 1' and a text input field containing '172.16.0.0/21'. To the right of the input field is a plus sign (+). Below the input field is a button labeled 'Discover Grid Network subnets'.

3. Klicken Sie Auf **Weiter**.

Ausstehende Grid-Nodes genehmigen

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

Bevor Sie beginnen

Sie haben alle virtuellen und StorageGRID Appliance Grid-Nodes implementiert.



Es ist effizienter, eine einzelne Installation aller Nodes durchzuführen, anstatt zu einem späteren Zeitpunkt einige Nodes zu installieren.

Schritte

1. Prüfen Sie die Liste ausstehender Nodes und bestätigen Sie, dass alle von Ihnen bereitgestellten Grid-Nodes angezeigt werden.



Wenn ein Grid-Node fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

2. Aktivieren Sie das Optionsfeld neben einem Knoten, der noch nicht genehmigt werden soll.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✘ Remove		Search		Q			
Grid Network MAC Address	↑↓	Name	↑↓	Type	↑↓	Platform	↑↓	Grid Network IPv4 Address	▼
<input checked="" type="radio"/>	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

✎ Edit		↺ Reset		✘ Remove		Search		Q			
Grid Network MAC Address	↑↓	Name	↑↓	Site	↑↓	Type	↑↓	Platform	↑↓	Grid Network IPv4 Address	▼
<input type="radio"/>	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21					
<input type="radio"/>	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21					
<input type="radio"/>	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21					
<input type="radio"/>	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21					
<input type="radio"/>	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21					

3. Klicken Sie Auf **Genehmigen**.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften, falls erforderlich:

Storage Node Configuration

General Settings

Site	<input type="text" value="Raleigh"/>
Name	<input type="text" value="NetApp-SGA"/>
NTP Role	<input type="text" value="Automatic"/>
ADC Service	<input type="text" value="Automatic"/>

Grid Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="172.16.5.20/21"/>
Gateway	<input type="text" value="172.16.5.20"/>

Admin Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="10.224.5.20/21"/>
Gateway	<input type="text" value="10.224.0.1"/>
Subnets (CIDR)	<input type="text" value="10.0.0.0/8"/> x
	<input type="text" value="172.19.0.0/16"/> x
	<input type="text" value="172.21.0.0/16"/> + x

Client Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="47.47.5.20/21"/>
Gateway	<input type="text" value="47.47.0.1"/>

- **Standort:** Der Systemname des Standorts für diesen Grid-Knoten.
- **Name:** Der Systemname für den Knoten. Der Name ist standardmäßig auf den Namen eingestellt, den Sie beim Konfigurieren des Nodes angegeben haben.

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



Bei einem VMware-Knoten können Sie hier den Namen ändern, aber durch diese Aktion wird nicht der Name der virtuellen Maschine in vSphere geändert.

- **NTP-Rolle:** Die NTP-Rolle (Network Time Protocol) des Grid-Knotens. Die Optionen sind **Automatic**, **Primary** und **Client**. Bei Auswahl von **automatisch** wird die primäre Rolle Administratorknoten, Speicherknoten mit ADC-Diensten, Gateway-Nodes und beliebigen Grid-Nodes mit nicht statischen IP-Adressen zugewiesen. Allen anderen Grid-Nodes wird die Client-Rolle zugewiesen.



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

- **ADC-Dienst** (nur Speicherknoten): Wählen Sie **automatisch** aus, damit das System feststellen kann, ob der Knoten den Dienst Administrative Domain Controller (ADC) benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten. Sie können den ADC-Dienst nicht zu einem Knoten hinzufügen, nachdem er bereitgestellt wurde.

5. Ändern Sie im Grid Network die Einstellungen für die folgenden Eigenschaften, falls erforderlich:

- **IPv4-Adresse (CIDR):** Die CIDR-Netzwerkadresse für die Grid-Netzwerkschnittstelle (eth0 im Container). Zum Beispiel: 192.168.1.234/21
- **Gateway:** Das Grid Network Gateway. Beispiel: 192.168.0.1



Das Gateway ist erforderlich, wenn es mehrere Grid-Subnetze gibt.



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

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

Geben Sie die Zielnetze 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 Konfiguration des Admin-Netzwerks ausgewählt haben und hier den Wert ändern, wird der neue Wert als statische Adresse auf dem Knoten konfiguriert. Sie müssen sicherstellen, dass sich die resultierende IP-Adresse nicht in einem DHCP-Adressenpool befindet.

Appliances: Wenn bei einer StorageGRID-Appliance das Admin-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Grid-Manager-Dialogfeld konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

- Starten Sie das Gerät neu: Wählen Sie im Appliance Installer die Option **Erweitert > Neustart**.

Ein Neustart kann mehrere Minuten dauern.

- Wählen Sie **Netzwerke konfigurieren > Link-Konfiguration** aus, und aktivieren Sie die entsprechenden Netzwerke.

- c. Wählen Sie **Netzwerke konfigurieren > IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.
- d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.
- e. Entfernen Sie im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, 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. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration des Appliance Installer angegeben haben.

Weitere Informationen finden Sie im "[Schnellstart für die Hardwareinstallation](#)" Anleitung für das Gerät finden.

7. Wenn Sie das Client-Netzwerk für den Grid-Node 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 es wird nach der Installation zum Standard-Gateway für den Node.



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

Appliances: Wenn bei einer StorageGRID-Appliance das Client-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Grid-Manager-Dialogfeld konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

- a. Starten Sie das Gerät neu: Wählen Sie im Appliance Installer die Option **Erweitert > Neustart**.

Ein Neustart kann mehrere Minuten dauern.

- b. Wählen Sie **Netzwerke konfigurieren > Link-Konfiguration** aus, und aktivieren Sie die entsprechenden Netzwerke.
- c. Wählen Sie **Netzwerke konfigurieren > IP-Konfiguration** und konfigurieren Sie die aktivierten Netzwerke.
- d. Kehren Sie zur Startseite zurück und klicken Sie auf **Installation starten**.
- e. Entfernen Sie im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, 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. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration des Appliance Installer angegeben haben.

Weitere Informationen finden Sie im "[Schnellstart für die Hardwareinstallation](#)" Anleitung für das Gerät finden.

8. Klicken Sie Auf **Speichern**.

Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
<input type="radio"/>	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
<input type="radio"/>	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
<input type="radio"/>	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
<input type="radio"/>	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
<input type="radio"/>	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
<input type="radio"/>	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

9. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

Sie müssen alle Knoten genehmigen, die Sie im Raster benötigen. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Übersichtsseite auf **Installieren** klicken. Sie können die Eigenschaften eines genehmigten Grid-Knotens ändern, indem Sie das entsprechende Optionsfeld auswählen und auf **Bearbeiten** klicken.

10. Wenn Sie die Genehmigung von Gitterknoten abgeschlossen haben, klicken Sie auf **Weiter**.

Geben Sie Informationen zum Network Time Protocol-Server an

Sie müssen die NTP-Konfigurationsinformationen (Network Time Protocol) für das StorageGRID-System angeben, damit die auf separaten Servern ausgeführten Vorgänge synchronisiert bleiben können.

Über diese Aufgabe

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 Zeitdrift zu vermeiden.



Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer älteren Windows-Version als Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, unterstützt.

"Begrenzung des Supports, um Windows Time Service für hochpräzise Umgebungen zu konfigurieren"

Die externen NTP-Server werden von den Nodes verwendet, denen Sie zuvor primäre NTP-Rollen zugewiesen haben.



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

Führen Sie zusätzliche Überprüfungen für VMware durch, beispielsweise um sicherzustellen, dass der Hypervisor dieselbe NTP-Quelle wie die Virtual Machine verwendet, und deaktivieren Sie die Zeitsynchronisierung zwischen dem Hypervisor und den StorageGRID Virtual Machines über VMTools.

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 zusätzliche Servereinträge hinzuzufügen.

The screenshot shows the NetApp StorageGRID installation wizard. At the top, there is a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP (highlighted in blue), 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the "Network Time Protocol" section is visible. It contains the instruction: "Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync." There are four input fields labeled "Server 1" through "Server 4". The values entered are: Server 1: 10.60.248.183, Server 2: 10.227.204.142, Server 3: 10.235.48.111, and Server 4: 0.0.0.0. A plus sign (+) is located to the right of the Server 4 field, indicating that more servers can be added.

3. Wählen Sie **Weiter**.

Geben Sie die DNS-Serverinformationen an

Sie müssen DNS-Informationen für Ihr StorageGRID-System angeben, damit Sie mit Hostnamen anstelle von IP-Adressen auf externe Server zugreifen können.

Über diese Aufgabe

Angeben "[Informationen zum DNS-Server](#)" Ermöglicht die Verwendung von vollständig qualifizierten Domännennamen (FQDN) anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport.

Um einen ordnungsgemäßen Betrieb zu gewährleisten, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, können aufgrund bekannter Einschränkungen des Betriebssystems auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie dies tun "[Passen Sie die DNS-Serverliste an](#)" Für einzelne Knoten (in der Regel alle Knoten an einem Standort) einen anderen Satz von bis zu drei DNS-Servern verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein Inselstandort die FQDNs für externe Ziele auflösen kann.

Wenn die DNS-Serverinformationen nicht angegeben oder falsch konfiguriert sind, wird ein DNST-Alarm für den SSM-Service jedes Grid-Knotens ausgelöst. Der Alarm wird gelöscht, wenn DNS richtig konfiguriert ist und die neuen Serverinformationen alle Grid-Knoten erreicht haben.

Schritte

1. Geben Sie die IPv4-Adresse für mindestens einen DNS-Server im Textfeld **Server 1** an.
2. Wählen Sie bei Bedarf das Pluszeichen neben dem letzten Eintrag aus, um zusätzliche Servereinträge hinzuzufügen.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there is a blue header with "NetApp® StorageGRID®" and a "Help" dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is visible. It contains the following text: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this text are two input fields for DNS servers. The first field is labeled "Server 1" and contains the IP address "10.224.223.130". To its right is a red "x" icon. The second field is labeled "Server 2" and contains the IP address "10.224.223.136". To its right are a red "+" icon and a red "x" icon.

Als Best Practice empfehlen wir, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Geben Sie die Passwörter für das StorageGRID-System an

Im Rahmen der Installation des StorageGRID-Systems müssen Sie die Passwörter eingeben, um das System zu sichern und Wartungsarbeiten durchzuführen.

Über diese Aufgabe

Geben Sie auf der Seite Passwörter installieren die Passphrase für die Bereitstellung und das Root-Benutzerpasswort für die Grid-Verwaltung an.

- Die Provisionierungs-Passphrase wird als Verschlüsselungsschlüssel verwendet und nicht vom StorageGRID System gespeichert.
- Sie benötigen die Provisionierungs-Passphrase für Installations-, Erweiterungs- und Wartungsverfahren, einschließlich Download des Recovery-Pakets. Daher ist es wichtig, dass Sie die Provisionierungs-Passphrase an einem sicheren Ort speichern.
- Sie können die Provisionierungs-Passphrase im Grid Manager ändern, wenn Sie die aktuelle haben.
- Das Root-Benutzerpasswort für das Grid-Management kann mit dem Grid Manager geändert werden.
- Zufällig generierte Befehlszeilen-Konsole und SSH-Passwörter werden im gespeichert `passwords.txt` Datei im Wiederherstellungspaket.

Schritte

1. Geben Sie unter **Provisionierungspassphrase** die Provisionierungs-Passphrase ein, die erforderlich ist, um Änderungen an der Grid-Topologie Ihres StorageGRID-Systems vorzunehmen.

Speichern Sie die Provisionierungs-Passphrase an einem sicheren Ort.



Wenn Sie nach Abschluss der Installation die Provisionierungs-Passphrase später ändern möchten, können Sie das Grid Manager verwenden. Wählen Sie **KONFIGURATION > Zugriffskontrolle > Grid-Passwörter**.

2. Geben Sie unter **Provisioning-Passphrase bestätigen** die Provisionierungs-Passphrase erneut ein, um sie zu bestätigen.
3. Geben Sie unter **Grid Management Root User Password** das Passwort ein, mit dem Sie auf den Grid Manager als „root“-Benutzer zugreifen können.

Speichern Sie das Passwort an einem sicheren Ort.

4. Geben Sie unter **Root-Benutzerpasswort bestätigen** das Grid Manager-Kennwort erneut ein, um es zu bestätigen.

Install



Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase	<input type="password"/>
Confirm Provisioning Passphrase	<input type="password"/>
Grid Management Root User Password	<input type="password"/>
Confirm Root User Password	<input type="password"/>

Create random command line passwords.

5. Wenn Sie ein Raster für Proof of Concept- oder Demo-Zwecke installieren, deaktivieren Sie optional das Kontrollkästchen **Random Command Line passwords**.

Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Löschen Sie **Create random command line passwords** nur für Demo-Grids, wenn Sie Standardpasswörter verwenden möchten, um über die Befehlszeile mit dem „root“- oder „admin“-Konto auf Grid-Nodes zuzugreifen.



Sie werden aufgefordert, die Recovery Package-Datei herunterzuladen (sgws-recovery-package-id-revision.zip) Nach dem Klick auf **Installieren** auf der Übersichtsseite. Unbedingt "[Laden Sie diese Datei herunter](#)" Um die Installation abzuschließen. Im werden die für den Zugriff auf das System erforderlichen Passwörter gespeichert `Passwords.txt` Datei, in der Recovery Package-Datei enthalten.

6. Klicken Sie Auf **Weiter**.

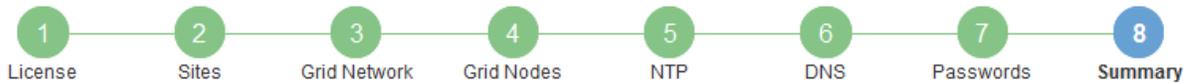
Überprüfung der Konfiguration und vollständige Installation

Sie müssen die von Ihnen eingegebenen Konfigurationsinformationen sorgfältig prüfen, um sicherzustellen, dass die Installation erfolgreich abgeschlossen wurde.

Schritte

1. Öffnen Sie die Seite **Übersicht**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1 dc1-g1 dc1-s1 dc1-s2 dc1-s3 NetApp-SGA		

- Vergewissern Sie sich, dass alle Informationen zur Grid-Konfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite Zusammenfassung, um zurück zu gehen und Fehler zu beheben.
- 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 unterbrochen wird, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Siehe "[Netzwerkrichtlinien](#)" Entsprechende Details.

- Klicken Sie Auf **Download Wiederherstellungspaket**.

Wenn die Installation bis zum Punkt weiterläuft, an dem die Grid-Topologie definiert ist, werden Sie aufgefordert, die Recovery Package-Datei herunterzuladen (.zip), und bestätigen, dass Sie erfolgreich auf den Inhalt dieser Datei zugreifen können. Sie müssen die Recovery Package-Datei herunterladen, damit Sie das StorageGRID-System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Die Installation wird im Hintergrund fortgesetzt, aber Sie können die Installation nicht abschließen und erst auf das StorageGRID-System zugreifen, wenn Sie diese Datei herunterladen und überprüfen.

- Stellen Sie sicher, dass Sie den Inhalt extrahieren können. .zip Speichern Sie die Datei an zwei sicheren und separaten Speicherorten.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

6. Aktivieren Sie das Kontrollkästchen **Ich habe die Wiederherstellungspaket-Datei erfolgreich heruntergeladen und verifiziert**, 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.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Name	Site	Grid Network IPv4 Address	Progress	Stage
dc1-adm1	Site1	172.16.4.215/21	<div style="width: 100%;"><div style="width: 100%;"></div></div>	Starting services
dc1-g1	Site1	172.16.4.216/21	<div style="width: 100%;"><div style="width: 100%;"></div></div>	Complete
dc1-s1	Site1	172.16.4.217/21	<div style="width: 50%;"><div style="width: 50%;"></div></div>	Waiting for Dynamic IP Service peers
dc1-s2	Site1	172.16.4.218/21	<div style="width: 20%;"><div style="width: 20%;"></div></div>	Downloading hotfix from primary Admin if needed
dc1-s3	Site1	172.16.4.219/21	<div style="width: 10%;"><div style="width: 10%;"></div></div>	Downloading hotfix from primary Admin if needed

Wenn die komplette Phase für alle Grid-Knoten erreicht ist, wird die Anmeldeseite für den Grid Manager angezeigt.

7. Melden Sie sich mit dem Benutzer „root“ und dem bei der Installation angegebenen Passwort beim Grid Manager an.

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Implementierung und Konfiguration des Grid-Node die folgenden Richtlinien für DHCP-Adressen und Änderungen der Netzwerkkonfiguration.

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

Sie können DHCP nur während der Bereitstellungsphase einrichten. DHCP kann während der Konfiguration nicht eingerichtet werden.



Nodes werden neu gebootet, wenn sich ihre IP-Adressen ändern. Dies kann zu Ausfällen führen, wenn sich eine DHCP-Adresse gleichzeitig auf mehrere Nodes auswirkt.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmaske und Standard-Gateways für einen Grid-Node ändern möchten. Siehe "[Konfigurieren Sie IP-Adressen](#)".
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, geht die Client-Verbindung zum primären Admin-Node und anderen Grid-Nodes unter Umständen verloren. Je nach den vorgenommenen Änderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Automatisieren der Installation (VMware)

Sie können VMware vSphere verwenden, um die Implementierung von Grid-Nodes zu automatisieren. Außerdem können Sie die Konfiguration von StorageGRID

automatisieren.

Automatisierte Grid Node-Implementierung

Einsatz von VMware vSphere zur Automatisierung der Implementierung von Grid-Nodes

Bevor Sie beginnen

- Sie haben Zugriff auf ein Linux/Unix System mit Bash 3.2 oder höher.
- Sie haben VMware OVF Tool 4.1 installiert und richtig konfiguriert.
- Sie kennen den Benutzernamen und das Kennwort, die für den Zugriff auf VMware vSphere mit dem OVF-Tool erforderlich sind.
- Sie kennen die VI-URL der virtuellen Infrastruktur für den Speicherort in vSphere, wo Sie die StorageGRID Virtual Machines bereitstellen möchten. Bei dieser URL handelt es sich in der Regel um eine vApp oder einen Ressourcen-Pool. Beispiel: `vi://vcenter.example.com/vi/sgws`



Sie können VMware verwenden `ovftool` Dienstprogramm, um diesen Wert zu ermitteln (siehe `ovftool` Dokumentation für Details).



Wenn Sie eine vApp bereitstellen, werden die virtuellen Maschinen nicht automatisch beim ersten Mal gestartet, und Sie müssen sie manuell einschalten.

- Sie haben alle für die Konfigurationsdatei erforderlichen Informationen gesammelt. Siehe ["Erfassen von Informationen über die Bereitstellungsumgebung"](#) Zur Information.
- Sie haben Zugriff auf die folgenden Dateien aus dem VMware Installationsarchiv für StorageGRID:

Dateiname	Beschreibung
NetApp-SG-Version-SHA.vmdk	Die Festplattendatei für Virtual Machines, die als Vorlage für die Erstellung von Grid-Node-Virtual Machines verwendet wird. Hinweis: Diese Datei muss sich im selben Ordner befinden wie der <code>.ovf</code> Und <code>.mf</code> Dateien:
vsphere-Primary-admin.ovf vsphere-Primary-admin.mf	Die Vorlagendatei „Open Virtualization Format“ (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung des primären Admin-Knotens.
vsphere-nicht-Primary-admin.ovf vsphere-nicht-Primary-admin.mf	Die Vorlagendatei (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung von nicht-primären Admin-Knoten.
vsphere-Archive.ovf vsphere-Archive.mf	Die Vorlagendatei (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung von Archiv-Knoten.
vsphere-Gateway.ovf vsphere-Gateway.mf	Die Vorlagendatei (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung von Gateway-Knoten.

Dateiname	Beschreibung
vsphere-Storage.ovf vsphere-Storage.mf	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Zur Bereitstellung von virtuellen Maschinen-basierten Speicherknoten.
deploy-vsphere-ovftool.sh	Das Bash Shell-Skript wird zur Automatisierung der Implementierung virtueller Grid-Nodes verwendet.
deploy-vsphere-ovftool-sample.ini	Die Beispielkonfigurationsdatei für die Verwendung mit dem <code>deploy-vsphere-ovftool.sh</code> Skript:

Legen Sie die Konfigurationsdatei für Ihre Bereitstellung fest

Sie geben die Informationen an, die zum Implementieren der virtuellen Grid-Nodes für StorageGRID in einer Konfigurationsdatei erforderlich sind, die von verwendet wird `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 gleichen Verzeichnis wie `deploy-vsphere-ovftool.sh`.
2. Offen `deploy-vsphere-ovftool.ini`.
3. Geben Sie alle für die Implementierung der virtuellen VMware Grid-Nodes erforderlichen Informationen ein.

Siehe [Konfigurationsdateieinstellungen](#) Zur Information.
4. Wenn Sie alle erforderlichen Informationen eingegeben und verifiziert haben, speichern und schließen Sie die Datei.

Konfigurationsdateieinstellungen

Der `deploy-vsphere-ovftool.ini` Die Konfigurationsdatei enthält die Einstellungen, die für die Implementierung der virtuellen Grid-Nodes erforderlich sind.

In der Konfigurationsdatei werden zunächst die globalen Parameter aufgelistet und anschließend die knotenspezifischen Parameter in Abschnitten aufgelistet, die durch den Knotennamen definiert sind. Wenn die Datei verwendet wird:

- *Globale Parameter* werden auf alle Grid-Knoten angewendet.
- *Node-spezifische Parameter* globale Parameter überschreiben.

Globale Parameter

Globale Parameter werden auf alle Rasterknoten angewendet, es sei denn, sie werden durch Einstellungen in einzelnen Abschnitten außer Kraft gesetzt. Platzieren Sie die Parameter, die für mehrere Knoten gelten, im globalen Parameterabschnitt und überschreiben Sie diese Einstellungen, wie in den Abschnitten für einzelne Knoten erforderlich.

- **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 das verwenden `--powerOffTarget` Und `--overwrite` Optionen zum Herunterfahren und Ersetzen vorhandener Virtual Machines.



Sie sollten Knoten auf verschiedenen Datastores bereitstellen und `OVFTOOL_ARGUMENTE` für jeden Knoten angeben, anstatt global.

- **QUELLE:** Der Pfad zur StorageGRID Virtual Machine Vorlage (`.vmdk`) Datei und die `.ovf` Und `.mf` Dateien für einzelne Grid-Nodes: Dies ist standardmäßig das aktuelle Verzeichnis.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **ZIEL:** Die virtuelle Infrastruktur (vi) von VMware vSphere für den Speicherort, an dem StorageGRID bereitgestellt wird. Beispiel:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG:** Die Methode, mit der IP-Adressen erworben werden, ENTWEDER STATISCH oder DHCP. Die Standardeinstellung IST STATISCH. Wenn alle oder die meisten Knoten dieselbe Methode zum Erwerb von IP-Adressen verwenden, können Sie diese Methode hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
GRID_NETWORK_CONFIG = DHCP
```

- **GRID_NETWORK_TARGET:** Der Name eines vorhandenen VMware-Netzwerks, das für das Grid-Netzwerk verwendet werden soll. Wenn alle oder die meisten Nodes denselben Netzwerknamen verwenden, können Sie ihn hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- **GRID_NETWORK_MASKE:** Die Netzwerkmaske für das Grid-Netzwerk. Wenn alle oder die meisten Nodes dieselbe Netzwerkmaske verwenden, können Sie sie hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY:** Das Netzwerk-Gateway für das Grid-Netzwerk. Wenn alle oder die meisten Nodes dasselbe Netzwerk-Gateway verwenden, können Sie ihn hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU:** OPTIONAL. Die maximale Übertragungseinheit (MTU) im Grid-Netzwerk. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Beispiel:

```
GRID_NETWORK_MTU = 8192
```

Wenn weggelassen wird, wird 1400 verwendet.

Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei.



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.



Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.

- **ADMIN_NETWORK_CONFIG:** Die Methode zum Abrufen von IP-Adressen, entweder DEAKTIVIERT, STATISCH oder DHCP. Die Standardeinstellung IST DEAKTIVIERT. Wenn alle oder die meisten Knoten dieselbe Methode zum Erwerb von IP-Adressen verwenden, können Sie diese Methode hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. 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, es sei denn, das Admin-Netzwerk ist deaktiviert. Wenn alle oder die meisten Nodes denselben Netzwerknamen verwenden, können Sie ihn hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- **ADMIN_NETWORK_MASKE:** Die Netzwerkmaske für das Admin-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie statische IP-Adressen verwenden. Wenn alle oder die meisten Nodes dieselbe Netzwerkmaske verwenden, können Sie sie hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten

festlegen. Beispiel:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY:** Das Netzwerk-Gateway für das Admin-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie statische IP-Adressen verwenden und externe Subnetze in DER EINSTELLUNG ADMIN_NETWORK_ESL angeben. (Das heißt, es ist nicht erforderlich, wenn ADMIN_NETWORK_ESL leer ist.) Wenn alle oder die meisten Nodes dasselbe Netzwerk-Gateway verwenden, können Sie ihn hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL:** Die externe Subnetz-Liste (Routen) für das Admin-Netzwerk, angegeben als kommagetrennte Liste der CIDR-Routenziele. Wenn alle oder die meisten Knoten dieselbe externe Subnetz Liste verwenden, können Sie sie hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. 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. Geben Sie nicht an, ob ADMIN_NETWORK_CONFIG = DHCP. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1400 verwendet. Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei. Wenn alle oder die meisten Knoten dieselbe MTU für das Admin-Netzwerk verwenden, können Sie diese hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG:** Die Methode zum Abrufen von IP-Adressen, entweder DEAKTIVIERT, STATISCH oder DHCP. Die Standardeinstellung IST DEAKTIVIERT. Wenn alle oder die meisten Knoten dieselbe Methode zum Erwerb von IP-Adressen verwenden, können Sie diese Methode hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. 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, es sei denn, das Client-Netzwerk ist deaktiviert. Wenn alle oder die meisten Nodes denselben Netzwerknamen verwenden, können Sie ihn hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- **CLIENT_NETWORK_MASKE:** Die Netzwerkmaske für das Client-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie statische IP-Adressen verwenden. Wenn alle oder die meisten Nodes dieselbe Netzwerkmaske verwenden, können Sie sie hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY:** Das Netzwerk-Gateway für das Client-Netzwerk. Diese Einstellung ist erforderlich, wenn Sie statische IP-Adressen verwenden. Wenn alle oder die meisten Nodes dasselbe Netzwerk-Gateway verwenden, können Sie ihn hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU:** OPTIONAL. Die maximale Übertragungseinheit (MTU) im Client-Netzwerk. Geben Sie nicht an, ob `CLIENT_NETWORK_CONFIG = DHCP`. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1400 verwendet. Wenn Sie Jumbo Frames verwenden möchten, setzen Sie die MTU auf einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert bei. Wenn alle oder die meisten Knoten dieselbe MTU für das Client-Netzwerk verwenden, können Sie diese hier angeben. Sie können die globale Einstellung dann überschreiben, indem Sie unterschiedliche Einstellungen für einen oder mehrere einzelne Knoten festlegen. Beispiel:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP:** Ordnet jeden Port, der von einem Knoten für interne Netzknoten-Kommunikation oder externe Kommunikation verwendet wird, neu zu. Ports müssen neu zugeordnet werden, wenn Netzwerkrichtlinien in Unternehmen eine oder mehrere von StorageGRID verwendete Ports einschränken. Eine Liste der von StorageGRID verwendeten Ports finden Sie unter interne Grid-Node-Kommunikation und externe Kommunikation in "[Netzwerkrichtlinien](#)".



Weisen Sie die Ports, die Sie für die Konfiguration der Load Balancer-Endpunkte verwenden möchten, nicht neu zu.



Wenn nur `PORT_REMAP` festgelegt ist, wird die Zuordnung, die Sie angeben, sowohl für eingehende als auch für ausgehende Kommunikation verwendet. Wenn AUCH `PORT_REMAP_INBOUND` angegeben wird, 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 ist, und das Protokoll tcp oder udp ist.

Beispiel:

```
PORT_REMAP = client/tcp/18082/443
```

Wenn diese Beispieleinstellung allein verwendet wird, ordnet sie symmetrisch ein- und ausgehende Kommunikation für den Grid-Knoten von Port 18082 bis Port 443 zu. Wenn dieses Beispiel zusammen mit `PORT_REMAP_INBOUND` verwendet wird, ordnet die ausgehende Kommunikation von Port 18082 zu Port 443 zu.

- **PORT_REMAP_INBOUND**: Ordnet eingehende Kommunikation für den angegebenen Port neu zu. Wenn SIE `PORT_REMAP_INBOUND` angeben, aber keinen Wert für `PORT_REMAP` angeben, bleiben die ausgehenden Kommunikationen für den Port unverändert.



Weisen Sie die Ports, die Sie für die Konfiguration der Load Balancer-Endpunkte 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 ist, und das Protokoll tcp oder udp ist.

Beispiel:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Dieses Beispiel nimmt den an Port 443 gesendeten Datenverkehr auf, um eine interne Firewall zu übergeben und ihn an Port 18082 zu leiten, wo der Grid-Node auf S3-Anforderungen hört.

Node-spezifische Parameter

Jeder Node befindet sich in einem eigenen Abschnitt der Konfigurationsdatei. Jeder Node muss die folgenden Einstellungen vornehmen:

- Der Abschnittskopf definiert den Knotennamen, der im Grid Manager angezeigt wird. Sie können diesen Wert außer Kraft setzen, indem Sie den optionalen `NODE_NAME` Parameter für den Node angeben.
- **NODE_TYPE**: `VM_Admin_Node`, `VM_Storage_Node`, `VM_Archive_Node` oder `VM_API_Gateway_Node`
- **GRID_NETWORK_IP**: Die IP-Adresse für den Knoten im Grid-Netzwerk.
- **ADMIN_NETWORK_IP**: Die IP-Adresse für den Knoten im Admin-Netzwerk. Erforderlich nur, wenn der Knoten mit dem Admin-Netzwerk verbunden ist und `ADMIN_NETWORK_CONFIG` auf `STATISCH` gesetzt ist.
- **CLIENT_NETWORK_IP**: Die IP-Adresse für den Knoten im Client-Netzwerk. Erforderlich nur, wenn der Knoten mit dem Client-Netzwerk verbunden ist und `CLIENT_NETWORK_CONFIG` für diesen Knoten auf `STATISCH` 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-Node angeben. Wenn Sie diesen Parameter nicht angeben, versucht der Node, die primäre Admin-Node-IP mit mDNS zu ermitteln. Weitere Informationen finden Sie unter "[Ermitteln der primären Admin-Node durch Grid-Nodes](#)".



Der `ADMIN_IP`-Parameter wird für den primären Admin-Node ignoriert.

- Parameter, die nicht global festgelegt wurden. Wenn beispielsweise ein Node mit dem Admin-Netzwerk verbunden ist und Sie ADMIN_NETWORK nicht global angeben, müssen Sie diese für den Node angeben.

Primärer Admin-Node

Für den primären Admin-Node sind folgende zusätzliche Einstellungen erforderlich:

- **NODE_TYPE:** VM_Admin_Node
- **ADMIN_ROLE:** Primär

Dieser Beispieleintrag gilt für einen primären Admin-Knoten, der sich auf allen drei Netzwerken befindet:

```
[DC1-ADM1]
ADMIN_ROLE = Primary
NODE_TYPE = VM_Admin_Node

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 optional für den primären Admin-Knoten:

- **DISK:** Admin Nodes werden standardmäßig zwei zusätzliche 200 GB-Festplatten für Audit und Datenbanknutzung zugewiesen. Diese Einstellungen können Sie mit dem FESTPLATTENPARAMETER erhöhen. Beispiel:

```
DISK = INSTANCES=2, CAPACITY=300
```



Bei Admin-Nodes müssen INSTANZEN immer gleich 2 sein.

Storage-Node

Für Speicherknoten ist die folgende zusätzliche Einstellung erforderlich:

- **NODE_TYPE:** VM_Storage_Node

Dieser Beispieleintrag gilt für einen Speicherknoten, der sich in Grid- und Admin-Netzwerken befindet, aber nicht im Client-Netzwerk. Dieser Knoten verwendet die EINSTELLUNG ADMIN_IP, 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
```

Der zweite Beispieleintrag gilt für einen Speicherknoten in einem Client-Netzwerk, in dem in der unternehmensweiten Netzwerkrichtlinie des Kunden angegeben ist, dass eine S3-Client-Anwendung nur über Port 80 oder 443 auf den Storage-Node zugreifen darf. Die Beispielkonfigurationsdatei verwendet PORT_REMAP, um den Storage Node zum Senden und Empfangen von S3-Meldungen an Port 443 zu aktivieren.

```
[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 Neuordnung für ssh-Verkehr von Port 22 zu Port 3022, legt aber explizit die Werte für den ein- und ausgehenden Datenverkehr 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 folgende zusätzliche Einstellung ist optional für Speicherknoten:

- **DISK:** Standardmäßig werden den Speicherknoten drei 4 TB-Festplatten für die RangeDB-Nutzung zugewiesen. Sie können diese Einstellungen mit dem FESTPLATTENPARAMETER erhöhen. Beispiel:

```
DISK = INSTANCES=16, CAPACITY=4096
```

Archiv-Node

Für Archiv-Knoten ist die folgende zusätzliche Einstellung erforderlich:

- **NODE_TYPE:** VM_Archive_Node

Dieser Beispieleintrag gilt für einen Archiv-Node, der sich auf Grid- und Admin-Netzwerken befindet, jedoch nicht im Client-Netzwerk.

```
[DC1-ARC1]
NODE_TYPE = VM_Archive_Node

GRID_NETWORK_IP = 10.1.0.4
ADMIN_NETWORK_IP = 10.3.0.4

ADMIN_IP = 10.1.0.2
```

Gateway-Node

Für Gateway-Knoten ist die folgende zusätzliche Einstellung erforderlich:

- **NODE_TYPE:** VM_API_GATEWAY

Dieser Beispieleintrag gilt für einen Beispiel-Gateway-Node auf allen drei Netzwerken. In diesem Beispiel wurden im globalen Abschnitt der Konfigurationsdatei keine Client-Netzwerkparameter angegeben, so dass sie für den Knoten angegeben werden müssen:

```
[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-Node

Die folgenden zusätzlichen Einstellungen sind für nicht-primäre Admin-Nodes erforderlich:

- **NODE_TYPE:** VM_Admin_Node
- **ADMIN_ROLE:** Nicht-Primary

Dieser Beispieleintrag gilt für einen nicht-primären Admin-Node, 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 optional für nicht-primäre Admin-Knoten:

- **DISK:** Admin Nodes werden standardmäßig zwei zusätzliche 200 GB-Festplatten für Audit und Datenbanknutzung zugewiesen. Diese Einstellungen können Sie mit dem FESTPLATTENPARAMETER erhöhen. Beispiel:

```
DISK = INSTANCES=2, CAPACITY=300
```



Bei Admin-Nodes müssen INSTANZEN immer gleich 2 sein.

Führen Sie das Bash-Skript aus

Sie können das verwendete `deploy-vsphere-ovftool.sh` Bash-Skript und die `deploy-vsphere-ovftool.ini`-Konfigurationsdatei, die Sie geändert haben, um die Implementierung von StorageGRID-Grid-Nodes 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 am Linux-Rechner an, den Sie verwenden, um das Bash-Skript auszuführen.
2. Wechseln Sie in das Verzeichnis, in dem Sie das Installationsarchiv extrahiert haben.

Beispiel:

```
cd StorageGRID-Webscale-version/vsphere
```

- Um alle Grid-Nodes 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
```

- Wenn ein Grid-Knoten aufgrund eines Fehlers nicht bereitgestellt werden konnte, 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 Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Bevor Sie beginnen

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

Dateiname	Beschreibung
configure-storagegrid.py	Python-Skript zur Automatisierung der Konfiguration

Dateiname	Beschreibung
Configure-storagegrid.sample.json	Beispielkonfigurationsdatei für die Verwendung mit dem Skript
Configure-storagegrid.blank.json	Leere Konfigurationsdatei für die Verwendung mit dem Skript

- Sie haben ein erstellt `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 das verwenden `configure-storagegrid.py` Python-Skript und das `configure-storagegrid.json` Konfigurationsdatei zur automatischen Konfiguration des StorageGRID Systems



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

Schritte

1. Melden Sie sich an der Linux-Maschine an, die Sie verwenden, um das Python-Skript auszuführen.
2. Wechseln Sie in das Verzeichnis, in dem 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 Recovery-Paket-Datei sichern, damit Sie das StorageGRID-System wiederherstellen können, wenn ein oder mehrere Grid-Knoten ausfallen. Zum Beispiel kopieren Sie den Text auf einen sicheren, gesicherten Netzwerkstandort und an einen sicheren Cloud-Storage-Standort.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

Wenn Sie angegeben haben, dass zufällige Passwörter generiert werden sollen, öffnen Sie die `Passwords.txt` Datei und suchen Sie nach den Kennwörtern, 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.           #####  
#####
```

Das StorageGRID System wird installiert und konfiguriert, wenn eine Bestätigungsmeldung angezeigt wird.

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

Verwandte Informationen

["Navigieren Sie zum Grid Manager"](#)

["Überblick über DIE REST API zur Installation"](#)

Überblick über DIE REST API zur Installation

StorageGRID stellt die StorageGRID Installations-API für die Durchführung von Installationsaufgaben bereit.

Die API verwendet die Swagger Open Source API-Plattform, um die API-Dokumentation bereitzustellen. Swagger ermöglicht Entwicklern und nicht-Entwicklern die Interaktion mit der API in einer Benutzeroberfläche, die zeigt, 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 mit der API Docs Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Jeder REST-API-Befehl umfasst die URL der API, eine HTTP-Aktion, alle erforderlichen oder optionalen URL-Parameter sowie eine erwartete API-Antwort.

StorageGRID Installations-API

Die StorageGRID Installations-API ist nur verfügbar, wenn Sie das StorageGRID-System zu Beginn konfigurieren und eine primäre Wiederherstellung des Admin-Knotens durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um auf die API-Dokumentation zuzugreifen, gehen Sie auf die Installations-Webseite des primären Admin-Knotens und wählen Sie in der Menüleiste **Hilfe > API-Dokumentation** aus.

Die StorageGRID Installations-API umfasst die folgenden Abschnitte:

- **Config** — Operationen bezogen auf die Produktversion und Versionen der API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Grid** — Konfigurationsvorgänge auf Grid-Ebene. Grid-Einstellungen erhalten und aktualisiert werden, einschließlich Grid-Details, Grid-Netzwerknetzen, Grid-Passwörter und NTP- und DNS-Server-IP-

Adressen.

- **Nodes** — Konfigurationsvorgänge auf Node-Ebene. Sie können eine Liste der Grid-Nodes abrufen, einen Grid-Node löschen, einen Grid-Node konfigurieren, einen Grid-Node anzeigen und die Konfiguration eines Grid-Node zurücksetzen.
- **Bereitstellung** — Provisioning Operationen. Sie können den Bereitstellungsprozess starten und den Status des Bereitstellungsprozesses anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsprozesses anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Schemas** — API-Schemata für erweiterte Bereitstellungen
- **Standorte** — Konfigurationsvorgänge auf Standortebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.

Weitere Schritte

Führen Sie nach Abschluss einer Installation die erforderlichen Integrations- und Konfigurationsaufgaben aus. Sie können die optionalen Aufgaben nach Bedarf ausführen.

Erforderliche Aufgaben

- Konfigurieren Sie VMware vSphere Hypervisor für automatischen Neustart.

Sie müssen den Hypervisor so konfigurieren, dass die virtuellen Maschinen beim Neustart des Servers neu gestartet werden. Ohne automatischen Neustart werden die virtuellen Maschinen und Grid-Knoten nach einem Neustart des Servers heruntergefahren. Weitere Informationen finden Sie in der Dokumentation zum VMware vSphere Hypervisor.

- ["Erstellen Sie ein Mandantenkonto"](#) Für jedes Client-Protokoll (Swift oder S3), das zum Speichern von Objekten auf Ihrem StorageGRID System verwendet wird.
- ["Kontrolle des Systemzugriffs"](#) Durch das Konfigurieren von Gruppen und Benutzerkonten. Optional können Sie ["Konfigurieren Sie eine föderierte Identitätsquelle"](#) (Z. B. Active Directory oder OpenLDAP), damit Sie Verwaltungsgruppen und Benutzer importieren können. Sie können es auch ["Erstellen Sie lokale Gruppen und Benutzer"](#).
- Integration und Test der ["S3-API"](#) Oder ["Swift-API"](#) Client-Anwendungen, mit denen Sie Objekte auf Ihr StorageGRID-System hochladen.
- ["Konfigurieren Sie die Regeln für Information Lifecycle Management \(ILM\) und die ILM-Richtlinie"](#) Sie möchten zum Schutz von Objektdaten verwenden.
- Wenn Ihre Installation Storage-Nodes der Appliance umfasst, führen Sie mithilfe von SANtricity OS die folgenden Aufgaben aus:
 - Stellen Sie Verbindungen zu jeder StorageGRID Appliance her.
 - Eingang der AutoSupport-Daten überprüfen.

Siehe ["Richten Sie die Hardware ein"](#).

- Überprüfen und befolgen Sie die ["Richtlinien zur StorageGRID-Systemhärtung"](#) Zur Vermeidung von Sicherheitsrisiken.

- ["Konfigurieren Sie E-Mail-Benachrichtigungen für Systemwarnungen"](#).
- Wenn Ihr StorageGRID-System Archivknoten enthält (veraltet), konfigurieren Sie die Verbindung des Archivknotens mit dem externen Archivierungssystem des Ziels.

Optionale Aufgaben

- ["Aktualisieren der IP-Adressen des Grid-Node"](#) Wenn sie sich seit der Planung der Bereitstellung geändert haben und das Wiederherstellungspaket erstellt haben.
- ["Konfigurieren Sie die Speicherverschlüsselung"](#), Bei Bedarf.
- ["Konfigurieren Sie die Storage-Komprimierung"](#) Um die Größe gespeicherter Objekte bei Bedarf zu reduzieren.
- ["Konfigurieren Sie den Zugriff auf das System für Überwachungszwecke"](#) Über eine NFS-Dateifreigabe

Fehlerbehebung bei Installationsproblemen

Falls bei der Installation des StorageGRID-Systems Probleme auftreten, können Sie auf die Installationsprotokolldateien zugreifen.

Im Folgenden finden Sie die wichtigsten Installationsprotokolldateien, die beim technischen Support eventuell zu Problemen führen müssen.

- `/var/local/log/install.log` (Auf allen Grid-Nodes gefunden)
- `/var/local/log/gdu-server.log` (Auf dem primären Admin-Node gefunden)

Verwandte Informationen

Informationen zum Zugriff auf die Protokolldateien finden Sie unter ["Referenz für Protokolldateien"](#).

Wenn Sie weitere Hilfe benötigen, wenden Sie sich an ["NetApp Support"](#).

Die Ressourcenreservierung für virtuelle Maschinen erfordert eine Anpassung

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 durch Bereitstellung dieser OVF-Dateien auf VMware erstellen und die vordefinierte Anzahl von Ressourcen nicht verfügbar ist, werden die virtuellen Maschinen nicht gestartet.

Über diese Aufgabe

Wenn Sie sicher sind, dass der VM-Host über ausreichende Ressourcen für jeden Grid-Node verfügt, passen Sie die Ressourcen, die für die einzelnen Virtual Machines zugewiesen sind, manuell an und starten Sie dann die Virtual Machines.

Schritte

1. Wählen Sie in der VMware vSphere Hypervisor-Clientstruktur die virtuelle Maschine aus, die nicht gestartet wird.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie im Fenster Eigenschaften von virtuellen Maschinen die Registerkarte **Ressourcen** aus.
4. Passen Sie die Ressourcen an, die der virtuellen Maschine zugewiesen sind:

- a. Wählen Sie **CPU** aus, und passen Sie mit dem Schieberegler Reservierung die für diese virtuelle Maschine reservierten MHz an.
 - b. Wählen Sie **Speicher**, und passen Sie mit dem Schieberegler Reservierung die für diese virtuelle Maschine reservierten MB an.
5. Klicken Sie auf **OK**.
 6. Wiederholen Sie diesen Vorgang für andere virtuelle Maschinen, die auf demselben VM-Host gehostet werden.

Upgrade der StorageGRID Software

Upgrade der StorageGRID Software: Übersicht

Verwenden Sie diese Anweisungen, um ein StorageGRID System auf eine neue Version zu aktualisieren.

Informationen zu diesen Anweisungen

Diese Anleitung beschreibt die Neuerungen in StorageGRID 11.7 und bietet eine Schritt-für-Schritt-Anleitung zum Upgrade aller Nodes in Ihrem StorageGRID-System auf die neue Version.

Bevor Sie beginnen

In diesen Themen erfahren Sie mehr über die neuen Funktionen und Verbesserungen in StorageGRID 11.7, können feststellen, ob Funktionen veraltet oder entfernt wurden, und Informationen zu Änderungen an StorageGRID APIs finden Sie unter.

- ["Was ist neu in StorageGRID 11.7"](#)
- ["Funktionen entfernt oder veraltet"](#)
- ["Änderungen an der Grid-Management-API"](#)
- ["Änderungen an der Mandantenmanagement-API"](#)

Neuerungen bei StorageGRID 11.7

Diese Version von StorageGRID stellt die folgenden Funktionen und Funktionsänderungen vor.

Neuer Funktionen

Grid-Verbund

Sie können eine Grid-Verbundverbindung zwischen zwei StorageGRID-Systemen konfigurieren, um Mandantenkontoinformationen zu klonen und Bucket-Objekte für die Disaster Recovery zwischen den Grids zu replizieren. Siehe ["Was ist Grid Federation?"](#), ["Was ist Account-Klon"](#), und ["Was ist Grid-übergreifende Replizierung"](#).

Bessere Leseverfügbarkeit

Die Konsistenzkontrolle „Read-after-New-write“ (Standard) wurde verbessert und steht nun mehr zur Verfügung. GET/HEAD-Anforderungen für nicht vorhandene Objekte werden erfolgreich ausgeführt, wenn bis zu ein Storage Node an jedem Standort offline ist. Buckets müssen nicht mehr auf die verfügbare

Konsistenzkontrolle für dieses Szenario eingestellt werden. Beispielsweise funktionieren Anwendungen, die das Vorhandensein eines Objekts vor der Erstellung prüfen, auch während des Softwareupgrades mit Read-after-New-Write ordnungsgemäß, wenn ein Storage Node offline ist.

Benennen Sie Raster, Standorte und Nodes um

Mit einem neuen Wartungsverfahren können Sie die Anzeigenamen ändern, die im Grid Manager angezeigt werden. Sie können Anzeigenamen sicher und jederzeit aktualisieren. Siehe ["Benennen Sie Raster, Standorte und Nodes um"](#).

FabricPool- und S3-Einrichtungsassistent

Der Einrichtungsassistent von FabricPool und S3 führt Sie durch jeden Schritt der Konfiguration von StorageGRID für die Verwendung mit ONTAP FabricPool oder einer anderen S3-Client-Applikation und erstellt eine Datei, mit der Sie die erforderlichen Werte in der anderen Applikation eingeben können. Siehe ["Verwenden Sie den FabricPool-Einrichtungsassistenten"](#) Und ["Verwenden Sie den S3-Einrichtungsassistenten"](#).

In Bezug auf diese Änderung wird jetzt ein Banner auf dem Dashboard angezeigt, um neue Benutzer an die Konfiguration zu erinnern ["Domänennamen des S3-Endpunkts"](#) Richten Sie Anforderungen im virtuellen Hosted-Stil von S3 ein und richten Sie sie ein ["E-Mail-Benachrichtigungen für Warnmeldungen"](#).

Firewall-Kontrollen

Auf der Seite „Firewall-Steuerung“ können Sie den externen Zugriff von Ports auf Knoten in Ihrem Grid verwalten und Hostadressen und IP-Subnetze definieren, denen der Zugriff auf geschlossene Ports gestattet ist. Die neue Seite enthält auch die Einstellungen für das nicht vertrauenswürdige Client-Netzwerk, mit denen Sie jetzt zusätzliche Ports auswählen können, die geöffnet werden sollen, wenn das nicht vertrauenswürdige Client-Netzwerk konfiguriert ist. Siehe ["Konfigurieren Sie die interne Firewall"](#).

Verbesserte Sicherheitsrichtlinien

Sie können nun festlegen, welche Protokolle und Chiffren verwendet werden, um sichere TLS-Verbindungen mit Clientanwendungen und sichere SSH-Verbindungen zu internen StorageGRID-Diensten herzustellen. Siehe ["Verwalten Sie die TLS- und SSH-Richtlinie"](#).

Änderungen am Endpunkt des Load Balancer

Wenn ["Konfigurieren der Lastausgleichsendpunkte"](#)Sie können jetzt:

- Allen Mandanten den Zugriff auf den Endpunkt erlauben (Standard), oder eine Liste zulässiger oder blockierter Mandanten angeben, um eine bessere Sicherheitsisolierung zwischen Mandanten und deren Endpunkten zu ermöglichen.
- Verwenden Sie den Bindungsmodus **Node Type**, um von Clients abhängig vom gewählten Node die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse eines beliebigen Gateway-Knotens zu verwenden.

SGF6112 All-Flash Appliance

Die neue StorageGRID SGF6112 Storage Appliance verfügt über ein kompaktes Design mit Computing-Controller und Storage Controller, die in ein 1-HE-Chassis integriert sind. Die Appliance unterstützt 12 SSD-NVMe-Laufwerke mit einer Speicherkapazität von bis zu 15.3 TB pro Laufwerk. Die SSD-Laufwerke befinden sich in einem RAID mit ausfallsicherem Objekt-Storage. Siehe ["SGF6112 Appliance: Überblick"](#).

Andere Verbesserungen am Grid Manager

ILM-Verbesserungen

Der verbesserte ILM-Assistent vereinfacht das Festlegen von Filtern, das Eingeben von Zeiträumen und Platzierungen und das Anzeigen von Aufbewahrungsdiagrammen. Profile für Erasure Coding werden automatisch erstellt, wenn Sie einen Storage-Pool und ein EC-Schema für eine Platzierung auswählen. Für neue StorageGRID 11.7-Installationen (keine Upgrades) wird automatisch ein Speicherpool für jeden Standort erstellt, und die neue Standardregel **1 Kopie pro Standort** stellt sicher, dass neue Installationen mit mehreren Standorten standardmäßig vor Standortausfällen geschützt sind. Siehe "[Objektmanagement mit ILM](#)".

Anpassbares Dashboard

Sie können jetzt benutzerdefinierte Dashboards für den Grid Manager konfigurieren. Siehe "[Das Dashboard anzeigen und verwalten](#)".

UI für die Volume-Wiederherstellung

Durch die Wiederherstellung eines Storage-Volumes können Sie Objektdaten wiederherstellen, wenn ein Storage-Volume ausfällt. Für StorageGRID 11.7 können Sie zusätzlich zur bestehenden Methode zur manuellen Eingabe von Befehlen die Volume-Wiederherstellung über den Grid-Manager starten. Die Verwendung von Grid Manager ist jetzt die bevorzugte Methode zum Wiederherstellen von Objektdaten. Siehe "[Stellen Sie Objektdaten mithilfe von Grid Manager wieder her](#)".

Upgrade und Hotfix-UI

Wenn Sie ein Upgrade auf StorageGRID 11.7 durchführen, können Sie gleichzeitig den neuesten 11.7-Hotfix installieren. Auf der StorageGRID Upgrade-Seite werden der empfohlene Upgrade-Pfad und Links direkt zu den richtigen Download-Seiten angezeigt. Siehe "[Upgrade durchführen](#)".

Einheiten für Speicherwerte

Sie können jetzt Basis-10- oder Basis-2-Einheiten für die Speicherwerte auswählen, die im Grid Manager und Tenant Manager angezeigt werden. Wählen Sie oben rechts im Grid Manager oder Tenant Manager das Dropdown-Menü Benutzer aus, und wählen Sie dann **Benutzereinstellungen** aus.

Greifen Sie über Grid Manager auf MIB zu

Sie können jetzt über den Grid Manager auf SNMP-konforme MIB-Dateien über die Seite SNMP Agent zugreifen. Siehe "[Zugriff auf MIB-Dateien](#)".

Individuelle Storage-Klassen für neue Nodes

Wenn Sie eine Erweiterung durchführen, um einen neuen Standort oder neue Storage-Nodes hinzuzufügen, können Sie jetzt jedem neuen Node eine benutzerdefinierte Speicherklasse zuweisen. Siehe "[Erweiterung durchführen](#)".

Tenant Manager wird aktualisiert

Grid-übergreifende Replizierung

Mandantenkonten, die über die Berechtigung verfügen, einen zu verwenden [Netzverbundverbindung](#) Mandanten, Benutzer und S3-Schlüssel können von einem Grid in ein anderes geklont und Bucket-Objekte zwischen zwei Grids mithilfe von Grid-Replizierung repliziert werden. Siehe "[Klonen von Mandantengruppen und Benutzern](#)" Und "[Grid-übergreifende Replizierung managen](#)".

Löschen Sie alle Objekte aus Bucket

Mandanten-Manager-Benutzer können jetzt alle Objekte in einem Bucket löschen, sodass der Bucket gelöscht werden kann. Siehe ["Löschen von Objekten in Bucket"](#).

S3 Object Lock – Standardaufbewahrung

Mandanten-Manager-Benutzer können jetzt beim Erstellen von S3 Object Lock-Buckets die Standardaufbewahrung aktivieren und konfigurieren. Siehe ["Erstellen eines S3-Buckets"](#).

S3-Updates

S3 Objektsperre Governance-Modus

Wenn Sie die S3 Object Lock-Einstellungen für ein Objekt oder die Standardaufbewahrungseinstellungen für einen Bucket angeben, können Sie jetzt den Governance-Modus verwenden. Mit diesem Aufbewahrungsmodus können Benutzer mit besonderer Berechtigung bestimmte Aufbewahrungseinstellungen umgehen. Siehe ["Verwenden Sie S3 Objektsperre, um Objekte beizubehalten"](#) Und ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

S3-Gruppenrichtlinie zur Minimierung von Ransomware

Wenn sie als Gruppenrichtlinie für ein S3-Mandantenkonto hinzugefügt wird, hilft die Beispielrichtlinie bei der Abwehr von Ransomware-Angriffen. Es verhindert, dass ältere Objektversionen dauerhaft gelöscht werden. Siehe ["Erstellen von Gruppen für einen S3-Mandanten"](#).

NewerNoncurrentVersions-Schwellenwert für S3-Buckets

Der `NewerNoncurrentVersions` Durch die Aktion in der Bucket-Lebenszykluskonfiguration wird die Anzahl der nicht-aktuellen Versionen angegeben, die in einem versionierten S3-Bucket aufbewahrt wurden. Dieser Schwellenwert überschreibt die Lebenszyklusregeln, die von ILM bereitgestellt werden. Siehe ["So werden Objekte gelöscht"](#).

S3 Select-Updates

S3 SelectObjectContent bietet jetzt Unterstützung für Parquet-Objekte. Darüber hinaus können Sie jetzt S3 Select mit Admin- und Gateway Load Balancer-Endpunkten verwenden, die Bare-Metal-Knoten sind, auf denen ein Kernel mit cgroup v2 aktiviert ist. Siehe ["S3 SelectObjectContent"](#).

Weitere Verbesserungen

ZertifikatStudienteilnehmer optional

Das Feld für den Betreff des Zertifikats ist jetzt optional. Wenn dieses Feld leer bleibt, verwendet das generierte Zertifikat den ersten Domännennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN). Siehe ["Verwalten von Sicherheitszertifikaten"](#).

ILM-Audit-Nachrichtenkategorie und neue Nachrichten

Für ILM-Vorgänge wurde eine Kategorie für Audit-Meldungen hinzugefügt, die IDEL-, LKCU- und ORLM-Meldungen enthält. Diese neue Kategorie ist auf **normal** gesetzt. Siehe ["Prüfmeldungen für den ILM-Betrieb"](#).

Zusätzlich wurden neue Audit-Meldungen hinzugefügt, die die neue 11.7-Funktionalität unterstützen:

- ["BROR: Bucket Read Only Request"](#)

- ["CGRR: Grid-übergreifende Replikationsanforderung"](#)
- ["EBDL: Leerer Bucket löschen"](#)
- ["EBKR: Anforderung für leeren Bucket"](#)
- ["S3SL: S3 Select Request"](#)

Neue Warnmeldungen

Die folgenden neuen Warnmeldungen wurden für StorageGRID 11.7 hinzugefügt:

- Fehler des Appliance-das-Laufwerks erkannt
- Wiederherstellung des Appliance-das-Laufwerks
- Fehler des Gerätelüfters erkannt
- Appliance-NIC-Fehler erkannt
- Kritische Warnung bei Appliance-SSD
- Fehler beim Senden der AutoSupport-Nachricht
- Cassandra-Fehler bei der Übergröße des Schreibvorgangs
- Fehler bei der Anforderung einer Grid-übergreifenden Replizierung
- Grid-übergreifende Replizierungsressourcen nicht verfügbar
- Leistungsbeeinträchtigung debuggen
- Ablauf des Netzverbundzertifikats
- FabricPool Bucket hat die nicht unterstützte Bucket-KonsistenzEinstellung
- Fehler bei der Firewall-Konfiguration
- Fehler bei der Verbindung mit dem Grid-Verbund
- Lüfterfehler des Speichergeräts erkannt
- Storage-Node befindet sich nicht im gewünschten Speicherzustand
- Das Storage-Volume muss beachtet werden
- Das Speicher-Volume muss wiederhergestellt werden
- Das Storage-Volume ist offline
- Trace-Konfiguration aktiviert
- Die Volume-Wiederherstellung konnte die Reparatur replizierter Daten nicht starten

Änderungen in der Dokumentation

- Eine neue Kurzübersicht zeigt, wie StorageGRID Amazon Simple Storage Service (S3) APIs unterstützt. Siehe ["Schnelle Referenz: Unterstützte S3-API-Anforderungen"](#).
- Das neue ["Quick Start Guide für StorageGRID"](#) Führt die allgemeinen Schritte zur Konfiguration und Verwendung eines StorageGRID-Systems auf und enthält Links zu den entsprechenden Anweisungen.
- Die Installationsanweisungen für die Appliance-Hardware wurden kombiniert und konsolidiert, um die Bedienung zu erleichtern. Ein schneller Einstieg wurde als allgemeine Anleitung zur Hardwareinstallation hinzugefügt. Siehe ["Schnellstart für die Hardwareinstallation"](#).
- Die für alle Gerätemodelle üblichen Wartungsanweisungen wurden kombiniert, konsolidiert und in den Wartungsbereich des Dokumentstandortes verschoben. Siehe ["Allgemeine Knotenwartung: Übersicht"](#).

- Die für jedes Gerätemodell spezifischen Wartungsanweisungen wurden ebenfalls in den Abschnitt „Wartung“ verschoben:

["Instandhaltung der SGF6112 Hardware"](#)

["Wartung der SG6000 Hardware"](#)

["Instandhaltung der SG5700 Hardware"](#)

["Instandhaltung der SG100 und SG1000 Hardware"](#)

Funktionen entfernt oder veraltet

Einige Funktionen wurden in dieser Version entfernt oder veraltet. Überprüfen Sie diese Elemente, um zu verstehen, ob Sie Clientanwendungen aktualisieren oder Ihre Konfiguration vor dem Upgrade ändern müssen.

Verbindungslastausgleich (CLB)-Service entfernt

Der Dienst Connection Load Balancer (CLB) auf Gateway-Nodes wurde in StorageGRID 11.4 veraltet und wurde nun vollständig aus der Software entfernt. Um eingehende Netzwerkverbindungen von Client-Anwendungen auf Speicher-Nodes zu verteilen, können Sie Load Balancer-Endpunkte für den Load Balancer-Dienst konfigurieren, der in allen Admin-Nodes und Gateway-Nodes enthalten ist, oder Sie können einen Load Balancer eines Drittanbieters integrieren. Siehe ["Überlegungen zum Lastausgleich"](#).

Wenn in der vorhandenen StorageGRID-Version benutzerdefinierte Zertifikate für die S3- oder Swift-API eingerichtet wurden, werden die CLB-Ports 8082, 8083, 8084 und 8085 während des Upgrades auf StorageGRID 11.7 automatisch in Load Balancer-Endpunkte konvertiert.

Die SG5600 Appliance wird nicht mehr unterstützt

Die SG5600 Appliance hat das Ende des Supports erreicht. Weitere Informationen zu Hardware-Aktualisierungen erhalten Sie von Ihrem NetApp Vertriebsmitarbeiter.

Wenn Sie Wartungsverfahren für SG5600-Hardware durchführen müssen, verwenden Sie die ["Anweisungen für StorageGRID 11.6"](#).

Die Unterstützung für Swift ist veraltet

Ab Version StorageGRID 11.7 ist die Unterstützung für Swift-Client-Applikationen veraltet. Die Benutzeroberfläche und APIs, die Swift-Client-Anwendungen unterstützen, werden in einem zukünftigen Release entfernt.

Unterstützung für Archive Node veraltet

Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Siehe:

- ["Migrieren von Objekten in einen Cloud-Storage-Pool"](#)

- ["Verwendung Von Cloud Storage Pools"](#)

Darüber hinaus sollten Sie Archivknoten aus der aktiven ILM-Richtlinie in StorageGRID 11.7 oder früher entfernen. Das Entfernen von Objektdaten, die auf Archive Nodes gespeichert sind, vereinfacht zukünftige Upgrades. Siehe ["Arbeiten mit ILM-Regeln und ILM-Richtlinien"](#).

Audit-Export über CIFS/Samba entfernt

Audit-Export über CIFS/Samba wurde in StorageGRID Webscale 11.1 veraltet und wurde jetzt entfernt. Bei Bedarf können Sie ["Verwenden Sie einen externen Syslog-Server"](#) Oder ["Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS"](#).

Option, um einen Speicherpool als temporären Speicherort anzugeben, der entfernt wurde

Wenn Sie zuvor eine ILM-Regel mit einer Objektplatzierung erstellt haben, die einen einzelnen Speicherpool umfasst, wurden Sie aufgefordert, einen zweiten Speicherpool anzugeben, der als temporärer Speicherort verwendet werden soll. Ab StorageGRID 11.7 wurde diese Option entfernt.

Die Grid Manager-Optionen wurden verschoben oder entfernt

Mehrere Grid Manager-Optionen wurden verschoben oder entfernt.

- Der ["Gespeicherte Objekte komprimieren"](#) Option wurde verschoben zu **CONFIGURATION > System > Objektkomprimierung**.
- Die interne Verbindungseinstellung **Network Transfer Encryption** wurde entfernt und durch ersetzt ["TLS- und SSH-Richtlinien"](#) Auf der neuen Seite **CONFIGURATION > Security > Security settings**.



Die AES256-SHA-Option war die Standardeinstellung in StorageGRID 11.6 und ist die einzige Einstellung, die in StorageGRID 11.7 verfügbar ist. Der AES128-SHA-Wert wird in der Grid-Management-API ignoriert. Während des StorageGRID 11.7-Upgrades ist der Verschlüsselungsalgorithmus für die Netzwerkübertragung auf AES256-SHA eingestellt.

- Die Optionen **Stored Object Encryption**, **Prevent Client modification** und **Enable HTTP for Storage Node Connections** wurden in die verschoben ["Registerkarte Netzwerk und Objekte"](#) Auf der neuen Seite **CONFIGURATION > Security > Security settings**.
- Der ["Zeitlimit für Inaktivität des Browsers"](#) Option wurde auf die neue Seite **CONFIGURATION > Security > Security settings** verschoben.
- Der ["Verbindungskosten"](#) Option wurde auf **SUPPORT > andere > Link Cost** verschoben.
- Die Liste der NMS Entities wurde in **SUPPORT > andere > NMS Entities** verschoben.
- Die Option **Stored Object Hashing** wurde entfernt. Die Einstellungen **SHA-1** und **SHA-256** werden nicht mehr für die interne Hintergrundüberprüfung verwendet, da sie zusätzliche CPU-Ressourcen über MD5 und Packet CRC32-Prüfung benötigen.
- Die Option **bevorzugter Absender** wurde entfernt. Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Nachrichten, SNMP-Traps und -Benachrichtigungen sowie ältere Alarmmeldungen. Wenn der primäre Admin-Node nicht mehr verfügbar ist, werden vorübergehend Benachrichtigungen von anderen Admin-Nodes gesendet. Siehe ["Was ist ein Admin-Node?"](#).
- Der ["Nicht vertrauenswürdige Client-Netzwerkeinstellungen"](#) Wurden in **CONFIGURATION > Firewall Control** verschoben.

Einschränkungen im Format für S3-Endpunktdomännennamen

Die Verwendung von IP-Adressen als Endpunkt-Domännennamen wird nicht unterstützt. Zukünftige Versionen verhindern die Konfiguration. Wenden Sie sich an den technischen Support, wenn Sie IP-Adressen für Domännennamen des Endpunkts verwenden müssen. Siehe ["Domännennamen des S3-Endpunkts"](#).

Der vom Benutzer initiierte Befehl „Volume Lost“ wurde entfernt

Der `proc/CMSI/Volume_Lost` wurde entfernt. Verwenden Sie die `repair-data start-replicated-volume-repair` Befehl zum Wiederherstellen replizierter Daten für ein Volume.

Änderungen an der Grid-Management-API

StorageGRID 11.7 verwendet Version 3 der Grid-Management-API. Version 3 depretiert Version 2; jedoch werden Version 1 und Version 2 weiterhin unterstützt.



Sie können Version 1 und Version 2 der Management-API mit StorageGRID 11.7 weiterhin verwenden. Allerdings wird die Unterstützung für diese Versionen der API in einem zukünftigen Release von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.7 können die veralteten v1- und v2-APIs mithilfe des deaktiviert werden `PUT /grid/config/management API:`

Weitere Informationen finden Sie unter ["Verwenden Sie die Grid-Management-API"](#).

Anzeigenamen sind jetzt in Antworten auf Anforderungen des Node-Systemzustands enthalten

Im Zusammenhang mit dem neuen ["Benennen Sie Raster, Standorte und Nodes um, Verfahren"](#), Nach dem Umbenennen eines Standorts oder Knotens werden der Name des Elements (sein Systemname) und dessen Anzeigename von der API **Node-Health** zurückgegeben.

Bucket und Zugriffsschlüssel für neue S3-Mandanten können erstellt werden

Neu `s3Bucket` Und `s3AccessKey` Optionen wurden der API **Accounts** hinzugefügt. Wenn Sie ein S3-Mandantenkonto mit der Grid-Management-API erstellen, können Sie optional einen Bucket für diesen Mandanten sowie die Zugriffsschlüssel-ID und den geheimen Schlüssel für den Root-Benutzer des Mandanten erstellen.

Kann den Speicherstatus für Storage-Node ändern

Sie können die neuen API-Endpunkte **Node-Storage-State** verwenden, um den Status des Speichers in einem Storage Node (online, offline, schreibgeschützt) zu bestimmen und zu ändern.

Änderungen an der Mandantenmanagement-API

StorageGRID 11.7 verwendet Version 3 der Mandantenmanagement-API. Version 3 depretiert Version 2; jedoch werden Version 1 und Version 2 weiterhin unterstützt.



Sie können Version 1 und Version 2 der Management-API mit StorageGRID 11.7 weiterhin verwenden. Allerdings wird die Unterstützung für diese Versionen der API in einem zukünftigen Release von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.7 können die veralteten v1- und v2-APIs mithilfe des deaktiviert werden `PUT /grid/config/management API:`

Neue Endpunkte für Grid-Verbund

Sie können die API-Endpunkte **Grid-Federation-connections** verwenden, um Grid Federation-Verbindungen für den aktuellen Mandanten aufzulisten und den letzten Grid-übergreifenden Replikationsfehler für die aktuelle Mandanten- und ausgewählte Grid Federation-Verbindung zu löschen.

Weitere Informationen finden Sie unter "[Mandantenmanagement-API verstehen](#)".

Planung und Vorbereitung für Upgrades

Schätzen Sie den Zeitaufwand für die Durchführung eines Upgrades ein

Bei der Planung eines Upgrades auf StorageGRID 11.7 müssen Sie anhand der Dauer des Upgrades berücksichtigen, wann ein Upgrade erforderlich ist. Außerdem müssen Sie sich darüber im Klaren sein, welche Vorgänge Sie in jeder Phase des Upgrades durchführen können und welche nicht.

Über diese Aufgabe

Die erforderliche Zeit zur Durchführung eines StorageGRID Upgrades hängt von verschiedenen Faktoren ab, beispielsweise von Client-Last und Hardware-Performance.

Die Tabelle fasst die wichtigsten Upgrade-Aufgaben zusammen und zeigt die ungefähre Zeit, die für jede Aufgabe erforderlich ist. Die Schritte nach der Tabelle enthalten Anweisungen zur Schätzung der Aktualisierungszeit für Ihr System.

Aufgabe aktualisieren	Beschreibung	Ungefähre Zeit erforderlich	Während dieser Aufgabe
Führen Sie Vorabprüfungen durch und aktualisieren Sie den primären Admin-Node	Die Upgrade-Vorabprüfungen werden ausgeführt, und der primäre Admin-Node wird angehalten, aktualisiert und neu gestartet.	30 Minuten bis 1 Stunde, wobei SG100- und SG1000-Appliance-Nodes die meiste Zeit erfordern. Ungelöste Vorabprüffehler erhöhen sich diesmal.	Sie können nicht auf den primären Admin-Node zugreifen. Möglicherweise werden Verbindungsfehler gemeldet, die Sie ignorieren können. Durch die Durchführung der Vorabprüfungen des Upgrades vor dem Start des Upgrades können Sie Fehler vor dem Wartungsfenster für geplante Upgrades beheben.
Starten Sie den Upgrade Service	Die Softwaredatei wird verteilt, und der Upgrade-Service wird gestartet.	3 Minuten pro Grid-Node	

Aufgabe aktualisieren	Beschreibung	Ungefähre Zeit erforderlich	Während dieser Aufgabe
Upgrade anderer Grid-Nodes	Die Software auf allen anderen Grid-Knoten wird aktualisiert, in der Reihenfolge, in der Sie die Knoten genehmigen. Jeder Knoten im System wird einzeln heruntergefahren.	15 Minuten bis 1 Stunde pro Node, wobei Appliance-Nodes die höchste Zeit erfordern Hinweis: Für Appliance-Knoten wird der StorageGRID-Appliance-Installer automatisch auf die neueste Version aktualisiert.	<ul style="list-style-type: none"> • Ändern Sie nicht die Grid-Konfiguration. • Ändern Sie nicht die Konfiguration auf Audit-Ebene. • Aktualisieren Sie nicht die ILM-Konfiguration. • Sie können keine weiteren Wartungsvorgänge wie Hotfix, Stilllegung oder Erweiterung durchführen. <p>Hinweis: Wenn Sie eine Wiederherstellung durchführen müssen, wenden Sie sich an den technischen Support.</p>
Aktivieren von Funktionen	Die neuen Funktionen für die neue Version sind aktiviert.	Weniger als 5 Minuten	<ul style="list-style-type: none"> • Ändern Sie nicht die Grid-Konfiguration. • Ändern Sie nicht die Konfiguration auf Audit-Ebene. • Aktualisieren Sie nicht die ILM-Konfiguration. • Ein weiterer Wartungsvorgang ist nicht möglich.
Datenbank aktualisieren	Der Upgrade-Prozess überprüft jeden Knoten, um zu überprüfen, ob die Cassandra-Datenbank nicht aktualisiert werden muss.	10 Sekunden pro Node oder einige Minuten für das gesamte Grid	<p>Für das Upgrade von StorageGRID 11.6 auf 11.7 ist kein Cassandra-Datenbank-Upgrade erforderlich. Der Cassandra-Service wird jedoch auf jedem Speicherknoten angehalten und neu gestartet.</p> <p>Bei künftigen StorageGRID-Funktionsversionen kann der Schritt für das Update der Cassandra-Datenbank mehrere Tage dauern.</p>
Abschließende Upgrade-Schritte	Temporäre Dateien werden entfernt und das Upgrade auf die neue Version wird abgeschlossen.	5 Minuten	Wenn die Aufgabe Letzte Aktualisierungsschritte abgeschlossen ist, können Sie alle Wartungsverfahren durchführen.

Schritte

1. Schätzen Sie die für das Upgrade aller Grid-Nodes erforderliche Zeit ein.

a. Multiplizieren Sie die Anzahl der Nodes in Ihrem StorageGRID System um 1 Stunde/Node.

In der Regel dauert das Upgrade von Appliance-Nodes länger als softwarebasierte Nodes.

b. Fügen Sie 1 Stunde zu diesem Zeitpunkt hinzu, um die Zeit zu berücksichtigen, die zum Herunterladen des erforderlich ist `.upgrade` Führen Sie die Vorabvalidierung aus, und führen Sie die letzten

Aktualisierungsschritte durch.

2. Wenn Sie Linux-Knoten haben, fügen Sie 15 Minuten für jeden Knoten hinzu, um die Zeit zu berücksichtigen, die zum Herunterladen und Installieren des RPM- oder DEB-Pakets erforderlich ist.
3. Berechnen Sie die geschätzte Gesamtdauer für das Upgrade, indem Sie die Ergebnisse der Schritte 1 und 2 hinzufügen.

Beispiel: Geschätzte Dauer für ein Upgrade auf StorageGRID 11.7

Angenommen, Ihr System verfügt über 14 Grid-Nodes, von denen 8 Linux-Nodes sind.

1. 14 mit 1 Stunde/Node multiplizieren.
2. Fügen Sie 1 Stunde hinzu, um den Download, die Vorabprüfung und die abschließenden Schritte zu berücksichtigen.

Die geschätzte Zeit für ein Upgrade aller Nodes beträgt 15 Stunden.

3. Multiplizieren Sie 8 x 15 Minuten/Node, um die Zeit für die Installation des RPM- oder DEB-Pakets auf den Linux-Knoten zu berücksichtigen.

Die voraussichtliche Zeit für diesen Schritt beträgt 2 Stunden.

4. Fügen Sie die Werte zusammen.

Für das Upgrade Ihres Systems auf StorageGRID 11.7 sollten Sie bis zu 17 Stunden benötigen.



Bei Bedarf können Sie das Wartungsfenster in kleinere Fenster aufteilen, indem Sie Untergruppen von Rasterknoten für die Aktualisierung in mehreren Sitzungen genehmigen. Sie sollten beispielsweise 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 mehr als einer Sitzung durchführen möchten, beachten Sie, dass Sie die neuen Funktionen erst verwenden können, wenn alle Knoten aktualisiert wurden.

Auswirkungen des Upgrades auf Ihr System

Sie müssen wissen, welche Auswirkungen das Upgrade auf Ihr StorageGRID System hat.

StorageGRID Upgrades sind unterbrechungsfrei

Das StorageGRID System ist in der Lage, während des Upgrades Daten von Client-Applikationen aufzunehmen und abzurufen. Wenn Sie alle Nodes desselben Typs für das Upgrade genehmigen (z. B. Storage Nodes), werden die Nodes nacheinander heruntergefahren. Es ist also keine Zeit, wenn alle Grid-Nodes oder alle Grid-Nodes eines bestimmten Typs nicht verfügbar sind.

Um die kontinuierliche Verfügbarkeit zu gewährleisten, stellen Sie sicher, dass Ihre ILM-Richtlinie Regeln enthält, die das Speichern mehrerer Kopien jedes Objekts festlegen. Es muss zudem sichergestellt werden, dass alle externen S3- oder Swift-Clients für das Senden von Anforderungen an eine der folgenden Komponenten konfiguriert sind:

- Eine virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit)
- Einen hochverfügbaren Drittanbieter-Load Balancer

- Mehrere Gateway-Nodes für jeden Client
- Mehrere Storage-Nodes für jeden Client

Die Appliance-Firmware wird aktualisiert

Während der StorageGRID 11.7-Aktualisierung:

- Alle StorageGRID Appliance Nodes werden automatisch auf die StorageGRID Appliance Installer-Firmware-Version 3.7 aktualisiert.
- SG6060 und SGF6024 Appliances werden automatisch auf die BIOS-Firmware-Version 3B07.EX und BMC-Firmware-Version 3.97.07 aktualisiert.
- SG100 und SG1000 Appliances werden automatisch auf die BIOS-Firmware-Version 3B12.EC und BMC-Firmware-Version 4.71.07 aktualisiert.

Möglicherweise werden Benachrichtigungen ausgelöst

Warnmeldungen können ausgelöst werden, wenn Services gestartet und beendet werden und wenn das StorageGRID System als Umgebung mit gemischten Versionen funktioniert (einige Grid-Nodes mit einer früheren Version, während andere auf eine neuere Version aktualisiert wurden). Nach Abschluss des Upgrades können weitere Warnmeldungen ausgelöst werden.

Beispielsweise wird möglicherweise die Warnmeldung **Unable to communicate with Node** angezeigt, wenn Dienste angehalten werden, oder Sie sehen möglicherweise die Warnmeldung **Cassandra-Kommunikationsfehler**, wenn einige Knoten auf StorageGRID 11.7 aktualisiert wurden, aber andere Knoten noch StorageGRID 11.6 ausführen. Im Allgemeinen werden diese Meldungen nach Abschluss des Upgrades gelöscht.

Die Warnung **ILM-Platzierung nicht erreichbar** kann ausgelöst werden, wenn Speicherknoten während des Upgrades auf StorageGRID 11.7 gestoppt werden. Dieser Alarm wird möglicherweise einen Tag nach Abschluss des Upgrades andauern.

Nachdem das Upgrade abgeschlossen ist, können Sie alle Upgrade-bezogenen Warnmeldungen überprüfen, indem Sie im Grid Manager-Dashboard **Kürzlich aufgelöste Warnmeldungen** oder **Aktuelle Warnmeldungen** auswählen.

Viele SNMP-Benachrichtigungen werden erzeugt

Beachten Sie, dass möglicherweise eine große Anzahl von SNMP-Benachrichtigungen generiert werden kann, wenn Grid-Knoten angehalten und während des Upgrades neu gestartet werden. Um zu viele Benachrichtigungen zu vermeiden, deaktivieren Sie das Kontrollkästchen **Enable SNMP Agent Notifications (CONFIGURATION > Monitoring > SNMP Agent)**, um SNMP-Benachrichtigungen vor dem Start des Upgrades zu deaktivieren. Aktivieren Sie dann die Benachrichtigungen wieder, nachdem das Upgrade abgeschlossen ist.

Konfigurationsänderungen sind eingeschränkt



Diese Liste gilt insbesondere für Upgrades von StorageGRID 11.6 auf StorageGRID 11.7. Wenn Sie ein Upgrade auf eine andere StorageGRID-Version durchführen, lesen Sie die Liste der eingeschränkten Änderungen in den Upgrade-Anweisungen für diese Version.

Bis die Aufgabe **Neues Feature** aktivieren abgeschlossen ist:

- Nehmen Sie keine Änderungen an der Grid-Konfiguration vor.

- Aktivieren oder deaktivieren Sie keine neuen Funktionen. Versuchen Sie beispielsweise erst dann, eine Grid-Federation-Verbindung zu erstellen, wenn beide StorageGRID Systeme auf StorageGRID 11.7 aktualisiert wurden.
- Aktualisieren Sie nicht die ILM-Konfiguration. Andernfalls kann es zu inkonsistenten und unerwarteten ILM-Verhaltensweisen kommen.
- Wenden Sie keinen Hotfix an, und stellen Sie keinen Grid-Knoten wieder her.



Wenden Sie sich an den technischen Support, wenn Sie einen Node während des Upgrades wiederherstellen müssen.

- Während Sie ein Upgrade auf StorageGRID 11.7 durchführen, sollten Sie keine HA-Gruppen, VLAN-Schnittstellen oder Load Balancer-Endpunkte managen.
- Löschen Sie keine HA-Gruppen, bevor Sie das Upgrade auf StorageGRID 11.7 abgeschlossen haben. Auf virtuelle IP-Adressen in anderen HA-Gruppen kann möglicherweise nicht mehr zugegriffen werden.

Bis die Aufgabe * Final Upgrade Steps* abgeschlossen ist:

- Führen Sie keine Erweiterungsschritte durch.
- Führen Sie keine Stilllegungsverfahren durch.

Sie können keine Bucket-Details anzeigen oder Buckets im Tenant Manager managen

Während des Upgrades auf StorageGRID 11.7 (d. h. während das System als Umgebung mit gemischten Versionen läuft) können Sie keine Bucket-Details anzeigen oder Buckets mithilfe des Tenant Manager managen. Auf der Seite Buckets in Tenant Manager wird einer der folgenden Fehler angezeigt:

- Sie können diese API nicht verwenden, während Sie ein Upgrade auf 11.7 durchführen.
- Sie können keine Details zur Bucket-Versionierung im Tenant Manager anzeigen, während Sie ein Upgrade auf 11.7 durchführen.

Dieser Fehler wird behoben, nachdem die Aktualisierung auf 11.7 abgeschlossen ist.

Behelfslösung

Solange das Upgrade 11.7 läuft, können Sie mit den folgenden Tools Bucket-Details anzeigen oder Buckets managen, anstatt den Tenant Manager zu verwenden:

- Verwenden Sie zum Durchführen von S3-Standardoperationen für einen Bucket entweder die "[S3-REST-API](#)" Oder im "[Mandantenmanagement-API](#)".
- Um benutzerdefinierte StorageGRID-Vorgänge auf einem Bucket durchzuführen (beispielsweise zum Anzeigen und Ändern der Bucket-Konsistenzstufe, zum Aktivieren oder Deaktivieren von Updates für die letzte Zugriffszeit oder zum Konfigurieren der Suchintegration), verwenden Sie die Mandantenmanagement-API.

TLS-Chiffren oder SSH-Konfigurationen können sich ändern

Wenn TLS-Chiffren oder SSH-Konfigurationen manuell geändert wurden oder für alle Nodes inkonsistent sind, werden alle Nodes nach dem Upgrade entweder als Legacy-Kompatibilität oder als Modern Compatibility überschrieben. Wenn Sie verwendet haben `fips-ciphers.sh` In StorageGRID 11.6 wird die Common Criteria-Richtlinie auf alle Nodes angewendet. Andernfalls wird die alte Kompatibilitätsrichtlinie angewendet. Für validierte Konfigurationen mit Common Criteria müssen Sie die Common Criteria-Richtlinie oder die FIPS-Strict-Richtlinie verwenden. Wenn Sie nicht verwendet haben `fips-ciphers.sh`, Sie sollten die neue

moderne Kompatibilitätseinstellung nach Abschluss des Upgrades verwenden. Um Chiffren zu konfigurieren, gehen Sie zu **CONFIGURATION > Security > Security settings** und wählen **TLS und SSH Policies** aus.

CLB-Ports können in Load Balancer-Endpunkte umgewandelt werden

Der Service für den älteren Verbindungslastausgleich (CLB) wurde in StorageGRID 11.7 entfernt. Wenn die CLB-Konfiguration während der Upgrade-Vorabprüfungen erkannt wird, wird die Warnmeldung **Legacy CLB Load Balancer Activity Detected** ausgelöst. Wenn in der vorhandenen StorageGRID-Version benutzerdefinierte Zertifikate für die S3- oder Swift-API eingerichtet wurden, werden die CLB-Ports 8082, 8083, 8084 und 8085 während des Upgrades auf StorageGRID 11.7 in Load Balancer-Endpunkte konvertiert.

Siehe auch "[Überlegungen zum Lastausgleich](#)".

Auswirkungen eines Upgrades auf Gruppen und Benutzerkonten

Sie müssen die Auswirkungen des StorageGRID Upgrades kennen, damit Sie Gruppen und Benutzerkonten nach Abschluss des Upgrades entsprechend aktualisieren können.

Änderungen an Gruppenberechtigungen und -Optionen

Nach dem Upgrade auf StorageGRID 11.7 weisen Sie den Benutzergruppen der Mandanten optional die folgende neue Berechtigung zu.

Berechtigung	Beschreibung
Tenant Manager > Objekte mithilfe der S3-Konsole managen	<p>In Kombination mit der Berechtigung zum Verwalten aller Buckets ermöglicht diese Berechtigung Benutzern den Zugriff auf "Experimentelle S3-Konsole" Auf der Seite „Planungsperioden“.</p> <p>Benutzer, die über diese Berechtigung verfügen, aber nicht über die Berechtigung zum Verwalten aller Buckets verfügen, können dennoch direkt zur Experimental S3 Console navigieren.</p>

Siehe "[Mandantenmanagement-Berechtigungen](#)".

Überprüfen Sie die installierte StorageGRID-Version

Bevor Sie mit dem Upgrade beginnen, müssen Sie überprüfen, ob die vorherige Version von StorageGRID derzeit mit dem neuesten verfügbaren Hotfix installiert ist.

Über diese Aufgabe

Vor dem Upgrade auf StorageGRID 11.7 muss StorageGRID 11.6 auf Ihrem Grid installiert sein. Wenn Sie derzeit eine frühere Version von StorageGRID verwenden, müssen Sie alle vorherigen Aktualisierungsdateien zusammen mit den neuesten Hotfixes installieren (dringend empfohlen), bis die aktuelle Version Ihres Grids StorageGRID 11.6 ist.x.y.

Ein möglicher Upgrade-Pfad wird im angezeigt [Beispiel](#).



NetApp empfiehlt dringend, vor dem Upgrade auf die nächste Version den aktuellen Hotfix für jede StorageGRID-Version anzuwenden und den aktuellen Hotfix für jede installierte neue Version anzuwenden. In einigen Fällen müssen Sie einen Hotfix anwenden, um das Risiko eines Datenverlusts zu vermeiden. Siehe ["NetApp Downloads: StorageGRID"](#) Und die Release Notes für jeden Hotfix, um mehr zu erfahren.

Beachten Sie, dass Sie in einem Schritt ein Skript zur Aktualisierung von 11.3.0.13+ auf 11.4.0.y und von 11.4.0.7+ bis 11.5.0.y ausführen können. Siehe ["NetApp Knowledge Base: So führen Sie umfassende Upgrades und Hotfix-Skripte für StorageGRID aus"](#).

Schritte

1. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).
2. Wählen Sie oben im Grid Manager die Option **Hilfe > Info**.
3. Stellen Sie sicher, dass **Version** 11.6.x.y ist.

In der StorageGRID 11.6.x.y Versionsnummer:

- Das **Major Release** hat einen x Wert von 0 (11.6.0).
 - Ein **Hotfix** hat, wenn man angewendet wurde, einen y Wert (z.B. 11.6.0.1).
4. Wenn **Version** nicht 11.6.x.y ist, gehen Sie zu ["NetApp Downloads: StorageGRID"](#) So laden Sie die Dateien für jede vorherige Version herunter, einschließlich des neuesten Hotfix für jede Version.
 5. Lesen Sie die Upgrade-Anweisungen für jede heruntergeladene Version. Führen Sie dann das Software-Upgrade-Verfahren für dieses Release durch, und wenden Sie den neuesten Hotfix für dieses Release an (dringend empfohlen).

Siehe ["StorageGRID Hotfix Verfahren"](#).

Beispiel: Upgrade auf StorageGRID 11.6 von Version 11.3.0.8

Das folgende Beispiel zeigt die Schritte zum Upgrade von StorageGRID Version 11.3.0.8 auf Version 11.6 als Vorbereitung auf ein StorageGRID 11.7-Upgrade.



Optional können Sie ein Skript ausführen, um die Schritte 2 und 3 (Update von 11.3.0.13+ auf 11.4.0.y) zu kombinieren und die Schritte 4 und 5 zu kombinieren (Aktualisierung von 11.4.0.7+ auf 11.5.0.y). Siehe ["NetApp Knowledge Base: So führen Sie umfassende Upgrades und Hotfix-Skripte für StorageGRID aus"](#).

Laden Sie die Software in der folgenden Reihenfolge herunter und installieren Sie sie, um Ihr System auf die Aktualisierung vorzubereiten:

1. Wenden Sie den aktuellen StorageGRID 11.3.0.y Hotfix an.
2. Upgrade auf StorageGRID 11.4.0 Hauptversion.
3. Wenden Sie den aktuellen StorageGRID 11.4.0.y Hotfix an.
4. Upgrade auf StorageGRID 11.5.0 Hauptversion.
5. Wenden Sie den aktuellen StorageGRID 11.5.0.y Hotfix an.
6. Upgrade auf die Hauptversion von StorageGRID 11.6.0.
7. Wenden Sie den aktuellen StorageGRID 11.6.0.y Hotfix an.

Beschaffen der erforderlichen Materialien für ein Software-Upgrade

Bevor Sie mit dem Software-Upgrade beginnen, müssen Sie alle erforderlichen Unterlagen beschaffen, damit das Upgrade erfolgreich abgeschlossen werden kann.

Element	Hinweise
Service-Laptop	Der Service-Laptop muss Folgendes haben: <ul style="list-style-type: none">• Netzwerkport• SSH-Client (z. B. PuTTY)
"Unterstützter Webbrowser"	Der Browser-Support ändert sich in der Regel für jede StorageGRID Version. Stellen Sie sicher, dass Ihr Browser mit der neuen StorageGRID-Version kompatibel ist.
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase wird im nicht aufgeführt <code>passwords.txt</code> Datei:
Linux RPM- oder DEB-Archiv	Wenn Knoten auf Linux-Hosts bereitgestellt werden, müssen Sie dies tun "Laden Sie das RPM- oder DEB-Paket herunter, und installieren Sie es auf allen Hosts" Bevor Sie mit dem Upgrade beginnen. Wichtig: Stellen Sie sicher, dass Ihr Betriebssystem auf Linux Kernel 4.15 oder höher aktualisiert wird.
StorageGRID-Dokumentation	<ul style="list-style-type: none">• "Versionshinweise" Für StorageGRID 11.7 (Anmeldung erforderlich). Lesen Sie diese vor Beginn des Upgrades sorgfältig durch.• "Lösungsfaden für StorageGRID Software-Upgrades" Für die Hauptversion, auf die Sie aktualisieren (Anmeldung erforderlich)• Andere "StorageGRID 11.7-Dokumentation" Bei Bedarf.

Überprüfen Sie den Zustand des Systems

Vor dem Upgrade eines StorageGRID Systems müssen Sie überprüfen, ob das System bereit ist, um das Upgrade durchzuführen. Sie müssen sicherstellen, dass das System ordnungsgemäß ausgeführt wird und alle Grid-Nodes funktionsfähig sind.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).
2. Aktive Warnmeldungen prüfen und beheben.
3. Bestätigen Sie, dass keine in Konflikt stehenden Grid-Aufgaben aktiv oder ausstehend sind.
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **site > primary Admin Node > CMN > Grid Tasks > Konfiguration** aus.

ILME-Tasks (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 lassen Sie ihre Sperre los.



Wenden Sie sich an den technischen Support, wenn eine Aufgabe nicht beendet ist oder ihre Sperre nicht freigegeben wird.

4. Siehe "[Interne Kommunikation mit Grid-Nodes](#)" Und "[Externe Kommunikation](#)" Um sicherzustellen, dass alle erforderlichen Ports für StorageGRID 11.7 geöffnet werden, bevor Sie ein Upgrade durchführen.

Im Folgenden "[Interne Ports](#)" Muss geöffnet sein, bevor Sie ein Upgrade auf StorageGRID 11.7 durchführen:

Port	Beschreibung
1055	Wird für das Protokoll zum Anklopfen von Firewall-Kontrollen verwendet.
8011	Vergewissern Sie sich vor der Aktualisierung, dass dieser Port zwischen allen Grid-Nodes im Grid-Netzwerk offen ist.
10342	
18086	TCP-Port wird für neuen LDR-Dienst verwendet. Vergewissern Sie sich vor dem Upgrade, dass dieser Port von allen Grid-Nodes zu allen Storage-Nodes offen ist.

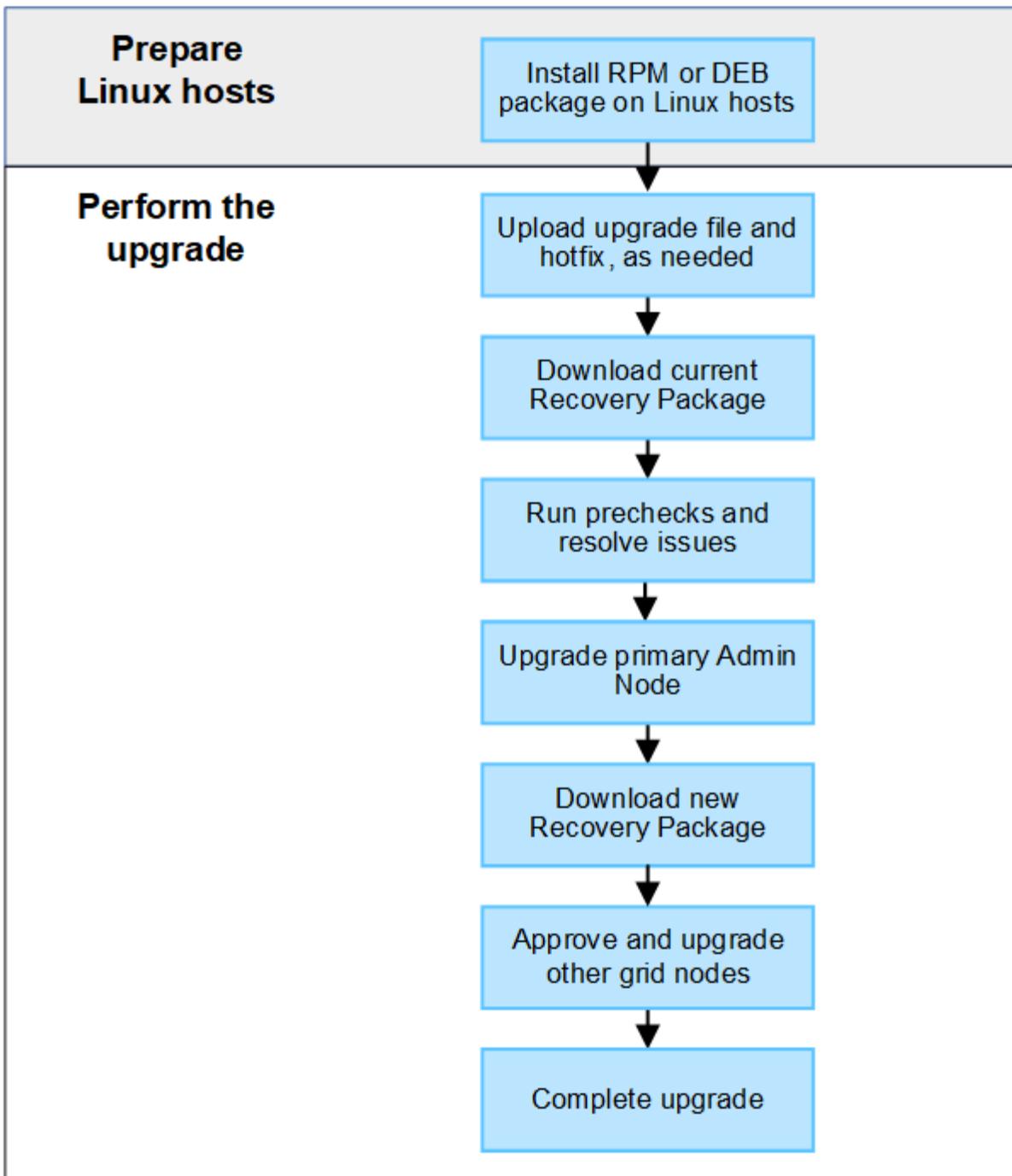


Wenn Sie benutzerdefinierte Firewall-Ports geöffnet haben, werden Sie während der Vorabprüfung des Upgrades benachrichtigt. Bevor Sie das Upgrade durchführen, müssen Sie sich an den technischen Support wenden.

Software-Upgrade

Workflow-Upgrade

Lesen Sie vor dem Upgrade den allgemeinen Workflow durch. Die Seite StorageGRID-Upgrade führt Sie durch die einzelnen Upgrade-Schritte.



1. Wenn StorageGRID Nodes auf Linux-Hosts bereitgestellt werden, "[Installieren Sie das RPM- oder DEB-Paket auf jedem Host](#)" Bevor Sie mit dem Upgrade beginnen.
2. Greifen Sie vom primären Administratorknoten aus auf die Seite StorageGRID-Aktualisierung zu, und laden Sie ggf. die Aktualisierungsdatei und die Hotfix-Datei hoch.
3. Laden Sie das aktuelle Wiederherstellungspaket herunter.
4. Führen Sie Vorabprüfungen für Upgrades durch, um Probleme zu erkennen und zu beheben, bevor Sie das eigentliche Upgrade starten.
5. Starten Sie das Upgrade, in dem Vorabprüfungen durchgeführt werden und der primäre Admin-Node automatisch aktualisiert wird. Sie können nicht auf den Grid-Manager zugreifen, während das Upgrade des primären Admin-Knotens durchgeführt wird. Auch Audit-Protokolle sind nicht verfügbar. Dieses Upgrade kann bis zu 30 Minuten in Anspruch nehmen.

- Nachdem der primäre Admin-Knoten aktualisiert wurde, laden Sie ein neues Wiederherstellungspaket herunter.
- Genehmigen Sie die Grid-Knoten. Sie können einzelne Grid-Nodes, Gruppen von Grid-Nodes oder alle Grid-Nodes genehmigen.



Genehmigen Sie das Upgrade für einen Grid-Node nur, wenn Sie sicher sind, dass der Node bereit ist, angehalten und neu gestartet zu werden.

- Setzen Sie den Betrieb fort. Wenn alle Grid-Nodes aktualisiert wurden, sind neue Funktionen aktiviert und der Betrieb kann fortgesetzt werden. Sie müssen warten, bis ein Deaktivierungs- oder Erweiterungsvorgang durchgeführt wird, bis die Hintergrundaufgabe **Datenbank aktualisieren** und die Aufgabe **Letzte Aktualisierungsschritte** abgeschlossen sind.

Verwandte Informationen

["Schätzen Sie den Zeitaufwand für die Durchführung eines Upgrades ein"](#)

Linux: Laden Sie das RPM- oder DEB-Paket herunter und installieren Sie es auf allen Hosts

Wenn StorageGRID-Knoten auf Linux-Hosts bereitgestellt werden, müssen Sie ein zusätzliches RPM- oder DEB-Paket auf jedem dieser Hosts herunterladen und installieren, bevor Sie mit dem Upgrade beginnen.

Laden Sie Upgrade-, Linux- und Hotfix-Dateien herunter

Wenn Sie ein StorageGRID-Upgrade über den Grid-Manager durchführen, werden Sie aufgefordert, das Upgrade-Archiv und den erforderlichen Hotfix als ersten Schritt 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

- Gehen Sie zu ["NetApp Downloads: StorageGRID"](#).
- Wählen Sie die Schaltfläche zum Herunterladen der neuesten Version, oder wählen Sie eine andere Version aus dem Dropdown-Menü aus und wählen Sie **Go**.

Die StorageGRID-Softwareversionen haben dieses Format: 11.x.y. StorageGRID-Hotfixes haben dieses Format: 11.x.y.z.

- Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
- Wenn ein Warnhinweis/MustRead angezeigt wird, notieren Sie sich die Hotfix-Nummer, und aktivieren Sie das Kontrollkästchen.
- Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren** aus.

Die Download-Seite für die ausgewählte Version wird angezeigt. Die Seite enthält drei Spalten.

- Laden Sie in der zweiten Spalte (**Upgrade StorageGRID**) zwei Dateien herunter:
 - Das Upgrade-Archiv für die neueste Version (dies ist die Datei im Abschnitt **VMware, SG1000 oder SG100 Primary Admin Node**). Diese Datei wird zwar erst benötigt, wenn Sie das Upgrade durchführen, aber das Herunterladen spart jetzt Zeit.
 - Ein RPM- oder DEB-Archiv in beiden `.tgz` Oder `.zip` Formatieren. Wählen Sie die aus `.zip` Datei,

wenn Windows auf dem Service-Laptop ausgeführt wird.

- Red hat Enterprise Linux oder CentOS+
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 Hotfix einem Warnhinweis/MustRead zustimmen müssen, laden Sie den Hotfix herunter:
 - a. Gehen Sie zurück zu ["NetApp Downloads: StorageGRID"](#).
 - b. Wählen Sie die Hotfix-Nummer aus der Dropdown-Liste aus.
 - c. Stimmen Sie den Vorsichtshinweis und EULA erneut zu.
 - d. Laden Sie den Hotfix und dessen README herunter und speichern Sie ihn.

Sie werden aufgefordert, die Hotfix-Datei auf der StorageGRID-Upgrade-Seite hochzuladen, wenn Sie mit dem Upgrade beginnen.

Installieren Sie Archive 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.

Siehe die Schritte zum Installieren von StorageGRID-Hostdiensten in der Installationsanleitung:

- ["Red hat Enterprise Linux oder CentOS: Installieren Sie StorageGRID-Hostdienste"](#)
- ["Ubuntu oder Debian: Installieren Sie StorageGRID-Hostdienste"](#)

Die neuen Pakete werden als zusätzliche Pakete installiert. Entfernen Sie nicht die vorhandenen Pakete.

Führen Sie das Upgrade durch

Sie können ein Upgrade auf StorageGRID 11.7 durchführen und gleichzeitig den neuesten Hotfix für diese Version anwenden. Die StorageGRID Upgrade-Seite enthält den empfohlenen Upgrade-Pfad und Links direkt zu den richtigen Download-Seiten.

Bevor Sie beginnen

Sie haben alle Überlegungen geprüft und alle Planungs- und Vorbereitungsschritte durchgeführt.

Rufen Sie die Seite StorageGRID Upgrade auf

Rufen Sie als ersten Schritt im Grid-Manager die Seite „StorageGRID-Upgrade“ auf.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).
2. Wählen Sie **WARTUNG > System > Software-Update**.

3. Wählen Sie in der StorageGRID-Upgrade-Kachel **Upgrade** aus.

Wählen Sie Dateien aus

Der Updatepfad auf der Seite StorageGRID-Aktualisierung zeigt an, welche Hauptversionen (z. B. 11.7.0) und Hotfixes (z. B. 11.7.0.1) installiert werden müssen, um die neueste StorageGRID-Version zu erhalten. Sie sollten die empfohlenen Versionen und Hotfixes in der angegebenen Reihenfolge installieren.



Falls kein Updatepfad angezeigt wird, kann Ihr Browser möglicherweise nicht auf die NetApp Support-Website zugreifen. Alternativ ist das Kontrollkästchen **nach Software-Updates suchen** auf der AutoSupport-Seite (**SUPPORT > Tools > AutoSupport**) möglicherweise deaktiviert.

Schritte

1. Überprüfen Sie für den Schritt **Dateien auswählen** den Updatepfad.
2. Klicken Sie im Bereich „Dateien herunterladen“ auf jeden Link **Download**, um die erforderlichen Dateien von der NetApp Support-Website herunterzuladen.

Wenn kein Aktualisierungspfad angezeigt wird, wechseln Sie zum "[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 möglicherweise bereits die StorageGRID-Upgrade- und Hotfix-Dateien im Updatepfad aufgelistet.

3. Wählen Sie **Browse**, um die Aktualisierungsdatei der Version auf StorageGRID hochzuladen:
`NetApp_StorageGRID_11.7.0_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 im Rahmen des Versions-Upgrades angewendet.
5. Wählen Sie **Weiter**.

Führen Sie Tests im Vorfeld durch

Durch das Ausführen von Vorabprüfungen können Sie Upgrade-Probleme erkennen und beheben, bevor Sie mit dem Grid-Upgrade beginnen.

Schritte

1. Geben Sie für den Schritt **run prechecks** zunächst die Provisionierungs-Passphrase für Ihr Grid ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.

Sie sollten die aktuelle Kopie der Wiederherstellungspaket-Datei herunterladen, bevor Sie den primären Admin-Knoten aktualisieren. Die Recovery Package-Datei ermöglicht es Ihnen, das System wiederherzustellen, wenn ein Fehler auftritt.

3. Wenn die Datei heruntergeladen wird, bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich der `Passwords.txt` Datei:
4. Kopieren Sie die heruntergeladene Datei (`.zip`) An zwei sichere und getrennte Stellen.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

5. Wählen Sie **Prechecks ausführen**, und warten Sie, bis die Vorabprüfungen abgeschlossen sind.
6. Überprüfen Sie die Details für jede gemeldete Vorabprüfung, und beheben Sie alle gemeldeten Fehler. Siehe "[Lösungleitfaden für StorageGRID Software-Upgrades](#)" Für StorageGRID 11.7.

Sie müssen alle Vorabprüfung *errors* beheben, bevor Sie Ihr System aktualisieren können. Sie müssen jedoch vor dem Upgrade keine Vorabprüfung *Warnings* durchführen.



Wenn Sie benutzerdefinierte Firewall-Ports geöffnet haben, werden Sie während der Vorabprüfung-Validierung benachrichtigt. Bevor Sie das Upgrade durchführen, müssen Sie sich an den technischen Support wenden.

7. Wenn Sie Konfigurationsänderungen vorgenommen haben, um die gemeldeten Probleme zu beheben, wählen Sie **Vorprüfungen 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-Node

Wenn Sie das Upgrade starten, werden die Upgrade-Vorabprüfungen erneut ausgeführt, und der primäre Admin-Node wird automatisch aktualisiert. Dieser Teil des Upgrades kann bis zu 30 Minuten dauern.



Während des Upgrades des primären Admin-Knotens können Sie nicht auf andere 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 die Aktualisierung zu starten.
3. Warten Sie, bis die Vorabprüfungen durchgeführt werden und der primäre Admin-Node aktualisiert wird.



Wenn Vorabprüffehler gemeldet werden, beheben Sie diese und wählen Sie erneut **Upgrade starten** aus.

Wenn das Raster 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 wird, können Sie die anderen Grid-Knoten genehmigen.

4. Wählen Sie bei Bedarf **Weiter**, um auf den Schritt **andere Knoten aktualisieren** zuzugreifen.

Aktualisieren Sie andere Nodes

Sie müssen alle Grid-Nodes aktualisieren, aber Sie können mehrere Upgrade-Sitzungen durchführen und die Upgrade-Sequenz anpassen. Sie sollten beispielsweise 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 mehr als einer Sitzung durchführen möchten, beachten Sie, dass Sie die neuen Funktionen erst verwenden können, wenn alle Knoten aktualisiert wurden.

Wenn die Reihenfolge des Upgrades von Nodes wichtig ist, genehmigen Sie Knoten oder Gruppen von Knoten jeweils eins und warten Sie, bis das Upgrade auf jedem Knoten abgeschlossen ist, bevor Sie den nächsten Knoten oder die nächste Gruppe von Nodes genehmigen.



Wenn das Upgrade auf einem Grid-Node startet, werden die Services auf diesem Node angehalten. Später wird der Grid-Node neu gebootet. Um Serviceunterbrechungen für Client-Applikationen zu vermeiden, die mit dem Node kommunizieren, genehmigen Sie das Upgrade für einen Node nur, wenn Sie sicher sind, dass der Node bereit ist, angehalten und neu gestartet zu werden. Planen Sie bei Bedarf ein Wartungsfenster oder benachrichtigen Sie die Kunden.

Schritte

1. Überprüfen Sie für den Schritt **andere Knoten aktualisieren** die Zusammenfassung, die die Startzeit für das Upgrade als Ganzes und den Status für jede größere Upgrade-Aufgabe enthält.
 - **Upgrade-Dienst starten** ist die erste Upgrade-Aufgabe. Während dieser Aufgabe wird die Softwaredatei an die Grid-Nodes verteilt, und der Upgrade-Service wird auf jedem Node gestartet.
 - Wenn der Task **Upgrade-Dienst starten** abgeschlossen ist, wird der Task **andere Grid-Knoten aktualisieren** gestartet und Sie werden aufgefordert, eine neue Kopie des Wiederherstellungspakets herunterzuladen.
2. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Provisionierungs-Passphrase ein, und laden Sie eine neue Kopie des Wiederherstellungspakets herunter.



Sie sollten eine neue Kopie der Wiederherstellungspaket-Datei herunterladen, nachdem der primäre Admin-Knoten aktualisiert wurde. Die Recovery Package-Datei ermöglicht es Ihnen, das System wiederherzustellen, wenn ein Fehler auftritt.

3. Überprüfen Sie die Statustabellen für jeden Node-Typ. Es gibt Tabellen für nicht primäre Admin-Nodes, Gateway-Nodes, Storage-Nodes und Archive Nodes.

Ein Gitterknoten kann sich in einer dieser Stufen befinden, wenn die Tabellen zuerst angezeigt werden:

- Auspacken des Upgrades
 - Download
 - Warten auf Genehmigung
4. Wenn Sie für die Aktualisierung Grid-Nodes auswählen möchten (oder wenn Sie die Genehmigung für ausgewählte Nodes aufheben müssen), gehen Sie wie folgt vor:

Aufgabe	Anweisung
Suchen Sie nach bestimmten Knoten, die genehmigt werden sollen, z. B. alle Knoten an einem bestimmten Standort	Geben Sie den Suchstring in das Feld Suche ein
Wählen Sie alle Nodes aus, die aktualisiert werden sollen	Wählen Sie Approve all Nodes

Aufgabe	Anweisung
Wählen Sie alle Nodes desselben Typs für das Upgrade aus (z. B. alle Storage-Nodes).	Wählen Sie die Schaltfläche Approve all für den Knotentyp Wenn Sie mehrere Knoten desselben Typs genehmigen, werden die Knoten nacheinander aktualisiert.
Wählen Sie einen einzelnen Node für das Upgrade aus	Klicken Sie auf die Schaltfläche approve für den Knoten
Verschieben Sie das Upgrade auf alle ausgewählten Knoten	Wählen Sie Alle Knoten ausweisen
Verschieben Sie das Upgrade auf alle ausgewählten Knoten desselben Typs	Wählen Sie für den Knotentyp die Schaltfläche Unapprove all
Verschieben Sie das Upgrade auf einen einzelnen Node	Wählen Sie die Schaltfläche Unapprove für den Knoten

5. Warten Sie, bis die genehmigten Nodes diese Upgrade-Phasen durchlaufen:

- Genehmigt und wartet auf ein Upgrade
- Dienste werden angehalten



Sie können einen Knoten nicht entfernen, wenn seine Stufe **stopping Services** erreicht. Die Schaltfläche **Unapprove** ist deaktiviert.

- Container wird angehalten
- Bereinigen von Docker-Images
- Aktualisieren der Basis-OS-Pakete



Wenn ein Appliance-Node diese Phase erreicht, wird die StorageGRID Appliance Installer-Software auf der Appliance aktualisiert. Durch diesen automatisierten Prozess wird sichergestellt, dass die Installationsversion der StorageGRID Appliance mit der StorageGRID-Softwareversion synchronisiert bleibt.

- Neustart



Einige Appliance-Modelle werden möglicherweise mehrmals neu gestartet, um die Firmware und das BIOS zu aktualisieren.

- Schritte nach dem Neustart durchführen
- Dienste werden gestartet
- Fertig

6. Wiederholen Sie den [Genehmigungsschritt](#) So oft wie nötig, bis alle Grid-Nodes aktualisiert wurden

Upgrade abgeschlossen

Wenn alle Grid-Knoten die Upgrade-Phasen abgeschlossen haben, wird die Aufgabe **andere Grid-Knoten aktualisieren** als abgeschlossen angezeigt. Die verbleibenden Upgrade-Aufgaben werden automatisch im Hintergrund ausgeführt.

Schritte

1. Sobald die Aufgabe **enable Features** abgeschlossen ist (was schnell passiert), können Sie mit der Verwendung des beginnen "[Neuer Funktionen](#)" In der aktualisierten StorageGRID-Version.
2. Während der Task **Datenbank aktualisieren** prüft der Upgrade-Prozess jeden Knoten, um sicherzustellen, dass die Cassandra-Datenbank nicht aktualisiert werden muss.



Für das Upgrade von StorageGRID 11.6 auf 11.7 ist kein Cassandra-Datenbank-Upgrade erforderlich. Der Cassandra-Service wird jedoch auf jedem Speicherknoten angehalten und neu gestartet. Bei künftigen StorageGRID-Funktionsversionen kann der Schritt für das Update der Cassandra-Datenbank mehrere Tage dauern.

3. Wenn die Aufgabe **Datenbank aktualisieren** abgeschlossen ist, warten Sie ein paar Minuten, bis die Schritte für das letzte Upgrade* abgeschlossen sind.
4. Nach Abschluss der **letzten Upgrade-Schritte** ist das Upgrade abgeschlossen. Der erste Schritt, **Dateien auswählen**, wird mit einem grünen Erfolgsbanner angezeigt.
5. Überprüfen Sie, ob die Grid-Vorgänge wieder den normalen Status aufweisen:
 - a. Überprüfen Sie, ob die Dienste normal funktionieren und keine unerwarteten Warnmeldungen vorliegen.
 - b. Vergewissern Sie sich, dass die Client-Verbindungen zum StorageGRID-System wie erwartet funktionieren.

Behebung von Upgrade-Problemen

Wenn beim Durchführen eines Upgrades etwas schief geht, können Sie das Problem möglicherweise selbst lösen. Wenn Sie ein Problem nicht lösen können, sammeln Sie so viele Informationen wie möglich, und wenden Sie sich dann an den technischen Support.

Upgrade wurde nicht abgeschlossen

In den folgenden Abschnitten wird die Wiederherstellung in Situationen beschrieben, in denen das Upgrade teilweise fehlgeschlagen ist.

Fehler bei der Vorabprüfung des Upgrades

Zur Erkennung und Behebung von Problemen können Sie die Vorabprüfungen manuell durchführen, bevor Sie das tatsächliche Upgrade starten. Die meisten Vorprüffehler enthalten Informationen zur Behebung des Problems.

Provisionierungsfehler

Wenden Sie sich an den technischen Support, wenn der automatische Bereitstellungsprozess fehlschlägt.

Der Grid-Node stürzt ab oder kann nicht gestartet werden

Wenn ein Grid-Node während des Upgrade-Prozesses abstürzt oder nicht erfolgreich gestartet werden kann,

nachdem das Upgrade abgeschlossen wurde, wenden Sie sich an den technischen Support, um eventuelle Probleme zu untersuchen und zu beheben.

Aufnahme oder Datenabfrage wird unterbrochen

Wenn die Aufnahme oder der Abruf von Daten unerwartet unterbrochen wird, wenn Sie kein Upgrade eines Grid-Node durchführen, wenden Sie sich an den technischen Support von.

Fehler beim Datenbank-Upgrade

Wenn das Datenbank-Upgrade mit einem Fehler fehlschlägt, versuchen Sie es erneut. Wenden Sie sich an den technischen Support, wenn dieser erneut fehlschlägt.

Verwandte Informationen

["Überprüfen Sie den Zustand des Systems, bevor Sie die Software aktualisieren"](#)

Probleme bei der Benutzeroberfläche

Möglicherweise treten während oder nach dem Upgrade Probleme mit dem Grid Manager oder dem Tenant Manager auf.

Der 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 „503: Service nicht verfügbar“- und „Problem beim Herstellen der Verbindung zum Server“-Meldungen angezeigt. Sie können diese Meldungen ohne Bedenken ignorieren – sie werden nicht mehr angezeigt, sobald der Knoten aktualisiert wird.

Wenn diese Meldungen länger als eine Stunde nach dem Start des Upgrades angezeigt werden, ist möglicherweise ein Upgrade des primären Admin-Node aufgetreten. Wenn Sie das Problem nicht alleine lösen können, wenden Sie sich an den technischen Support.

Web-Oberfläche reagiert nicht wie erwartet

Der Grid-Manager oder der Mandantenmanager reagieren nach einem Upgrade der StorageGRID-Software möglicherweise nicht wie erwartet.

Wenn Probleme mit der Weboberfläche auftreten:

- Stellen Sie sicher, dass Sie ein verwenden ["Unterstützter Webbrowser"](#).



Der Browser-Support ändert sich in der Regel für jede StorageGRID Version.

- Löschen Sie den Cache Ihres Webbrowsers.

Beim Löschen des Caches werden veraltete Ressourcen entfernt, die von der vorherigen Version der StorageGRID-Software verwendet werden, und die Benutzeroberfläche kann wieder ordnungsgemäß ausgeführt werden. Anweisungen hierzu finden Sie in der Dokumentation Ihres Webbrowsers.

Fehlermeldungen „Docker Image Availability Check“

Beim Versuch, den Upgrade-Prozess zu starten, wird möglicherweise eine Fehlermeldung mit der Meldung „die folgenden Probleme wurden durch die Suite zur Überprüfung der Verfügbarkeit

von Docker Images identifiziert.“ Alle Probleme müssen behoben werden, bevor Sie das Upgrade abschließen können.

Wenden Sie sich an den technischen Support, wenn Sie sich nicht sicher sind, welche Änderungen zur Behebung der erkannten Probleme erforderlich sind.

Nachricht	Ursache	Nutzen
Upgrade-Version kann nicht ermittelt werden. Upgrade-Version Info-Datei {file_path} Das erwartete Format wurde nicht erreicht.	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-Version Info-Datei {file_path} Wurde nicht gefunden. Upgrade-Version kann 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 derzeit installierte Version auf {node_name} kann nicht ermittelt werden.	Eine kritische Datei auf dem Node ist beschädigt.	Wenden Sie sich an den technischen Support.
Verbindungsfehler beim Versuch, Versionen auf aufzulisten {node_name}	Der Node ist offline oder die Verbindung wurde unterbrochen.	Überprüfen Sie, ob alle Knoten online und über den primären Admin-Node erreichbar sind, und versuchen Sie es erneut.
Der Host für den Node {node_name} Verfügt nicht über StorageGRID {upgrade_version} Bild geladen. Images 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 gilt nur für Knoten, die als Container unter Linux ausgeführt werden.	Vergewissern Sie sich, dass die RPM- oder DEB-Pakete auf allen Linux-Hosts, auf denen Knoten ausgeführt werden, installiert wurden. 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. Siehe "Linux: Installieren Sie RPM oder DEB-Paket auf allen Hosts".
Fehler beim Prüfen des Knotens {node_name}	Ein unerwarteter Fehler ist aufgetreten.	Warten Sie einige Minuten, und versuchen Sie es erneut.
Nicht beharrter Fehler beim Ausführen von Vorabprüfungen. {error_string}	Ein unerwarteter Fehler ist aufgetreten.	Warten Sie einige Minuten, und versuchen Sie es erneut.

Konfiguration und Management

StorageGRID verwalten

Administration StorageGRID: Überblick

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

Informationen zu diesen Anweisungen

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

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

Bevor Sie beginnen

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

Erste Schritte mit Grid Manager

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

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

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Melden Sie sich beim Grid Manager an

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

Überblick

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

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

Stellen Sie eine Verbindung mit der HA-Gruppe her

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

Verwenden Sie SSO

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

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

Bevor Sie beginnen

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

```
https://FQDN_or_Admin_Node_IP/
```

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

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

```
https://FQDN_or_Admin_Node_IP:port/
```



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

Schritte

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

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

SSO wird nicht verwendet

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



NetApp StorageGRID[®]

Grid Manager

Username

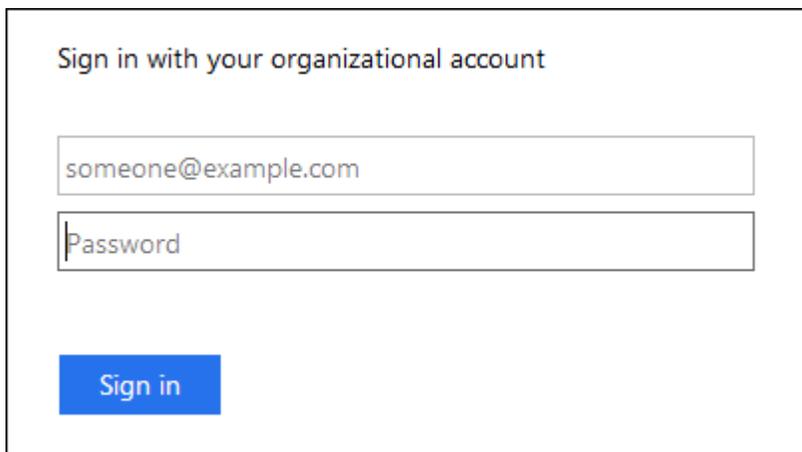
Password

Sign in

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

SSO wird verwendet

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



Sign in with your organizational account

Password

Sign in

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

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

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

StorageGRID dashboard

You have 4 notifications: 1 ● 3 ▲

Overview Performance Storage ILM Nodes

Health status

!
License
1
License

Data space usage breakdown

2.11 MB (0%) of 3.09 TB used overall

Site name	Data storage usage	Used space	Total space
Data Center 2	0%	682.53 KB	926.62 GB
Data Center 3	0%	646.12 KB	926.62 GB
Data Center 1	0%	779.21 KB	1.24 TB

Total objects in the grid

0

Metadata allowed space usage breakdown

3.62 MB (0%) of 25.76 GB used in Data Center 1

Data Center 1 has the highest metadata space usage and it determines the metadata space available in the grid.

Site name	Metadata space usage	Used space	Allowed space
Data Center 3	0%	2.71 MB	19.32 GB

Melden Sie sich bei einem anderen Admin-Node an

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

SSO wird nicht verwendet

Schritte

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

SSO wird verwendet

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

Schritte

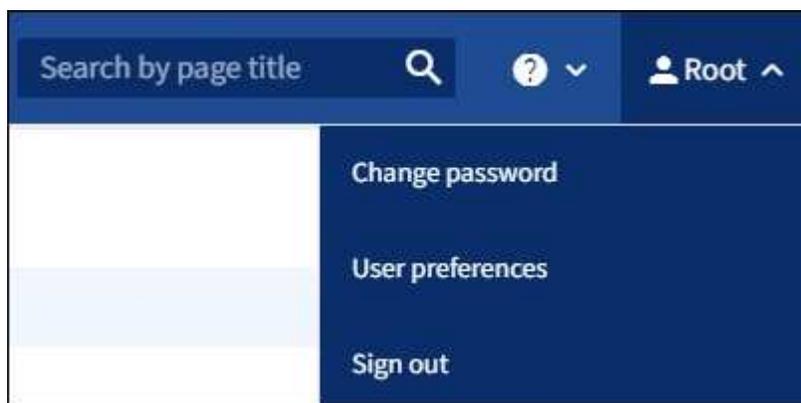
1. Geben Sie den vollständig qualifizierten Domännennamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers ein.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldedaten erneut ein.

Melden Sie sich vom Grid Manager ab

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

Schritte

1. Wählen Sie oben rechts Ihren Benutzernamen aus.



2. Wählen Sie **Abmelden**.

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

Passwort ändern

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

Bevor Sie beginnen

Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

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

Schritte

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

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

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

Zeigen Sie StorageGRID Lizenzinformationen an

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

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

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



Schritte

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

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

- Inhalt der Lizenztext-Datei



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

Aktualisieren Sie die StorageGRID-Lizenzinformationen

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

Bevor Sie beginnen

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

Schritte

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

Die neue Lizenzdatei wird validiert und angezeigt.

4. Wählen Sie **Speichern**.

Verwenden Sie die API

Verwenden Sie die Grid-Management-API

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

Allgemeine Ressourcen

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

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

API-Anforderungen ausgeben

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

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

Bevor Sie beginnen

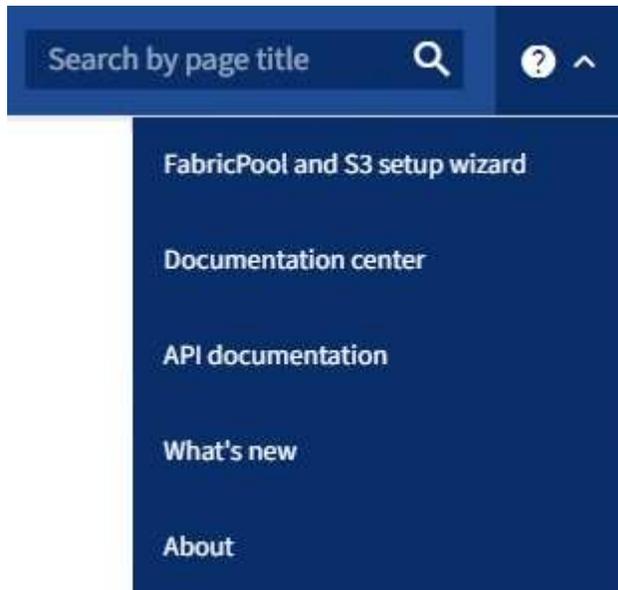
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.



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

Schritte

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



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

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

3. Wählen Sie den gewünschten Vorgang aus.

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

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

GET
/grid/groups Lists Grid Administrator Groups
🔒

Try it out

Name	Description
type string <small>(query)</small>	filter by group type Available values : local, federated <input type="text" value="--"/>
limit integer <small>(query)</small>	maximum number of results Default value : 25 <input type="text" value="25"/>
marker string <small>(query)</small>	marker-style pagination offset (value is Group's URN) <input type="text" value="marker - marker-style pagination offset (value"/>
includeMarker boolean <small>(query)</small>	if set, the marker element is also returned <input type="text" value="--"/>
order string <small>(query)</small>	pagination order (desc requires marker) Available values : asc, desc <input type="text" value="--"/>

Responses
Response content type

Code	Description
200	successfully retrieved Example Value Model <pre style="background-color: #2e3436; color: #eeeeec; padding: 10px; font-family: monospace; font-size: 0.9em;"> { "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre>

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

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



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

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

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



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

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

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

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



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

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

Die Grid Management API-Versionierung

Die Grid Management API verwendet Versionierung zur Unterstützung unterbrechungsfreier Upgrades.

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

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

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

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

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



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

Veraltete Anfragen werden wie folgt als veraltet markiert:

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

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

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

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

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

Geben Sie eine API-Version für eine Anforderung an

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

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

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

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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



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

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

Schritte

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

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

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

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

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

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

3. Wenn Sie Curl-Anforderungen verwenden möchten, gehen Sie wie folgt vor.
 - a. Deklarieren der Variablen, die für die Anmeldung erforderlich sind.

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



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

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

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

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

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

```
{  
  "apiVersion": "3.0",  
  "data":  
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...  
  sS1%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...sS1%2BfQ33cvfwA%3D'
```

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

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

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

Die Antwort umfasst die Client-Anforderungs-ID:

```
<form method="post" id="loginForm" autocomplete="off" novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13) Login.submitLoginRequest();" action="/adfs/ls/?SAMLRequest=fZHRT0MwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

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

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

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

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

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



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

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRT0MwFIZfhb...UJikvo77sXPw%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.

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

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

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

Die Antwort umfasst das Authentifizierungs-Token.

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

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

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

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

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

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

Über diese Aufgabe

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

Schritte

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

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

Es wird eine Abmeldung-URL zurückgegeben:

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

2. Speichern Sie die Abmeldung-URL.

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

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

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

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

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

4. Löschen Sie das StorageGRID-Überträger-Token.

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

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

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

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

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

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

Um ein 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 Verzeichnis der StorageGRID Installationsdateien (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder Debian, und `./vsphere` Für VMware).

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

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

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

Schritte

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

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

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

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

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

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****

StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



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

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

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

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

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

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

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

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



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

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

Schritte

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- g. Den Wert „Aktion“ exportieren:

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

- h. Senden von Cookies zusammen mit den Zugangsdaten:

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

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

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

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

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

der Grid Management-API anmelden möchten.

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

Die Antwort umfasst das Authentifizierungs-Token.

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

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

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

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

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

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

Über diese Aufgabe

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

Schritte

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

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

Es wird eine Abmeldung-URL zurückgegeben:

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

2. Speichern Sie die Abmeldung-URL.

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

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

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

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

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

4. Löschen Sie das StorageGRID-Überträger-Token.

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

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

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

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

Deaktivieren Sie Funktionen mit der API

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

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

Deaktivieren Funktionen erneut aktivieren

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



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

Schritte

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

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

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



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

```
{ "grid": { "alarmAcknowledgment": true } }
```

Kontrolle des Zugriffs auf StorageGRID

Control StorageGRID Access: Übersicht

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

Den Zugriff auf den Grid Manager steuern

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

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



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

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

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

Aktivieren Sie Single Sign On

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

Provisionierungs-Passphrase ändern

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

Ändern der Passwörter für die Node-Konsole

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

Ändern Sie die Provisionierungs-Passphrase

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

Bevor Sie beginnen

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

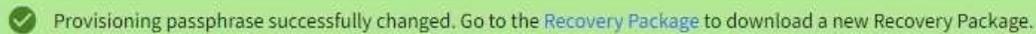
Über diese Aufgabe

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

Schritte

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

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

 Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

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



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

Ändern der Passwörter für die Node-Konsole

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

Bevor Sie beginnen

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

Über diese Aufgabe

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



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

Greifen Sie auf den Assistenten zu

Schritte

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

Geben Sie die Provisionierungs-Passphrase ein

Schritte

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

Laden Sie das aktuelle Wiederherstellungspaket herunter

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

Schritte

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



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

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

Sie können diesen Vorgang nach dem Start nicht abbrechen.

Ändern der Passwörter für die Node-Konsole

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

Schritte

1. Warten Sie, bis das neue Wiederherstellungspaket erstellt wurde, was einige Minuten dauern kann.
2. Wählen Sie **Neues Wiederherstellungspaket herunterladen**.
3. Wenn der Download abgeschlossen ist:
 - a. Öffnen Sie das .zip Datei:
 - b. Bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich `passwords.txt` Datei, die die neuen Passwörter für die Node-Konsole enthält.
 - c. Kopieren Sie die neue Wiederherstellungspaket-Datei (.zip) An zwei sichere und getrennte Stellen.



Überschreiben Sie das alte Wiederherstellungspaket nicht.

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

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

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

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

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

Wenn die Kennwortaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

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



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

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

Verwenden Sie den Identitätsverbund

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

Konfigurieren Sie die Identitätsföderation für Grid Manager

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

Bevor Sie beginnen

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



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

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

Über diese Aufgabe

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

können die folgenden Gruppen importieren:

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

Geben Sie die Konfiguration ein

Schritte

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

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
-------------------------	-------	----------	-------

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

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

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



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

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

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

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

- `sAMAccountName` Oder `uid`
- `objectGUID`, `entryUUID`, Oder `nsuniqueid`
- `cn`
- `memberOf` Oder `isMemberOf`
- **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl`, und `userPrincipalName`
- **Azure:** `accountEnabled` Und `userPrincipalName`

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



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

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



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

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

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

Geben Sie eines der folgenden Muster ein:

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

`example\[USERNAME]`

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

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

6. Wählen Sie im Abschnitt Transport Layer Security (TLS) eine Sicherheitseinstellung aus.

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



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

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, mit dem die Verbindung gesichert werden soll.

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

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

Testen Sie die Verbindung und speichern Sie die Konfiguration

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

Schritte

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

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

Test Connection ✕

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel
Test Connection

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

Synchronisierung mit der Identitätsquelle erzwingen

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

Schritte

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

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



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

Deaktivieren Sie den Identitätsverbund

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

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

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

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

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

Schritte

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

Richtlinien für die Konfiguration eines OpenLDAP-Servers

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



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

Überlagerungen in Memberof und Refint

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

Indizierung

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

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

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

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

Managen von Admin-Gruppen

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

Bevor Sie beginnen

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

Erstellen einer Admin-Gruppe

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

Greifen Sie auf den Assistenten zu

Schritte

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

Wählen Sie einen Gruppentyp aus

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

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

Lokale Gruppe

Schritte

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

Föderierte Gruppe

Schritte

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

Gruppenberechtigungen verwalten

Schritte

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



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

2. Wählen Sie eine oder mehrere Antworten aus "[Berechtigungen für Administratorgruppen](#)".

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

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

Benutzer hinzufügen (nur lokale Gruppen)

Schritte

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

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

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

Anzeigen und Bearbeiten von Admin-Gruppen

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

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

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Gruppendetails an	<ol style="list-style-type: none">a. Aktivieren Sie das Kontrollkästchen für die Gruppe.b. Wählen Sie Aktionen > Gruppendetails anzeigen.	Wählen Sie den Gruppennamen in der Tabelle aus.

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

Duplizieren einer Gruppe

Schritte

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

Gruppe löschen

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

Schritte

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

Berechtigungen für Admin-Gruppen

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

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

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

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

Interaktion zwischen Berechtigungen und Zugriffsmodus

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

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

Root-Zugriff

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

Alarmer quittieren (alt)

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

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

Root-Passwort des Mandanten ändern

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



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

Konfiguration der Seite der Grid-Topologie

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

ILM

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

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



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

Wartung

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

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

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

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

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

Verwalten von Meldungen

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

Abfrage von Kennzahlen

Diese Berechtigung bietet Zugriff auf:

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

Suche nach Objektmetadaten

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

Andere Grid-Konfiguration

Diese Berechtigung ermöglicht den Zugriff auf zusätzliche Grid-Konfigurationsoptionen.



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

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

Storage Appliance-Administrator

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

Mandantenkonten

Mit dieser Berechtigung können Sie:

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

Benutzer managen

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

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Erstellen Sie einen lokalen Benutzer

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

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

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



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

Greifen Sie auf den Assistenten zu

Schritte

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

Geben Sie die Anmeldedaten des Benutzers ein

Schritte

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

Zu Gruppen zuweisen

Schritte

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

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

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

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

Lokale Benutzer anzeigen und bearbeiten

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

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

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

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



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

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Benutzerdetails an	<ol style="list-style-type: none">a. Aktivieren Sie das Kontrollkästchen für den Benutzer.b. Wählen Sie Aktionen > Benutzerdetails anzeigen.	Wählen Sie den Benutzernamen in der Tabelle aus.
Vollständigen Namen bearbeiten (nur lokale Benutzer)	<ol style="list-style-type: none">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.	<ol style="list-style-type: none">a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen.b. Wählen Sie das Bearbeitungssymbol .c. Geben Sie den neuen Namen ein.d. Wählen Sie Änderungen speichern.

Aufgabe	Menü „Aktionen“	Detailseite
StorageGRID-Zugriff verweigern oder zulassen	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen. c. Wählen Sie die Registerkarte Zugriff aus. d. Wählen Sie Ja aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie Nein aus, damit der Benutzer sich anmelden kann. e. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Zugriff aus. c. Wählen Sie Ja aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie Nein aus, damit der Benutzer sich anmelden kann. d. Wählen Sie Änderungen speichern.
Passwort ändern (nur lokale Benutzer)	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen. c. Wählen Sie die Registerkarte Kennwort aus. d. Geben Sie ein neues Passwort ein. e. Wählen Sie Passwort ändern. 	<ul style="list-style-type: none"> a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Kennwort aus. c. Geben Sie ein neues Passwort ein. d. Wählen Sie Passwort ändern.
Gruppen ändern (nur lokale Benutzer)	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie Aktionen > Benutzerdetails anzeigen. c. Wählen Sie die Registerkarte Gruppen aus. d. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. e. Wählen Sie Gruppen bearbeiten, um verschiedene Gruppen auszuwählen. f. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Gruppen aus. c. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. d. Wählen Sie Gruppen bearbeiten, um verschiedene Gruppen auszuwählen. e. Wählen Sie Änderungen speichern.

Duplizieren eines Benutzers

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

Schritte

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

Löschen Sie einen Benutzer

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



Sie können den Root-Benutzer nicht löschen.

Schritte

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

Single Sign On (SSO) verwenden

Konfigurieren Sie Single Sign-On

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

Funktionsweise von Single Sign-On

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

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

Melden Sie sich an, wenn SSO aktiviert ist

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

Schritte

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

Die Seite StorageGRID-Anmeldung wird angezeigt.

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

NetApp StorageGRID®

Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

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



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

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

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

Sign in with your organizational account

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

Falls Ihre SSO-Anmeldedaten korrekt sind:

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



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

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

Sie müssen Ihre SSO-Anmeldedaten nicht erneut eingeben.

Abmelden, wenn SSO aktiviert ist

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

Schritte

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

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

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



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

Voraussetzungen und Überlegungen für Single Sign-On

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

Anforderungen an Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

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

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

Konfigurierter LDAP-Servicetyp	Optionen für SSO-Identitätsanbieter
Active Directory	<ul style="list-style-type: none"> • Active Directory • Azure • PingFederate
Azure	Azure

AD-FS-Anforderungen

Sie können eine der folgenden Versionen von AD FS verwenden:

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



Windows Server 2016 sollte den verwenden "[KB3201845-Update](#)", Oder höher.

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

Zusätzlichen Anforderungen

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

Überlegungen zu Azure

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

Serverzertifikate-Anforderungen

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

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



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

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

Port-Anforderungen

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

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

Bestätigen Sie, dass verbundene Benutzer sich anmelden können

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

Bevor Sie beginnen

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

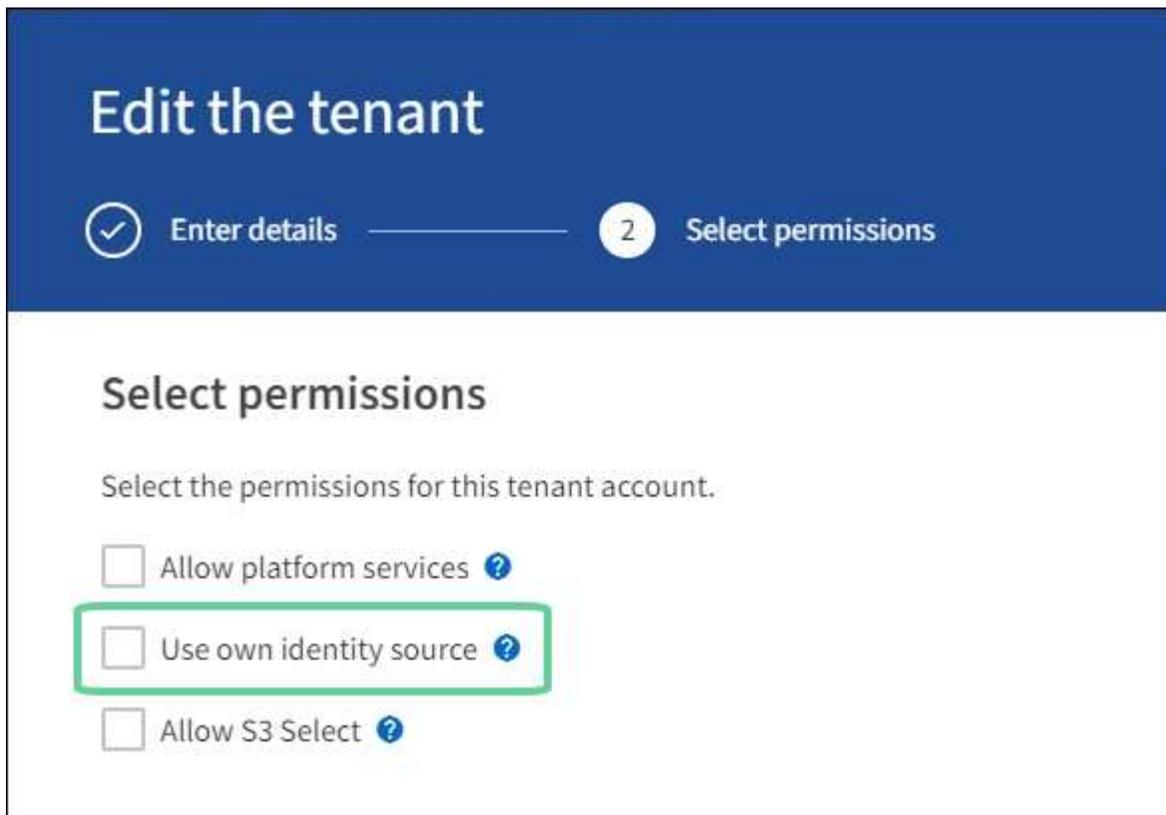
Schritte

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



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

- a. Melden Sie sich für jedes Mandantenkonto bei Tenant Manager an.
 - b. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
 - c. Bestätigen Sie, dass das Kontrollkästchen **Enable Identity Federation** nicht aktiviert ist.
 - d. Wenn dies der Fall ist, bestätigen Sie, dass keine föderierten Gruppen mehr für dieses Mandantenkonto benötigt werden, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.
2. Bestätigen Sie, dass ein verbundener Benutzer auf den Grid Manager zugreifen kann:
 - a. Wählen Sie im Grid Manager die Option **KONFIGURATION** > **Zugriffskontrolle** > **Admin-Gruppen** aus.
 - b. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus der Active Directory-Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
 - c. Abmelden.
 - d. Bestätigen Sie, dass Sie sich wieder bei Grid Manager als Benutzer in der föderierten Gruppe anmelden können.
 3. Wenn es bereits bestehende Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root-Zugriffsberechtigung anmelden kann:
 - a. Wählen Sie im Grid Manager die Option **MITERS** aus.
 - b. Wählen Sie das Mandantenkonto aus und wählen Sie **Aktionen** > **Bearbeiten**.
 - c. Wählen Sie auf der Registerkarte Details eingeben die Option **Weiter**.
 - d. Wenn das Kontrollkästchen **eigene Identitätsquelle verwenden** aktiviert ist, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern** aus.



Die Seite Mandant wird angezeigt.

- Wählen Sie das Mandantenkonto aus, wählen Sie **Anmelden** und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.
- Wählen Sie im Mandantenmanager die Option **ZUGRIFFSVERWALTUNG > Gruppen** aus.
- Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus dem Grid Manager die Root-Zugriffsberechtigung für diesen Mandanten zugewiesen wurde.
- Abmelden.
- Bestätigen Sie, dass Sie sich wieder bei dem Mandanten als Benutzer in der föderierten Gruppe anmelden können.

Verwandte Informationen

- ["Voraussetzungen und Überlegungen für Single Sign-On"](#)
- ["Managen von Admin-Gruppen"](#)
- ["Verwenden Sie ein Mandantenkonto"](#)

Verwenden Sie den Sandbox-Modus

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

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).

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

Konfigurierter LDAP-Servicetyp	Optionen für SSO-Identitätsanbieter
Active Directory	<ul style="list-style-type: none"> • Active Directory • Azure • PingFederate
Azure	Azure

Über diese Aufgabe

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

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

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

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

Zugriff auf den Sandbox-Modus

Schritte

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

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

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status  Disabled Sandbox Mode Enabled

Save



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

2. Wählen Sie **Sandbox-Modus**.

Der Abschnitt „Identitätsanbieter“ wird angezeigt.

Geben Sie die Daten des Identitätsanbieters ein

Schritte

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

Active Directory

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



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

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

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

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



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

4. Wählen Sie **Speichern**.

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



Azure

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

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

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

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

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

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



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

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

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



PingFederate

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

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

- **Verwenden Sie keine TLS:** Verwenden Sie kein TLS-Zertifikat, um die Verbindung zu sichern.
2. Geben Sie im Abschnitt Dienstanbieter (SP) die **SP-Verbindungs-ID** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede SP-Verbindung in PingFederate verwenden.
 - Wenn Ihr Grid beispielsweise nur über einen Admin-Node verfügt und Sie in Zukunft nicht mehr Admin-Nodes hinzufügen möchten, geben Sie ein `SG Oder StorageGRID`.
 - Wenn Ihr Grid mehr als einen Admin-Node enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` in der Kennung. Beispiel: `SG-[HOSTNAME]`. Dadurch wird basierend auf dem Hostnamen des Node eine Tabelle mit der SP-Verbindungs-ID für jeden Admin-Node im System generiert.



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

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

Verwenden Sie das folgende Format:

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

4. Wählen Sie **Speichern**.

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



Konfigurieren Sie Vertrauensstellungen von Drittanbietern, Unternehmensanwendungen oder SP-Verbindungen

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

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

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

Active Directory

Schritte

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

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

Weitere Anweisungen finden Sie unter ["Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS"](#).

Azure

Schritte

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

PingFederate

Schritte

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

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

Testen Sie SSO-Verbindungen

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

Active Directory

Schritte

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

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

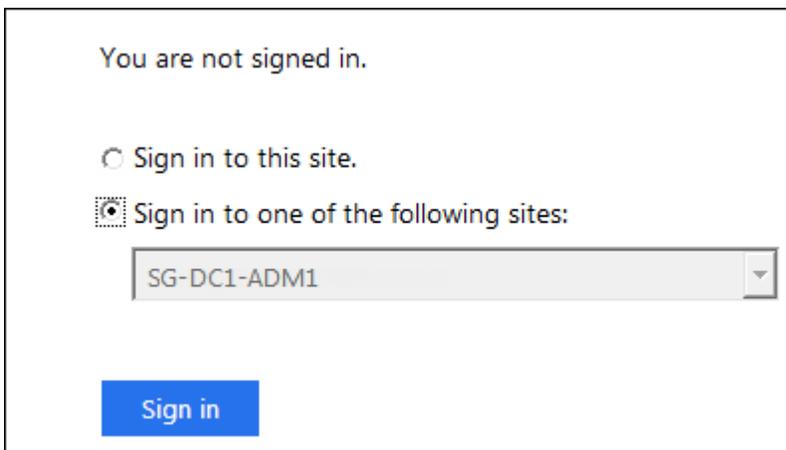
Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

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



You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

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

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

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

überprüfen.

Azure

Schritte

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

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

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

PingFederate

Schritte

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

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

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

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

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

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

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

Aktivieren Sie Single Sign On

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



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

Schritte

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

Single Sign-On ist jetzt aktiviert.



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

Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS

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

Bevor Sie beginnen

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



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

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

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

Über diese Aufgabe

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

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

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

Schritte

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

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

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

Das AD FS Management Tool wird angezeigt.

4. Wählen Sie **AD FS > vertraut auf Partei**.

Die Liste der Vertrauensstellen wird angezeigt.

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

- c. Wählen Sie **Regel hinzufügen**.
- d. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
- e. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID an Name ID**.

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

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

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

Erstellen Sie durch den Import von Federationmetadaten ein Vertrauen von Kunden

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

Schritte

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

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

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

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

vertrauenden Partei und schließen Sie den Assistenten.



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

7. Fügen Sie eine Antragsregel hinzu:

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

Beispiel: **ObjectGUID an Name ID**.

- e. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
- f. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
- g. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
- h. Wählen Sie **Fertig**, und wählen Sie **OK**.

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

- a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
- b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifizier** und **Signatur** ausgefüllt sind.

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

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

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

Erstellen Sie manuell ein Vertrauen der Vertrauensbasis

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

Schritte

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

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

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

- b. Überspringen Sie den Schritt, um ein optionales Token-Verschlüsselungszertifikat zu konfigurieren.
- c. Aktivieren Sie auf der Seite URL konfigurieren das Kontrollkästchen **Unterstützung für das SAML 2.0 WebSSO-Protokoll** aktivieren.
- d. Geben Sie die Endpunkt-URL des SAML-Service für den Admin-Node ein:

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

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

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

`Admin_Node_Identifier`

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

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

Das Dialogfeld „Forderungsrichtlinie bearbeiten“ wird angezeigt.



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

6. Um den Assistenten für die Antragsregel zu starten, wählen Sie **Regel hinzufügen**:
 - a. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
 - b. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID an Name ID**.
 - c. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
 - d. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
 - e. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
 - f. Wählen Sie **Fertig**, und wählen Sie **OK**.
7. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
8. Konfigurieren Sie auf der Registerkarte **Endpunkte** den Endpunkt für einzelne Abmeldung (SLO):
 - a. Wählen Sie **SAML hinzufügen**.

- b. Wählen Sie **Endpunkttyp > SAML Logout**.
- c. Wählen Sie **Bindung > Umleiten**.
- d. Geben Sie im Feld **Trusted URL** die URL ein, die für Single Logout (SLO) von diesem Admin-Node verwendet wird:

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

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

- a. Wählen Sie **OK**.
9. Geben Sie auf der Registerkarte **Signatur** das Signaturzertifikat für dieses Vertrauen der bevertrauenden Partei an:
- a. Fügen Sie das benutzerdefinierte Zertifikat hinzu:
 - Wenn Sie über das benutzerdefinierte Managementzertifikat verfügen, das Sie in StorageGRID hochgeladen haben, wählen Sie dieses Zertifikat aus.
 - Wenn Sie nicht über das benutzerdefinierte Zertifikat verfügen, melden Sie sich beim Admin-Knoten an, wechseln Sie zum `/var/local/mgmt-api` Verzeichnis des Admin-Knotens, und fügen Sie das `custom-server.crt` Zertifikatdatei.

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

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

Die Eigenschaften der zu vertrauenden Partei werden gespeichert und geschlossen.

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

Erstellen von Enterprise-Applikationen in Azure AD

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

Bevor Sie beginnen

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



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

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

Zugriff auf Azure AD

Schritte

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

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

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

Schritte

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

Laden Sie für jeden Admin-Node SAML-Metadaten herunter

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

Schritte

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

Hochladen von SAML-Metadaten in jede Enterprise-Applikation

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

Schritte

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



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

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

Erstellen von SP-Verbindungen (Service Provider) in PingFederate

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

Bevor Sie beginnen

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

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

- Sie haben die Administratorberechtigung für PingFederate Server.

Über diese Aufgabe

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

Alle Voraussetzungen in PingFederate

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

Datenspeicher erstellen

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

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

Passwortvalididator[[Password-Validator] erstellen

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

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

IdP-Adapterinstanz erstellen

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

Schritte

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

7. Wählen Sie **Speichern**.

Signaturzertifikat erstellen oder importieren

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

Schritte

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

Erstellen Sie eine SP-Verbindung in PingFederate

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



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

Wählen Sie den SP-Verbindungstyp

Schritte

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

Importieren der SP-Metadaten

Schritte

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

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

4. Wählen Sie **Weiter**.

Konfigurieren Sie SSO für den IdP-Browser

Schritte

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

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

Adapterinstanz zuordnen

Schritte

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

Konfigurieren von Protokolleinstellungen

Schritte

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

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

Anmeldedaten konfigurieren

Schritte

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

Erstellen Sie zusätzliche SP-Verbindungen

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



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

Schritte

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

- b. Wählen Sie **Browser-SSO konfigurieren > Assertion-Erstellung konfigurieren > Attributvertrag** aus.
- c. Löschen Sie den Eintrag für **Urne:oid**.
- d. Wählen Sie **Speichern**.

Deaktivieren Sie Single Sign-On

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

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

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

Die Seite Single Sign-On wird angezeigt.

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

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

4. Wählen Sie **OK**.

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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



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

Schritte

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

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

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

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

3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

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

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

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

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

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

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

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

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

Bestätigen Sie, dass Sie SSO aktivieren möchten.

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

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

Grid-Verbund verwenden

Was ist Grid Federation?

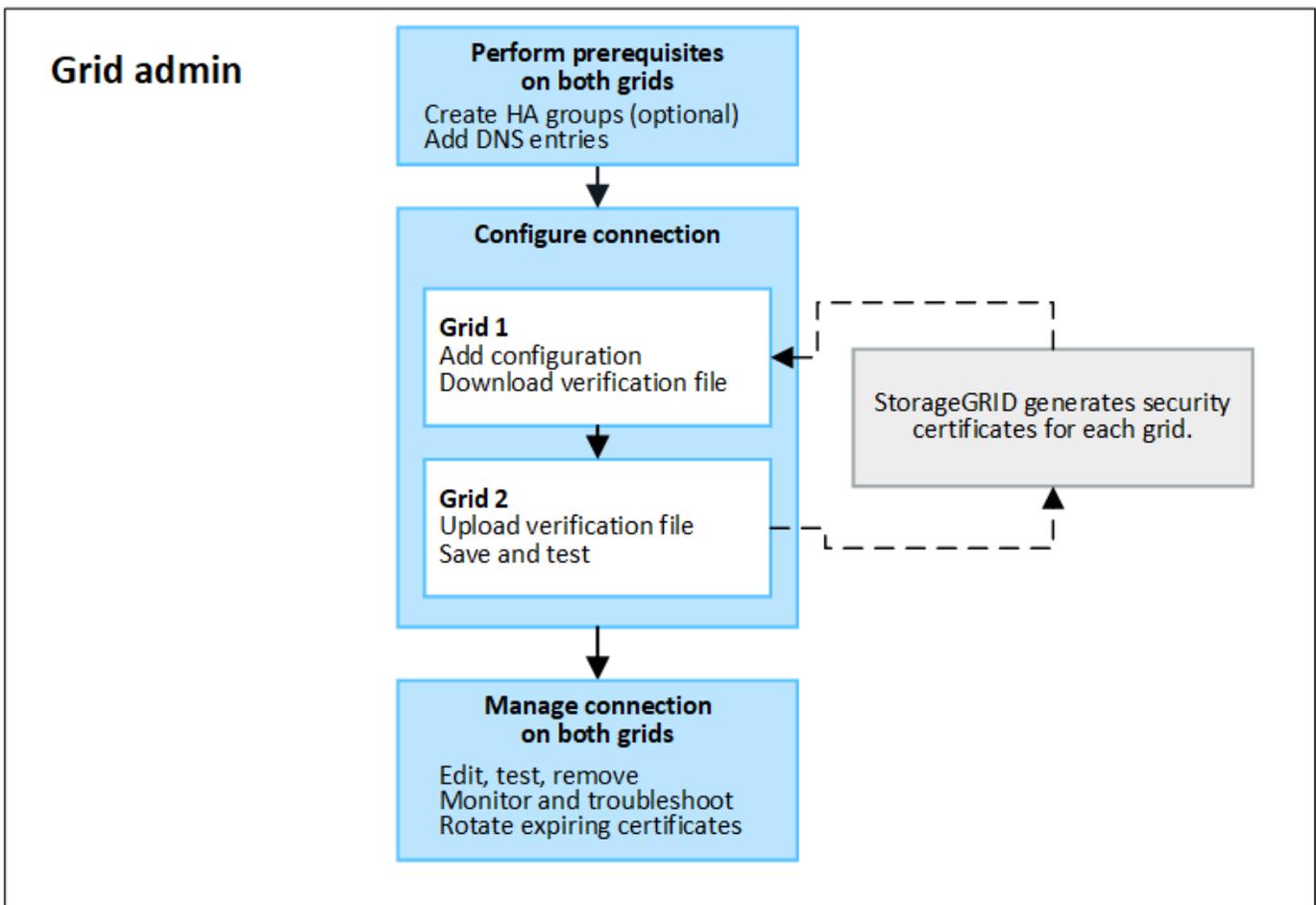
Mithilfe des Grid-Verbunds können Mandanten geklont und ihre Objekte zwischen zwei StorageGRID Systemen für das Disaster Recovery repliziert werden.

Was ist eine Netzverbundverbindung?

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

Workflow für Grid-Verbund

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



Überlegungen und Anforderungen für Netzverbundverbindungen

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

Netzwerkanforderungen und IP-Adresse

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

Verwenden Sie FQDNs, um die Verbindung auszugleichen

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

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

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

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

Port-Anforderungen

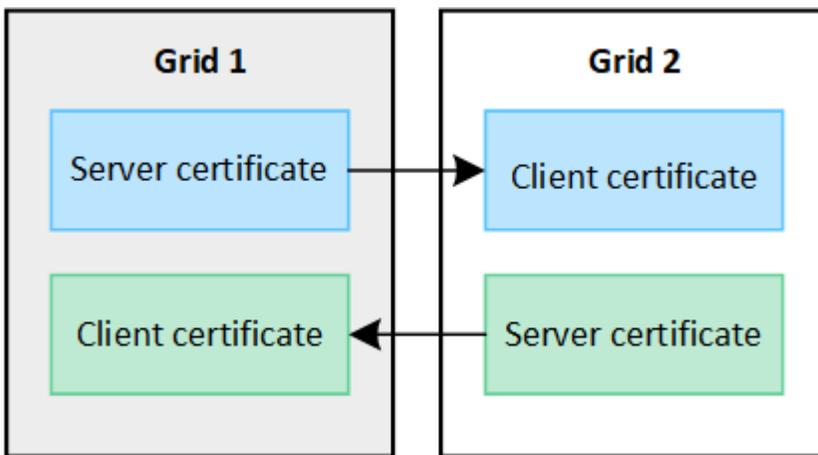
Beim Erstellen einer Grid-Federation-Verbindung können Sie alle nicht verwendeten Portnummern zwischen 23000 und 23999 angeben. Beide Grids in dieser Verbindung verwenden den gleichen Port.

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

Zertifikatanforderungen

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

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



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



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

Weitere Informationen .

- ["Erstellen von Grid Federation-Verbindungen"](#)
- ["Grid-Verbindungen verwalten"](#)
- ["Fehler beim Grid-Verbund beheben"](#)

Was ist Account-Klon?

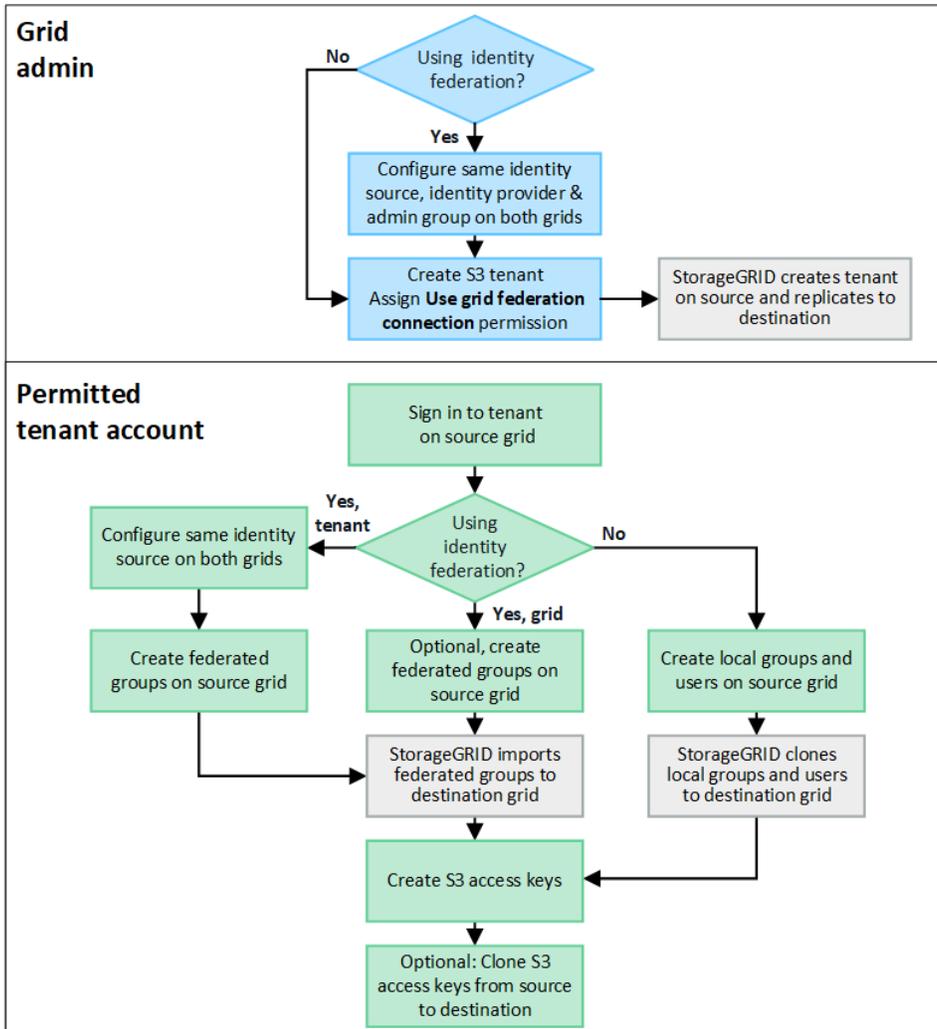
Der Account-Klon ist die automatische Replizierung eines Mandantenkontos, von Mandantengruppen und Mandantenbenutzern sowie optional: S3-Zugriffstasten zwischen den StorageGRID-Systemen in einem **"Netzverbundverbindung"**.

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

können.

Workflow für Konto-Klon

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



Grid-Administrator-Workflow

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

SSO für Kontoklone konfigurieren (optional)

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

Schritte

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

3. "[Erstellen Sie dieselbe Administratorgruppe](#)" Auf beiden Rastern durch Importieren derselben Verbundgruppe.

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



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

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

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

Schritte

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



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

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

Zulässiges S3-Mandantenkonto erstellen

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

Schritte

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

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

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

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

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

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

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

Weitere Informationen finden Sie unter "[Management zulässiger Mandanten für Grid-Verbund](#)".

Zulässiger Mandantenkonto-Workflow

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

Schritte

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

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

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

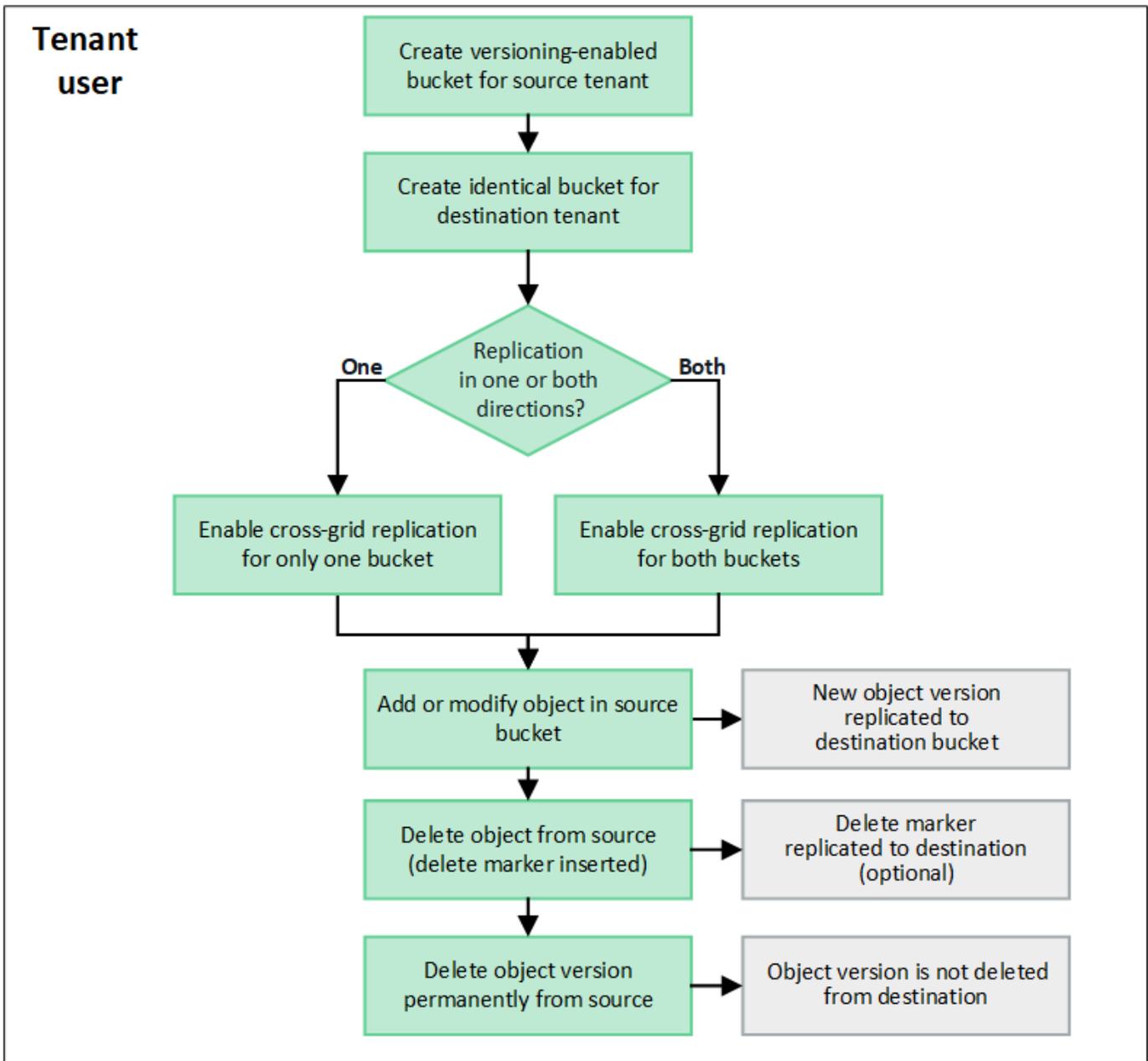
Informationen zum Workflow zulässiger Mandantenkonten und zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln finden Sie unter "[Klonen von Mandantengruppen und Benutzern](#)" Und "[Klonen von S3-Zugriffsschlüsseln mithilfe der API](#)".

Was ist Grid-übergreifende Replizierung?

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

Workflow für Grid-übergreifende Replizierung

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



Anforderungen für die Grid-übergreifende Replizierung

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

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

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

Weitere Informationen .

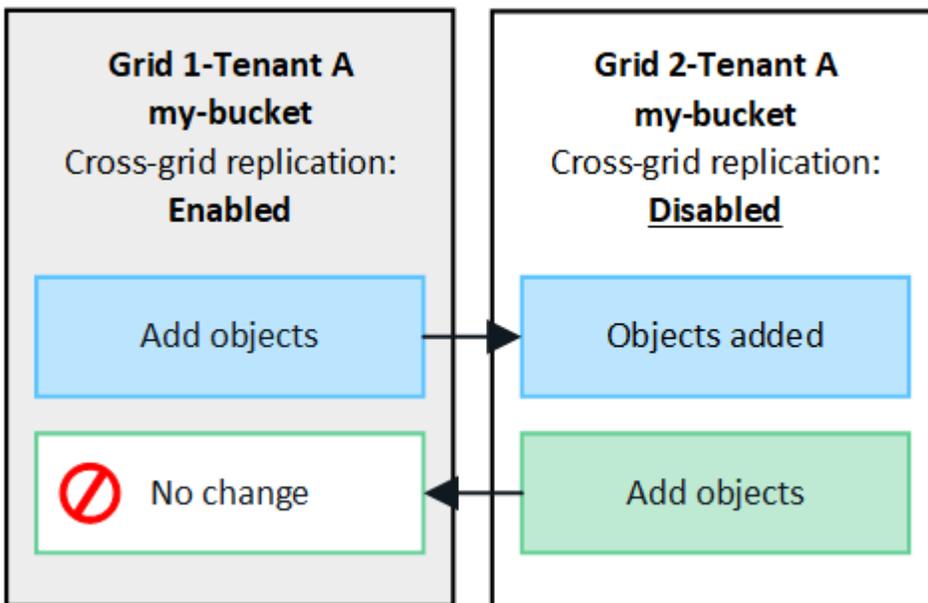
"Grid-übergreifende Replizierung managen"

Funktionsweise der Grid-übergreifenden Replizierung

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

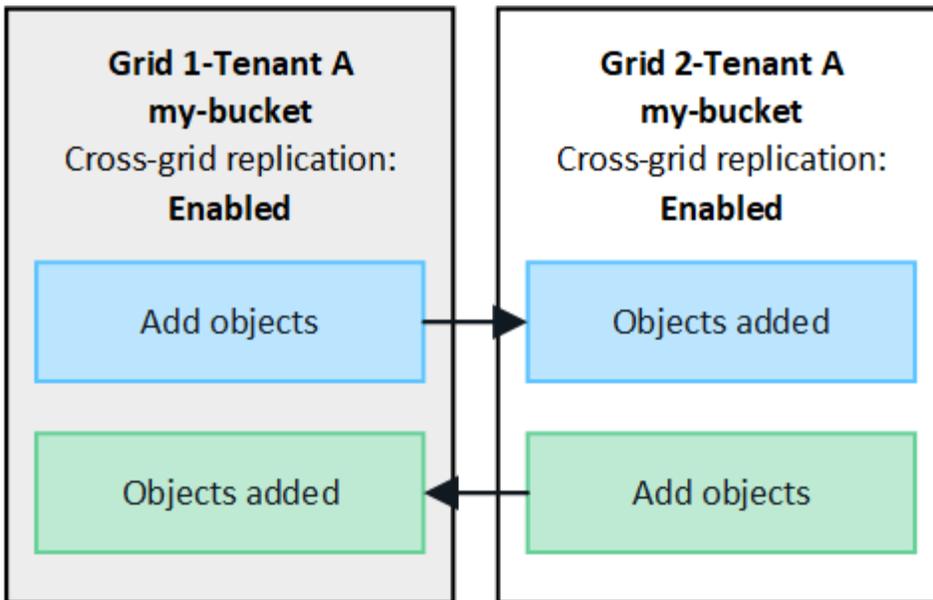
Replikation in eine Richtung

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



Replikation in beide Richtungen

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



Was passiert, wenn Objekte aufgenommen werden?

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

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

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

Raster	Replikationsstatus
Quelle	<ul style="list-style-type: none"> • SUCCESS: Die Replikation war für alle Grid-Verbindungen erfolgreich. • AUSSTEHEND: Das Objekt wurde nicht auf mindestens eine Grid-Verbindung repliziert. • FAILURE: Die Replikation steht nicht für eine Netzverbindung aus und mindestens eine ist mit einem dauerhaften Fehler ausgefallen. Ein Benutzer muss den Fehler beheben.
Ziel	REPLIKAT: Das Objekt wurde aus dem Quellraster repliziert.



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

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

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

Was passiert, wenn Objekte gelöscht werden?

Wie in beschrieben "[Löschen des Datenflusses](#)", StorageGRID kann ein Objekt aus einem der folgenden Gründe löschen:

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

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

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

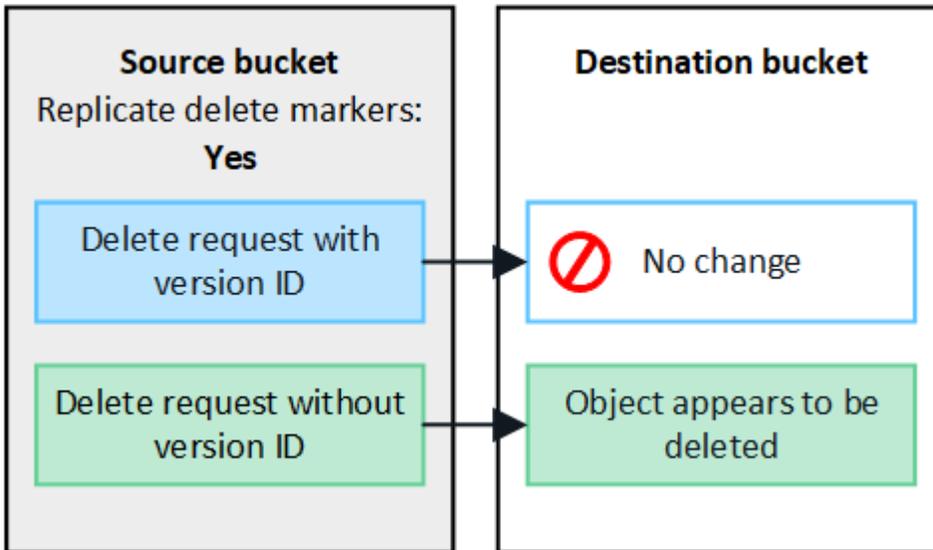
- Wenn ein S3-Client eine Löschanfrage mit einer Versions-ID ausstellt, wird diese Version des Objekts dauerhaft entfernt. Dem Bucket wurde keine Löschkennzeichnung hinzugefügt.
- Wenn ein S3-Client eine Löschanfrage ausstellt, die keine Versions-ID enthält, löscht StorageGRID keine Objektversionen.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

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

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

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

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



Wenn Sie Objektlöschungen zwischen den Rastern synchron halten möchten, erstellen Sie entsprechende "[S3 Lifecycle-Konfigurationen](#)" für die Eimer auf beiden Rastern.

Wie verschlüsselte Objekte repliziert werden

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

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



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

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

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



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

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

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

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

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

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

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

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

Wie segmentierte Objekte repliziert werden

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

Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung

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

	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Was ist der primäre Zweck?	Ein StorageGRID System fungiert als Disaster Recovery-System. Objekte in einem Bucket können zwischen den Grids in eine oder beide Richtungen repliziert werden.	Ermöglicht einem Mandanten, automatisch Objekte aus einem Bucket in StorageGRID (Quelle) in einen externen S3-Bucket (Ziel) zu replizieren Bei der CloudMirror-Replizierung wird eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur erstellt. Diese unabhängige Kopie wird nicht als Backup verwendet, sondern häufig weiter in der Cloud verarbeitet.
Wie ist es eingerichtet?	<ol style="list-style-type: none"> 1. Konfigurieren Sie eine Grid Federation-Verbindung zwischen zwei Grids. 2. Fügen Sie neue Mandantenkonten hinzu, die automatisch in der anderen Tabelle geklont werden. 3. Fügen Sie neue Mandantengruppen und -Benutzer hinzu, die ebenfalls geklont werden. 4. Erstellen Sie entsprechende Buckets in jedem Grid und ermöglichen Sie die Grid-übergreifende Replizierung in eine oder beide Richtungen. 	<ol style="list-style-type: none"> 1. Ein Mandantenbenutzer konfiguriert die CloudMirror-Replizierung mithilfe des Tenant Manager oder der S3-API durch Definition eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.). 2. Jeder Bucket dieses Mandantenkontos kann so konfiguriert werden, dass er auf den CloudMirror-Endpunkt verweisen kann.
Wer ist für die Einrichtung zuständig?	<ul style="list-style-type: none"> • Ein Grid-Administrator konfiguriert die Verbindung und die Mandanten. • Mandantenbenutzer konfigurieren die Gruppen, Benutzer, Schlüssel und Buckets. 	Normalerweise wird ein Mandantenbenutzer verwendet.
Was ist das Ziel?	Ein entsprechender und identischer S3-Bucket auf dem anderen StorageGRID-System in der Grid-Federation-Verbindung.	<ul style="list-style-type: none"> • Kompatible S3-Infrastruktur (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Ist eine Objektversionierung erforderlich?	Ja, sowohl in den Quell- als auch in den Ziel-Buckets muss die Objektversionierung aktiviert sein.	Nein, die CloudMirror Replizierung unterstützt beliebige Kombinationen aus unversionierten und versionierten Buckets sowohl am Quell- als auch am Zielsystem.

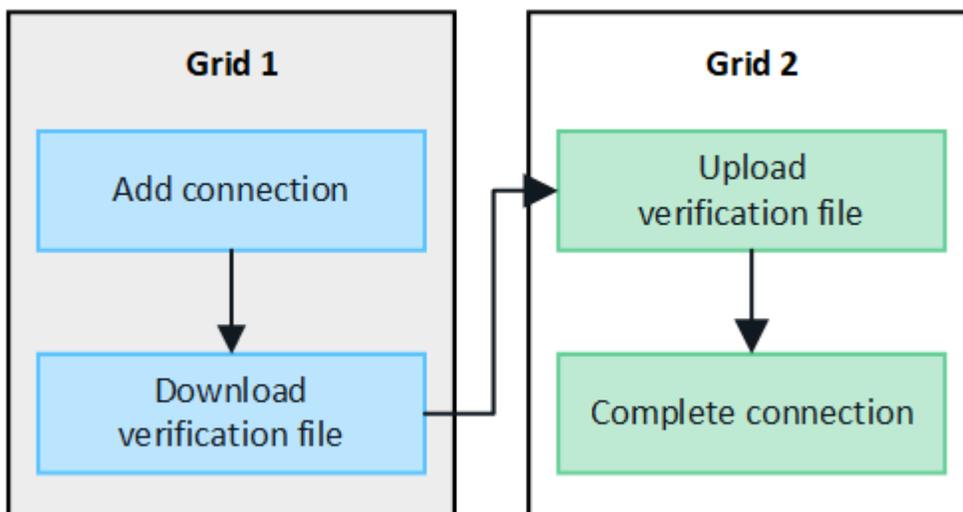
	Grid-übergreifende Replizierung	CloudMirror Replikationservice
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Objekte werden automatisch repliziert, wenn sie zu einem Bucket hinzugefügt werden, für den die Grid-übergreifende Replizierung aktiviert ist.	Objekte werden automatisch repliziert, wenn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

	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Was passiert, wenn ein Objekt gelöscht wird?	<ul style="list-style-type: none"> • Löschanforderungen, die eine Versions-ID enthalten, werden nie in das Zielraster repliziert. • Löschanforderungen, die keine Versions-ID enthalten, fügen dem Quell-Bucket eine Löschkmarkierung hinzu, die optional in das Zielraster repliziert werden kann. • Wenn die Grid-übergreifende Replizierung nur für eine Richtung konfiguriert ist, können Objekte im Ziel-Bucket gelöscht werden, ohne die Quelle zu beeinträchtigen. 	<p>Die Ergebnisse variieren je nach Versionsstatus der Quell- und Ziel-Buckets (die nicht identisch sein müssen):</p> <ul style="list-style-type: none"> • Wenn beide Buckets versioniert sind, wird bei einer Löschanforderung an beiden Standorten eine Löschkmarkierung hinzugefügt. • Wenn nur der Quell-Bucket versioniert ist, fügt eine Löschanforderung der Quelle eine Löschkmarkierung hinzu, nicht jedoch dem Ziel. • Wenn kein Bucket versioniert ist, wird das Objekt durch eine Löschanforderung aus der Quelle, aber nicht aus dem Ziel gelöscht. <p>Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass die Quelle beeinträchtigt wird.</p>

Erstellen von Grid Federation-Verbindungen

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

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



Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen](#)" Zur Konfiguration von Grid Federation-Verbindungen.

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

Verbindung hinzufügen

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

Schritte

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

Feld	Beschreibung
Verbindungsname	Ein eindeutiger Name, der Ihnen hilft, diese Verbindung zu erkennen, z. B. „Raster 1-Raster 2“
FQDN oder IP für dieses Raster	Eine der folgenden Optionen: <ul style="list-style-type: none"> • Der FQDN des Rasters, bei dem Sie derzeit angemeldet sind • Eine VIP-Adresse einer HA-Gruppe in diesem Raster • Eine IP-Adresse eines Admin-Knotens oder Gateway-Knotens in diesem Grid. Die IP kann sich auf jedem Netzwerk befinden, das das Zielraster erreichen kann.
Port	Der Port, den Sie für diese Verbindung verwenden möchten. Sie können eine beliebige nicht verwendete Portnummer zwischen 23000 und 23999 eingeben. Beide Grids in dieser Verbindung verwenden den gleichen Port. Sie müssen sicherstellen, dass kein Node in einem Grid diesen Port für andere Verbindungen verwendet.
Zertifikat gültige Tage für dieses Raster	Die Anzahl der Tage, an denen die Sicherheitszertifikate für dieses Raster in der Verbindung gültig sein sollen. Der Standardwert ist 730 Tage (2 Jahre), Sie können jedoch einen beliebigen Wert zwischen 1 und 762 Tagen eingeben. StorageGRID generiert automatisch Client- und Serverzertifikate für jedes Grid, wenn Sie die Verbindung speichern.
Provisionierungs-Passphrase für dieses Grid	Die Provisionierungs-Passphrase für das Grid, bei dem Sie angemeldet sind.

Feld	Beschreibung
FQDN oder IP für das andere Raster	<p>Eine der folgenden Optionen:</p> <ul style="list-style-type: none"> • Der FQDN des Rasters, mit dem Sie eine Verbindung herstellen möchten • Eine VIP-Adresse einer HA-Gruppe im anderen Raster • Eine IP-Adresse eines Admin-Knotens oder Gateway-Knotens im anderen Grid. Die IP kann sich auf jedem Netzwerk befinden, das das Quellraster erreichen kann.

5. Wählen Sie **Speichern und fortfahren**.

6. Wählen Sie für den Schritt zum Download der Überprüfungsdatei **Download der Überprüfungsdatei** aus.

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

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



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

8. Wählen Sie **Schließen**, um zur Seite Grid Federation zurückzukehren.

9. Bestätigen Sie, dass die neue Verbindung angezeigt wird und ihr **Verbindungsstatus Waiting to connect** ist.

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

Vollständige Verbindung

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

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.

2. Wählen Sie **CONFIGURATION > System > Grid Federation**.

3. Wählen Sie **Upload Verification file**, um auf die Seite Upload zuzugreifen.

4. Wählen Sie **Überprüfungsdatei hochladen**. Navigieren Sie dann zu der Datei, die aus dem ersten Raster heruntergeladen wurde, und wählen Sie sie aus (*connection-name.grid-federation*).

Die Details für die Verbindung werden angezeigt.

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

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



Wenn die Zertifikate an einem der beiden Enden der Verbindung ablaufen, wird die Verbindung unterbrochen und Replikationen stehen aus, bis die Zertifikate aktualisiert werden.

6. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie derzeit angemeldet sind.

7. Wählen Sie **Speichern und testen**.

Die Zertifikate werden generiert und die Verbindung wird getestet. Wenn die Verbindung gültig ist, wird eine Erfolgsmeldung angezeigt, und die neue Verbindung wird auf der Seite Grid Federation aufgeführt. Der **Verbindungsstatus** wird **verbunden**.

Wenn eine Fehlermeldung angezeigt wird, beheben Sie alle Probleme. Siehe "[Fehler beim Grid-Verbund beheben](#)".

8. Rufen Sie die Seite Grid Federation im ersten Raster auf, und aktualisieren Sie den Browser. Bestätigen Sie, dass der **Verbindungsstatus** jetzt **verbunden** ist.

9. Löschen Sie nach dem Verbindungsaufbau alle Kopien der Überprüfungsdatei sicher.

Wenn Sie diese Verbindung bearbeiten, wird eine neue Überprüfungsdatei erstellt. Die Originaldatei kann nicht wiederverwendet werden.

Nachdem Sie fertig sind

- Besprechen Sie die Überlegungen für "[Management zulässiger Mandanten](#)".
- "[Erstellen Sie ein oder mehrere neue Mandantenkonten](#)", Weisen Sie die Berechtigung **use Grid Federation connection** zu und wählen Sie die neue Verbindung aus.
- "[Verwalten Sie die Verbindung](#)" Nach Bedarf. Sie können Verbindungswerte bearbeiten, eine Verbindung testen, Verbindungszertifikate drehen oder eine Verbindung entfernen.
- "[Überwachen Sie die Verbindung](#)" Im Rahmen Ihrer normalen StorageGRID-Monitoring-Aktivitäten.
- "[Beheben Sie die Verbindungsherstellung](#)", Einschließlich der Behebung von Warnungen und Fehlern im Zusammenhang mit Account-Clone und Grid-Replikation.

Grid-Verbindungen verwalten

Das Management von Grid-Verbindungen zwischen StorageGRID Systemen umfasst das Bearbeiten von Verbindungsdetails, das Drehen der Zertifikate, das Entfernen von Mandantenberechtigungen und das Entfernen nicht verwendeter Verbindungen.

Bevor Sie beginnen

- Sie sind auf beiden Rastergittern mit einem beim Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Root-Zugriffsberechtigung für das Raster, bei dem Sie angemeldet sind.

Bearbeiten einer Verbindung zum Grid Federation

Sie können eine Grid Federation-Verbindung bearbeiten, indem Sie sich beim primären Admin-Node auf einem der beiden Raster der Verbindung anmelden. Nachdem Sie Änderungen am ersten Raster vorgenommen haben, müssen Sie eine neue Überprüfungsdatei herunterladen und in das andere Raster hochladen.



Während die Verbindung bearbeitet wird, werden Kontoklone- oder Grid-übergreifende Replikationsanforderungen weiterhin die vorhandenen Verbindungseinstellungen verwenden. Alle Änderungen, die Sie am ersten Raster vornehmen, werden lokal gespeichert, aber erst dann verwendet, wenn sie in das zweite Raster hochgeladen, gespeichert und getestet wurden.

Beginnen Sie mit der Bearbeitung der Verbindung

Schritte

1. Melden Sie sich über den primären Admin-Node auf beiden Grids beim Grid-Manager an.
2. Wählen Sie **NODES** aus und bestätigen Sie, dass alle anderen Admin-Knoten in Ihrem System online sind.



Beim Bearbeiten einer Grid-Federation-Verbindung versucht StorageGRID, eine Datei „Candidate Configuration“ auf allen Admin-Knoten im ersten Raster zu speichern. Wenn diese Datei nicht in allen Admin-Knoten gespeichert werden kann, wird eine Warnmeldung angezeigt, wenn Sie **Speichern und Testen** auswählen.

3. Wählen Sie **CONFIGURATION > System > Grid Federation**.
4. Bearbeiten Sie die Verbindungsdetails über das Menü **actions** auf der Seite Grid Federation oder über die Detailseite für eine bestimmte Verbindung. Siehe "[Erstellen von Grid Federation-Verbindungen](#)" Für das, was zu betreten ist.

Menü „Aktionen“

- a. Wählen Sie das Optionsfeld für die Verbindung aus.
- b. Wählen Sie **Actions > Edit**.
- c. Geben Sie die neuen Informationen ein.

Detailseite

- a. Wählen Sie einen Verbindungsnamen aus, um dessen Details anzuzeigen.
- b. Wählen Sie **Bearbeiten**.
- c. Geben Sie die neuen Informationen ein.

5. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie angemeldet sind.
6. Wählen Sie **Speichern und fortfahren**.

Die neuen Werte werden gespeichert, werden aber erst dann auf die Verbindung angewendet, wenn Sie die neue Überprüfungsdatei auf das andere Raster hochgeladen haben.

7. Wählen Sie **Überprüfungsdatei herunterladen**.

Um diese Datei zu einem späteren Zeitpunkt herunterzuladen, gehen Sie zur Detailseite für die Verbindung.

8. Suchen Sie die heruntergeladene Datei (*connection-name.grid-federation*), und speichern Sie es an einem sicheren Ort.



Die Überprüfungsdatei enthält Geheimnisse und muss sicher gespeichert und übertragen werden.

9. Wählen Sie **Schließen**, um zur Seite Grid Federation zurückzukehren.
10. Bestätigen Sie, dass der **Verbindungsstatus ausstehende Bearbeitung** ist.



Wenn der Verbindungsstatus etwas anderes als **Verbunden** war, als Sie mit der Bearbeitung der Verbindung begonnen haben, ändert er sich nicht in **Ausstehende Bearbeitung**.

11. Versorgen `connection-name.grid-federation` Datei an den Grid-Administrator für das andere Grid.

Schließen Sie die Bearbeitung der Verbindung ab

Schließen Sie die Bearbeitung der Verbindung ab, indem Sie die Überprüfungsdatei auf das andere Raster hochladen.

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **CONFIGURATION > System > Grid Federation**.
3. Wählen Sie **Upload Verification file**, um auf die Upload-Seite zuzugreifen.
4. Wählen Sie **Überprüfungsdatei hochladen**. Navigieren Sie dann zu der Datei, die aus dem ersten Raster heruntergeladen wurde, und wählen Sie sie aus.
5. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie derzeit angemeldet sind.
6. Wählen Sie **Speichern und testen**.

Wenn die Verbindung über die bearbeiteten Werte hergestellt werden kann, wird eine Erfolgsmeldung angezeigt. Andernfalls wird eine Fehlermeldung angezeigt. Überprüfen Sie die Nachricht und beheben Sie alle Probleme.

7. Schließen Sie den Assistenten, um zur Seite „Grid Federation“ zurückzukehren.
8. Bestätigen Sie, dass der **Verbindungsstatus verbunden** ist.
9. Rufen Sie die Seite Grid Federation im ersten Raster auf, und aktualisieren Sie den Browser. Bestätigen Sie, dass der **Verbindungsstatus** jetzt **verbunden** ist.
10. Löschen Sie nach dem Verbindungsaufbau alle Kopien der Überprüfungsdatei sicher.

Testen einer Netzverbundverbindung

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **CONFIGURATION > System > Grid Federation**.
3. Testen Sie die Verbindung mit dem Menü **actions** auf der Seite Grid Federation oder der Detailseite für eine bestimmte Verbindung.

Menü „Aktionen“

- a. Wählen Sie das Optionsfeld für die Verbindung aus.
- b. Wählen Sie **Actions > Test**.

Detailseite

- a. Wählen Sie einen Verbindungsnamen aus, um dessen Details anzuzeigen.
- b. Wählen Sie **Verbindung testen**.

4. Überprüfen Sie den Verbindungsstatus:

Verbindungsstatus	Beschreibung
Verbunden	Beide Netze sind angeschlossen und kommunizieren normal.
Fehler	Die Verbindung befindet sich in einem Fehlerzustand. Beispielsweise ist ein Zertifikat abgelaufen oder ein Konfigurationswert ist nicht mehr gültig.
Bearbeitung ausstehend	Sie haben die Verbindung in diesem Raster bearbeitet, aber die Verbindung verwendet weiterhin die vorhandene Konfiguration. Um die Bearbeitung abzuschließen, laden Sie die neue Überprüfungsdatei in das andere Raster hoch.
Warten auf Verbindung	Sie haben die Verbindung in diesem Raster konfiguriert, aber die Verbindung wurde auf dem anderen Raster nicht abgeschlossen. Laden Sie die Überprüfungsdatei von diesem Raster herunter, und laden Sie sie in das andere Raster hoch.
Unbekannt	Die Verbindung befindet sich in einem unbekanntem Zustand, möglicherweise aufgrund eines Netzwerkproblems oder eines Offline-Knotens.

5. Wenn der Verbindungsstatus **Error** lautet, beheben Sie alle Probleme. Wählen Sie dann erneut **Verbindung testen** aus, um zu bestätigen, dass das Problem behoben wurde.

Verbindungszertifikate drehen

Jede Grid Federation-Verbindung verwendet vier automatisch generierte SSL-Zertifikate, um die Verbindung zu sichern. Wenn die beiden Zertifikate für jedes Raster in der Nähe ihres Ablaufdatums liegen, erinnert die Warnung **Ablauf des Grid Federation Certificate** Sie daran, die Zertifikate zu drehen.



Wenn die Zertifikate an einem der beiden Enden der Verbindung ablaufen, wird die Verbindung unterbrochen und Replikationen stehen aus, bis die Zertifikate aktualisiert werden.

Schritte

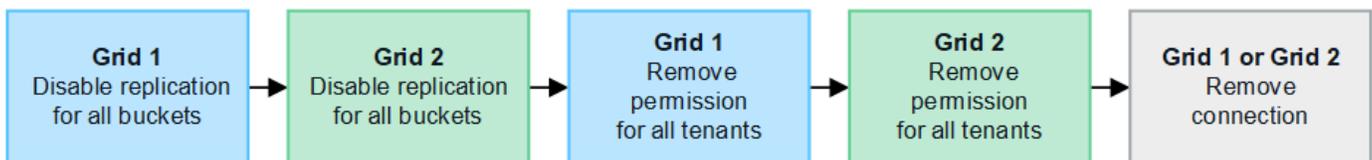
1. Melden Sie sich über den primären Admin-Node auf beiden Grids beim Grid-Manager an.
2. Wählen Sie **CONFIGURATION > System > Grid Federation**.

3. Wählen Sie auf einer der Registerkarten auf der Seite Grid Federation den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
4. Wählen Sie die Registerkarte **Zertifikate** aus.
5. Wählen Sie **Zertifikate drehen**.
6. Geben Sie an, wie viele Tage die neuen Zertifikate gültig sein sollen.
7. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie angemeldet sind.
8. Wählen Sie **Zertifikate drehen**.
9. Wiederholen Sie diese Schritte bei Bedarf auf dem anderen Raster der Verbindung.

Verwenden Sie im Allgemeinen die gleiche Anzahl von Tagen für die Zertifikate auf beiden Seiten der Verbindung.

Entfernen Sie eine Netzverbundverbindung

Sie können eine Netzverbundverbindung aus jedem Raster der Verbindung entfernen. Wie in der Abbildung gezeigt, müssen Sie auf beiden Rastern erforderliche Schritte ausführen, um zu bestätigen, dass die Verbindung nicht von einem Mandanten in einem der beiden Raster verwendet wird.



Beachten Sie vor dem Entfernen einer Verbindung Folgendes:

- Durch das Entfernen einer Verbindung werden keine Elemente gelöscht, die bereits zwischen den Rastern kopiert wurden. So werden beispielsweise Mandantenbenutzer, -Gruppen und -Objekte, die auf beiden Grids vorhanden sind, nicht aus beiden Grids gelöscht, wenn die Berechtigung des Mandanten entfernt wird. Wenn Sie diese Elemente löschen möchten, müssen Sie sie manuell aus beiden Rastern löschen.
- Wenn Sie eine Verbindung entfernen, wird die Replikation aller Objekte, die noch nicht repliziert werden (aufgenommen, aber noch nicht in das andere Grid repliziert), dauerhaft fehlgeschlagen.

Deaktivieren Sie die Replizierung für alle Mandanten-Buckets

Schritte

1. Melden Sie sich vom primären Admin-Node aus an einem der beiden Raster beim Grid Manager an.
2. Wählen Sie **CONFIGURATION > System > Grid Federation**.
3. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
4. Bestimmen Sie auf der Registerkarte **zulässige Mieter**, ob die Verbindung von einem Mieter verwendet wird.
5. Wenn Mieter aufgeführt sind, weisen Sie alle Mieter an "[Deaktivieren Sie die Grid-übergreifende Replizierung](#)" Für alle Eimer auf beiden Rastern in der Verbindung.



Sie können die Berechtigung **use Grid Federation connection** nicht entfernen, wenn in einem Mandanten-Buckets die Grid-übergreifende Replikation aktiviert ist. Jedes Mandantenkonto muss die Grid-übergreifende Replizierung für seine Buckets auf beiden Grids deaktivieren.

Berechtigung für jeden Mandanten entfernen

Nachdem die Grid-übergreifende Replikation für alle Mandanten-Buckets deaktiviert wurde, entfernen Sie die **use Grid Federation permission** von allen Mandanten auf beiden Grids.

Schritte

1. Wählen Sie **CONFIGURATION > System > Grid Federation**.
2. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
3. Entfernen Sie für jeden Mandanten auf der Registerkarte **zulässige Mieter** die Berechtigung **Grid Federation connection** von jedem Mandanten. Siehe "[Management zulässiger Mandanten](#)".
4. Wiederholen Sie diese Schritte für die zulässigen Mandanten im anderen Raster.

Verbindung entfernen

Schritte

1. Wenn keine Mieter in einem der beiden Raster die Verbindung verwenden, wählen Sie **Entfernen**.
2. Überprüfen Sie die Bestätigungsmeldung, und wählen Sie **Entfernen**.
 - Wenn die Verbindung entfernt werden kann, wird eine Erfolgsmeldung angezeigt. Die Netzverbundverbindung wird nun aus beiden Grids entfernt.
 - Wenn die Verbindung nicht entfernt werden kann (z. B. wird sie noch verwendet oder es liegt ein Verbindungsfehler vor), wird eine Fehlermeldung angezeigt. Sie können eine der folgenden Aktionen ausführen:
 - Beheben Sie den Fehler (empfohlen). Siehe "[Fehler beim Grid-Verbund beheben](#)".
 - Entfernen Sie die Verbindung mit Gewalt. Siehe nächster Abschnitt.

Entfernen Sie eine Verbindung zum Grid-Verbund mit Gewalt

Bei Bedarf können Sie das Entfernen einer Verbindung erzwingen, die nicht den Status **Verbunden** hat.

Das Entfernen erzwingen löscht nur die Verbindung aus dem lokalen Grid. Um die Verbindung vollständig zu entfernen, führen Sie die gleichen Schritte auf beiden Rastern aus.

Schritte

1. Wählen Sie im Bestätigungsdialogfeld **Entfernen erzwingen** aus.

Eine Erfolgsmeldung wird angezeigt. Diese Netzverbundverbindung kann nicht mehr verwendet werden. Allerdings ist für Mandanten-Buckets möglicherweise weiterhin die Grid-übergreifende Replizierung aktiviert, und einige Objektkopien wurden möglicherweise bereits zwischen den Grids in der Verbindung repliziert.

2. Melden Sie sich vom anderen Raster der Verbindung aus über den primären Admin-Node beim Grid Manager an.
3. Wählen Sie **CONFIGURATION > System > Grid Federation**.
4. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
5. Wählen Sie **Entfernen** und **Ja**.
6. Wählen Sie **Entfernen erzwingen**, um die Verbindung aus diesem Raster zu entfernen.

Verwalten Sie die zulässigen Mandanten für den Grid-Verbund

Sie können neuen S3-Mandantenkonten die Verwendung einer Grid-Federation-Verbindung zwischen zwei StorageGRID-Systemen gestatten. Wenn Mandanten eine Verbindung verwenden dürfen, sind spezielle Schritte erforderlich, um die Mandantendetails zu bearbeiten oder die Berechtigung eines Mandanten zur Verwendung der Verbindung dauerhaft zu entfernen.

Bevor Sie beginnen

- Sie sind auf beiden Rastergittern mit einem beim Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie verfügen über die Root-Zugriffsberechtigung für das Raster, bei dem Sie angemeldet sind.
- Das ist schon ["Grid Federation-Verbindung erstellt"](#) Zwischen zwei Rastern.
- Sie haben die Workflows für überprüft ["Konto-Klon"](#) Und ["Grid-übergreifende Replizierung"](#).
- Bei Bedarf haben Sie bereits Single Sign-On (SSO) oder Identify Federation für beide Grids in der Verbindung konfiguriert. Siehe ["Was ist Account-Klon"](#).

Erstellen Sie eine zulässige Serviceeinheit

Wenn Sie einem Mandantenkonto die Verwendung einer Grid-Federation-Verbindung für den Account-Klon und die Grid-übergreifende Replizierung erlauben möchten, befolgen Sie die allgemeinen Anweisungen auf ["Erstellen Sie einen neuen S3-Mandanten"](#) Und beachten Sie Folgendes:

- Sie können die Serviceeinheit aus jedem Raster der Verbindung erstellen. Das Raster, in dem ein Mandant erstellt wird, ist das Quellraster des *Mandanten*.
- Der Status der Verbindung muss **connected** sein.
- Sie können nur die Berechtigung **Grid Federation connection** verwenden auswählen, wenn Sie einen neuen S3-Mandanten erstellen; Sie können diese Berechtigung nicht aktivieren, wenn Sie einen vorhandenen Mandanten bearbeiten.
- Wenn der neue Mandant im ersten Grid gespeichert wird, wird ein identischer Mandant automatisch in das andere Grid repliziert. Das Grid, in dem der Mandant repliziert wird, ist das Zielraster des *Mandanten*.
- Die Mandanten in beiden Grids haben die gleiche 20-stellige Konto-ID, den gleichen Namen, die gleiche Beschreibung, das gleiche Kontingent und die gleichen Berechtigungen. Optional können Sie das Feld **Beschreibung** verwenden, um zu ermitteln, welcher Quellmandant und welcher Zielmandant ist. Beispielsweise wird diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den Mandanten angezeigt, der in Grid 2 repliziert wurde: „dieser Mandant wurde in Grid 1 erstellt.“
- Aus Sicherheitsgründen wird das Kennwort für einen lokalen Root-Benutzer nicht in das Zielraster kopiert.



Bevor ein lokaler Root-Benutzer sich beim replizierten Mandanten im Zielraster anmelden kann, muss ein Grid-Administrator für dieses Grid angemeldet sein ["Ändern Sie das Passwort für den lokalen Root-Benutzer"](#).

- Nachdem der neue Mandant auf beiden Grids verfügbar ist, können Mandantenbenutzer die folgenden Aufgaben durchführen:
 - Erstellen Sie im Quellraster des Mandanten Gruppen und lokale Benutzer, die automatisch im Zielraster des Mandanten geklont werden. Siehe ["Klonen von Mandantengruppen und Benutzern"](#).
 - Erstellen neuer S3-Zugriffsschlüssel, die optional im Zielraster des Mandanten geklont werden können. Siehe ["Klonen von S3-Zugriffsschlüsseln mithilfe der API"](#).

- Erstellen Sie auf beiden Grids in der Verbindung identische Buckets und ermöglichen Sie die Grid-übergreifende Replizierung in eine oder beide Richtungen. Siehe "[Grid-übergreifende Replizierung managen](#)".

Zeigen Sie eine zulässige Serviceeinheit an

Sie können Details zu einem Mandanten anzeigen, der eine Verbindung mit dem Grid Federation verwenden darf.

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie auf der Seite Tenants den Namen der Serviceeinheit aus, um die Seite mit den Details der Serviceeinheit anzuzeigen.

Wenn es sich hierbei um das Quellraster für den Mandanten handelt (d. h. wenn der Mandant in diesem Raster erstellt wurde), wird ein Banner angezeigt, das Sie daran erinnert, dass der Mandant in einem anderen Raster geklont wurde. Wenn Sie diesen Mandanten bearbeiten oder löschen, werden Ihre Änderungen nicht mit dem anderen Raster synchronisiert.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

[Sign in](#) [Edit](#) [Actions](#) ▾

i This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

[Space breakdown](#) [Allowed features](#) **Grid federation**

[Remove permission](#) [Clear error](#) Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
Grid 1 to Grid 2	Connected	10.96.106.230	Check for errors

3. Wählen Sie optional die Registerkarte **Grid Federation** aus "[Überwachen der Netzverbundverbindung](#)".

Bearbeiten Sie eine zulässige Serviceeinheit

Wenn Sie einen Mandanten bearbeiten müssen, der über die Berechtigung **Grid Federation connection** verfügt, befolgen Sie die allgemeinen Anweisungen für "[Bearbeiten eines Mandantenkontos](#)" Und beachten Sie Folgendes:

- Wenn ein Mandant über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Mandantendetails von beiden Rastergittern in der Verbindung bearbeiten. Alle Änderungen, die Sie vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Details der Serviceeinheit zwischen den Rastern synchronisieren möchten, müssen Sie die gleichen Änderungen an beiden Rastern vornehmen.
- Sie können die Berechtigung **Grid Federation connection** verwenden* nicht löschen, wenn Sie einen Mandanten bearbeiten.
- Sie können keine andere Grid Federation-Verbindung auswählen, wenn Sie eine Serviceeinheit bearbeiten.

Löschen Sie eine zulässige Serviceeinheit

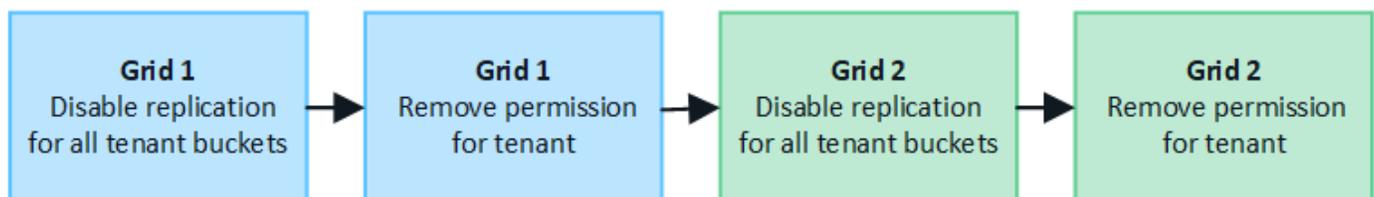
Wenn Sie einen Mieter entfernen müssen, der über die Berechtigung **Grid Federation connection** verfügt, befolgen Sie die allgemeinen Anweisungen für "[Löschen eines Mandantenkontos](#)" Und beachten Sie Folgendes:

- Bevor Sie den ursprünglichen Mandanten im Quellraster entfernen können, müssen Sie alle Buckets für das Konto im Quellraster entfernen.
- Bevor Sie den geklonten Mandanten im Zielraster entfernen können, müssen Sie alle Buckets für das Konto im Zielraster entfernen.
- Wenn Sie den ursprünglichen oder den geklonten Mandanten entfernen, kann das Konto nicht mehr für die Grid-übergreifende Replizierung verwendet werden.
- Wenn Sie den ursprünglichen Mandanten im Quellraster entfernen, werden alle Mandantengruppen, Benutzer oder Schlüssel, die im Zielraster geklont wurden, nicht beeinträchtigt. Sie können den geklonten Mandanten entweder löschen oder seiner eigenen Gruppe, Benutzern, Zugriffsschlüsseln und Buckets verwalten.
- Wenn Sie den geklonten Mandanten im Zielraster entfernen, treten Klonfehler auf, wenn dem ursprünglichen Mandanten neue Gruppen oder Benutzer hinzugefügt werden.

Um diese Fehler zu vermeiden, entfernen Sie die Berechtigung des Mandanten zur Verwendung der Grid Federation-Verbindung, bevor Sie den Mandanten aus diesem Raster löschen.

Remove Use Grid Federation connection permission

Um zu verhindern, dass ein Mandant eine Netzverbundverbindung verwendet, müssen Sie die Berechtigung **Grid Federation Connection** verwenden entfernen.



Beachten Sie Folgendes, bevor Sie die Berechtigung eines Mandanten zur Verwendung einer Grid-Federation-Verbindung entfernen:

- Das Entfernen der Berechtigung **use Grid Federation connection** von einem Mieter ist eine permanente Aktion. Sie können die Berechtigung für diesen Mandanten nicht erneut aktivieren.
- Sie können die Berechtigung **use Grid Federation connection** nicht entfernen, wenn eine der Buckets des Mandanten Grid-übergreifende Replikation aktiviert hat. Das Mandantenkonto muss zunächst die Grid-übergreifende Replizierung für alle Buckets deaktivieren.
- Wenn Sie die Berechtigung **Grid Federation connection** verwenden entfernen, werden keine Elemente gelöscht, die bereits zwischen den Rastern repliziert wurden. So werden beispielsweise alle Mandantenbenutzer, -Gruppen und -Objekte, die auf beiden Grids vorhanden sind, nicht aus beiden Grids gelöscht, wenn die Berechtigung des Mandanten entfernt wird. Wenn Sie diese Elemente löschen möchten, müssen Sie sie manuell aus beiden Rastern löschen.

Bevor Sie beginnen

- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Root-Zugriffsberechtigung für beide Raster.

Deaktivieren Sie die Replizierung für Mandanten-Buckets

Deaktivieren Sie als ersten Schritt die Grid-übergreifende Replizierung für alle Mandanten-Buckets.

Schritte

1. Melden Sie sich vom primären Admin-Node aus an einem der beiden Raster beim Grid Manager an.
2. Wählen Sie **CONFIGURATION > System > Grid Federation**.
3. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
4. Bestimmen Sie auf der Registerkarte **zulässige Mieter**, ob der Mieter die Verbindung nutzt.
5. Wenn der Mieter aufgeführt ist, weisen Sie ihn an "[Deaktivieren Sie die Grid-übergreifende Replizierung](#)" Für alle Eimer auf beiden Rastern in der Verbindung.



Sie können die Berechtigung **use Grid Federation connection** nicht entfernen, wenn in einem Mandanten-Buckets die Grid-übergreifende Replikation aktiviert ist. Der Mandant muss die Grid-übergreifende Replizierung für seine Buckets auf beiden Grids deaktivieren.

Berechtigung für Serviceeinheit entfernen

Nachdem die Grid-übergreifende Replizierung für Mandanten-Buckets deaktiviert ist, können Sie die Berechtigung des Mandanten zur Verwendung der Grid-Verbundverbindung entfernen.

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Entfernen Sie die Berechtigung von der Seite „Grid Federation“ oder der Seite „Tenants“.

Seite „Grid Federation“

- a. Wählen Sie **CONFIGURATION > System > Grid Federation**.
- b. Wählen Sie den Verbindungsnamen aus, um die Detailseite anzuzeigen.
- c. Wählen Sie auf der Registerkarte **zulässige Mieter** die Optionsschaltfläche für den Mieter aus.
- d. Wählen Sie **Berechtigung entfernen**.

Mandanten werden gestartet

- a. Wählen Sie **MIETER**.
- b. Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen.
- c. Wählen Sie auf der Registerkarte **Grid Federation** das Optionsfeld für die Verbindung aus.
- d. Wählen Sie **Berechtigung entfernen**.

3. Überprüfen Sie die Warnungen im Bestätigungsdiaologfeld, und wählen Sie **Entfernen**.
 - Wenn die Berechtigung entfernt werden kann, kehren Sie zur Detailseite zurück, und eine Erfolgsmeldung wird angezeigt. Dieser Mandant kann die Grid Federation-Verbindung nicht mehr verwenden.
 - Wenn für einen oder mehrere Mandanten-Buckets die Grid-übergreifende Replizierung weiterhin aktiviert ist, wird ein Fehler angezeigt.

Remove permission to use grid federation connection ✕

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

 Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

 Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel Force remove Remove

Sie können eine der folgenden Aktionen ausführen:

- (Empfohlen.) Melden Sie sich beim Tenant Manager an und deaktivieren Sie die Replikation für jeden Buckets des Mandanten. Siehe "[Grid-übergreifende Replizierung managen](#)". Wiederholen Sie dann die Schritte, um die Berechtigung **Grid-Verbindung verwenden** zu entfernen.
 - Entfernen Sie die Berechtigung mit Gewalt. Siehe nächster Abschnitt.
4. Gehen Sie zum anderen Raster, und wiederholen Sie diese Schritte, um die Berechtigung für denselben Mandanten auf dem anderen Raster zu entfernen.

Entfernen Sie die Berechtigung mit Gewalt

Bei Bedarf können Sie das Entfernen der Berechtigung eines Mandanten zur Verwendung einer Grid-Verbundverbindung erzwingen, selbst wenn für Mandanten-Buckets die Grid-übergreifende Replizierung aktiviert ist.

Bevor Sie die Erlaubnis eines Mandanten gewaltsam entfernen, beachten Sie die allgemeinen Überlegungen für [Entfernen der Berechtigung](#) sowie folgende weitere Überlegungen anzustellen:

- Wenn Sie die Berechtigung **use Grid Federation connection** per Force entfernen, werden alle Objekte, die eine Replikation auf das andere Grid ausstehen (aufgenommen, aber noch nicht repliziert), weiterhin

repliziert. Um zu verhindern, dass diese in-Process-Objekte den Ziel-Bucket erreichen, müssen Sie auch die Berechtigung des Mandanten für das andere Raster entfernen.

- Alle Objekte, die in den Quell-Bucket aufgenommen wurden, nachdem Sie die Berechtigung **Grid Federation Connection** verwenden entfernt haben, werden niemals in den Ziel-Bucket repliziert.

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **CONFIGURATION > System > Grid Federation**.
3. Wählen Sie den Verbindungsnamen aus, um die Detailseite anzuzeigen.
4. Wählen Sie auf der Registerkarte **zulässige Mieter** die Optionsschaltfläche für den Mieter aus.
5. Wählen Sie **Berechtigung entfernen**.
6. Überprüfen Sie die Warnungen im Bestätigungsdialogfeld, und wählen Sie **Entfernen erzwingen**.

Eine Erfolgsmeldung wird angezeigt. Dieser Mandant kann die Grid Federation-Verbindung nicht mehr verwenden.

7. Gehen Sie bei Bedarf zum anderen Raster, und wiederholen Sie diese Schritte, um die Berechtigung für das gleiche Mandantenkonto im anderen Raster zu erzwingen. Sie sollten diese Schritte beispielsweise auf dem anderen Raster wiederholen, um zu verhindern, dass in-Process-Objekte den Ziel-Bucket erreichen.

Fehler beim Grid-Verbund beheben

Unter Umständen müssen Sie Warnmeldungen und Fehler in Bezug auf Grid-Verbindungen, Account-Klone und Grid-Replizierung beheben.

Warnungen und Fehler der Grid Federation-Verbindung

Möglicherweise erhalten Sie Warnmeldungen oder Fehler bei den Verbindungen des Grid-Verbunds.

Nachdem Sie Änderungen vorgenommen haben, um ein Verbindungsproblem zu beheben, testen Sie die Verbindung, um sicherzustellen, dass der Verbindungsstatus wieder auf **Connected** zurückkehrt. Anweisungen hierzu finden Sie unter "[Grid-Verbindungen verwalten](#)".

Warnmeldung bei Ausfall der Grid-Verbindung

Problem

Die Warnung **Grid Federation Connection failure** wurde ausgelöst.

Details

Diese Warnung zeigt an, dass die Verbindung zwischen den Rastern nicht funktioniert.

Empfohlene Maßnahmen

1. Überprüfen Sie die Einstellungen auf der Seite „Grid Federation“ für beide Raster. Vergewissern Sie sich, dass alle Werte korrekt sind. Siehe "[Grid-Verbindungen verwalten](#)".
2. Überprüfen Sie die für die Verbindung verwendeten Zertifikate. Stellen Sie sicher, dass keine Warnungen für abgelaufene Grid Federation-Zertifikate vorhanden sind und dass die Details für jedes Zertifikat gültig sind. Weitere Informationen finden Sie in den Anweisungen für rotierende Verbindungszertifikate unter "[Grid-Verbindungen verwalten](#)".
3. Vergewissern Sie sich, dass alle Admin- und Gateway-Nodes in beiden Grids online und verfügbar sind. Beheben Sie alle Warnmeldungen, die sich auf diese Knoten auswirken könnten, und versuchen Sie es

erneut.

4. Wenn Sie einen vollständig qualifizierten Domännennamen (FQDN) für das lokale oder Remote-Grid angegeben haben, vergewissern Sie sich, dass der DNS-Server online und verfügbar ist. Siehe "[Was ist Grid Federation?](#)" Für Netzwerk-, IP-Adresse- und DNS-Anforderungen.

Ablauf der Warnmeldung für das Grid-Verbundzertifikat

Problem

Die Warnung **Ablauf des Grid Federation Certificate** wurde ausgelöst.

Details

Diese Warnmeldung gibt an, dass ein oder mehrere Grid-Verbundzertifikate bald ablaufen.

Empfohlene Maßnahmen

Weitere Informationen finden Sie in den Anweisungen für rotierende Verbindungszertifikate unter "[Grid-Verbindungen verwalten](#)".

Fehler beim Bearbeiten einer Verbindung zum Grid Federation

Problem

Beim Bearbeiten einer Grid Federation-Verbindung wird die folgende Warnmeldung angezeigt, wenn Sie **Speichern und Testen** auswählen: "Es konnte keine Kandidatenkonfigurationsdatei auf einem oder mehreren Knoten erstellt werden."

Details

Wenn Sie eine Grid-Federation-Verbindung bearbeiten, versucht StorageGRID, eine Datei mit der Kandidatenkonfiguration auf allen Admin-Knoten im ersten Grid zu speichern. Eine Warnmeldung wird angezeigt, wenn diese Datei nicht in allen Admin-Knoten gespeichert werden kann, z. B. weil ein Admin-Knoten offline ist.

Empfohlene Maßnahmen

1. Wählen Sie aus dem Raster, mit dem Sie die Verbindung bearbeiten, **KNOTEN** aus.
2. Vergewissern Sie sich, dass alle Admin-Nodes für dieses Grid online sind.
3. Wenn Knoten offline sind, schalten Sie sie wieder online und versuchen Sie erneut, die Verbindung zu bearbeiten.

Fehler beim Klonen des Kontos

Keine Anmeldung bei einem geklonten Mandantenkonto möglich

Problem

Sie können sich nicht bei einem geklonten Mandantenkonto anmelden. Die Fehlermeldung auf der Anmeldeseite von Tenant Manager lautet „Ihre Anmeldedaten für dieses Konto waren ungültig. Bitte versuchen Sie es erneut.“

Details

Wenn ein Mandantenkonto aus dem Quellraster des Mandanten im Zielraster des Mandanten geklont wird, wird aus Sicherheitsgründen das Passwort, das Sie für den lokalen Stammbenutzer des Mandanten festgelegt haben, nicht geklont. Wenn ein Mandant lokale Benutzer in seinem Quellraster erstellt, werden die lokalen Benutzerpasswörter nicht im Zielraster geklont.

Empfohlene Maßnahmen

Bevor sich der Root-Benutzer im Zielraster des Mandanten anmelden kann, muss zunächst ein Grid-Administrator angemeldet werden "[Ändern Sie das Passwort für den lokalen Root-Benutzer](#)" Im Zielraster.

Bevor ein geklonter lokaler Benutzer sich im Zielraster des Mandanten anmelden kann, muss der Root-Benutzer für den geklonten Mandanten ein Passwort für den Benutzer im Zielraster hinzufügen. Anweisungen hierzu finden Sie unter "[Managen Sie lokale Benutzer](#)" In der Anleitung zur Verwendung des Tenant Managers.

Mandant wird ohne Klon erstellt

Problem

Sie sehen die Meldung "Tenant created without a Clone", nachdem Sie einen neuen Tenant mit der Berechtigung **use Grid Federation connection** erstellt haben.

Details

Dieses Problem kann auftreten, wenn Aktualisierungen des Verbindungsstatus verzögert werden, was dazu führen kann, dass eine fehlerhafte Verbindung als **verbunden** aufgeführt wird.

Empfohlene Maßnahmen

1. Überprüfen Sie den in der Fehlermeldung aufgeführten Grund, und beheben Sie alle Netzwerk- oder anderen Probleme, die möglicherweise die Funktion der Verbindung verhindern. Siehe [Warnmeldungen und Fehler bei der Grid-Verbundverbindung](#).
2. Befolgen Sie die Anweisungen, um eine Netzverbundverbindung in zu testen "[Grid-Verbindungen verwalten](#)" Um zu bestätigen, dass das Problem behoben wurde.
3. Wählen Sie im Quellraster des Mandanten **TENANTS** aus.
4. Suchen Sie das Mandantenkonto, das nicht geklont werden konnte.
5. Wählen Sie den Namen der Serviceeinheit aus, um die Detailseite anzuzeigen.
6. Wählen Sie **Kontoklone wiederholen**.

The screenshot shows the 'Tenants > test' page in the Tenant Manager. The tenant details are as follows:

Tenant ID:	0040 2213 8117 4859 6503	Quota utilization:	—
Protocol:	S3	Logical space used:	0 bytes
Object count:	0	Quota:	—

Below the details are buttons for 'Sign in', 'Edit', and 'Actions'. A red error message is displayed at the bottom:

× Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

A 'Retry account clone' button is located below the error message.

Wenn der Fehler behoben wurde, wird das Mandantenkonto jetzt in das andere Raster geklont.

Letzter Fehler für Verbindung oder Mandant

Problem

Wenn "[Anzeigen einer Netzverbundverbindung](#)" (Oder wenn "[Verwalten der zulässigen Mandanten](#)" Für eine Verbindung), bemerken Sie einen Fehler in der Spalte **Last error** auf der Seite mit den Verbindungsdetails. Beispiel:

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64
Port: 23000
Remote hostname (other grid): 10.96.130.76
Connection status: ✔ Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

Permitted tenants [Certificates](#)

[Remove permission](#) [Clear error](#) Displaying one result

Tenant name	Last error
<input type="radio"/> Tenant A	<p>2022-12-22 16:19:20 MST</p> <p>Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 13916508109026943924)</p> <p>Check for errors</p>

Details

Für jede Grid Federation-Verbindung zeigt die Spalte **Last error** den zuletzt auftretenden Fehler an, falls vorhanden, wenn die Daten eines Mandanten in das andere Grid repliziert wurden. In dieser Spalte wird nur der letzte gitterübergreifende Replikationsfehler angezeigt. Frühere Fehler, die möglicherweise aufgetreten sind, werden nicht angezeigt. Ein Fehler in dieser Spalte kann aus einem der folgenden Gründe auftreten:

- Die Version des Quellobjekts wurde nicht gefunden.
- Der Quell-Bucket wurde nicht gefunden.
- Der Ziel-Bucket wurde gelöscht.
- Der Ziel-Bucket wurde von einem anderen Konto neu erstellt.
- Im Ziel-Bucket ist die Versionierung angehalten.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist aber jetzt nicht mehr versioniert.

Empfohlene Maßnahmen

Wenn in der Spalte **Last error** eine Fehlermeldung angezeigt wird, gehen Sie wie folgt vor:

1. Überprüfen Sie den Nachrichtentext.
2. Führen Sie alle empfohlenen Aktionen aus. Wenn beispielsweise die Versionierung auf dem Ziel-Bucket für die Grid-übergreifende Replizierung angehalten wurde, aktivieren Sie die Versionierung für diesen Bucket neu.
3. Wählen Sie das Verbindungs- oder Mandantenkonto aus der Tabelle aus.
4. Wählen Sie **Fehler löschen**.
5. Wählen Sie **Ja**, um die Meldung zu löschen und den Systemstatus zu aktualisieren.
6. Warten Sie 5-6 Minuten, und nehmen Sie dann ein neues Objekt in den Bucket auf. Bestätigen Sie, dass die Fehlermeldung nicht erneut angezeigt wird.



Um sicherzustellen, dass die Fehlermeldung gelöscht wird, warten Sie mindestens 5 Minuten nach dem Zeitstempel in der Nachricht, bevor Sie ein neues Objekt aufnehmen.



Nachdem Sie den Fehler gelöscht haben, kann ein neuer **Last error** auftreten, wenn Objekte in einem anderen Bucket aufgenommen werden, der ebenfalls einen Fehler hat.

7. Informationen zum Bestimmen, ob Objekte aufgrund des Bucket-Fehlers nicht repliziert werden konnten, finden Sie unter "[Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut](#)".

Grid-übergreifende Replizierung mit permanenter Fehlerwarnung

Problem

Die Warnung **Cross-Grid Replikation Permanent Failure** wurde ausgelöst.

Details

Diese Warnmeldung weist darauf hin, dass Tenant-Objekte aus einem Grund, der vom Benutzer behoben werden muss, nicht zwischen den Buckets auf zwei Grids repliziert werden können. Diese Warnmeldung wird in der Regel durch eine Änderung an der Quelle oder dem Ziel-Bucket verursacht.

Empfohlene Maßnahmen

1. Melden Sie sich am Raster an, in dem die Warnmeldung ausgelöst wurde.
2. Gehen Sie zu **CONFIGURATION > System > Grid Federation**, und suchen Sie den in der Warnung aufgeführten Verbindungsnamen.
3. Sehen Sie auf der Registerkarte zulässige Mieter in der Spalte **Letzter Fehler** nach, um zu bestimmen, welche Mandantenkonten Fehler aufweisen.
4. Weitere Informationen zum Fehler finden Sie in den Anweisungen unter "[Überwachen von Netzverbundverbindungen](#)" Um die Grid-übergreifenden Replizierungsmetriken zu überprüfen.
5. Für jedes betroffene Mandantenkonto:
 - a. Siehe die Anweisungen unter "[Überwachen Sie die Mandantenaktivität](#)" Um zu bestätigen, dass der Mandant sein Kontingent im Zielraster für die Grid-übergreifende Replikation nicht überschritten hat.
 - b. Erhöhen Sie bei Bedarf das Kontingent des Mandanten im Zielraster, damit neue Objekte gespeichert werden können.
6. Melden Sie sich für jeden betroffenen Mandanten in beiden Grids bei Tenant Manager an, damit Sie die Liste der Buckets vergleichen können.
7. Bestätigen Sie für jeden Bucket, für den die Grid-übergreifende Replizierung aktiviert ist:
 - Es gibt einen entsprechenden Bucket für denselben Mandanten auf dem anderen Grid (muss den

genauen Namen verwenden).

- Beide Buckets haben die Objektversionierung aktiviert (die Versionierung kann in keinem Grid ausgesetzt werden).
- Bei beiden Buckets ist die S3-Objektsperre deaktiviert.
- Keiner der Buckets befindet sich im Status **delete objects: Read-only**.

8. Um zu bestätigen, dass das Problem behoben wurde, lesen Sie die Anweisungen unter "[Überwachen von Netzverbundverbindungen](#)". So überprüfen Sie die Grid-übergreifenden Replikationsmetriken oder führen folgende Schritte aus:

- a. Kehren Sie zur Seite „Grid Federation“ zurück.
- b. Wählen Sie den betroffenen Mandanten aus, und wählen Sie in der Spalte **Letzter Fehler** die Option **Fehler löschen** aus.
- c. Wählen Sie **Ja**, um die Meldung zu löschen und den Systemstatus zu aktualisieren.
- d. Warten Sie 5-6 Minuten, und nehmen Sie dann ein neues Objekt in den Bucket auf. Bestätigen Sie, dass die Fehlermeldung nicht erneut angezeigt wird.



Um sicherzustellen, dass die Fehlermeldung gelöscht wird, warten Sie mindestens 5 Minuten nach dem Zeitstempel in der Nachricht, bevor Sie ein neues Objekt aufnehmen.



Es kann bis zu einem Tag dauern, bis die Warnmeldung gelöscht wird, nachdem sie behoben wurde.

- a. Gehen Sie zu "[Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut](#)". Um Objekte zu identifizieren oder Marker zu löschen, die nicht in das andere Grid repliziert wurden, und die Replikation bei Bedarf erneut zu versuchen.

Warnung: Grid-übergreifende Replikationsressource nicht verfügbar

Problem

Die Warnung **Grid-übergreifende Replikationsressource nicht verfügbar** wurde ausgelöst.

Details

Diese Warnmeldung weist darauf hin, dass Grid-übergreifende Replikationsanforderungen ausstehen, da eine Ressource nicht verfügbar ist. Es kann beispielsweise ein Netzwerkfehler auftreten.

Empfohlene Maßnahmen

1. Überwachen Sie die Warnmeldung, um zu prüfen, ob das Problem eigenständig gelöst wird.
2. Wenn das Problem weiterhin besteht, prüfen Sie, ob eines der Grid-Netze eine Warnmeldung für die Verbindung **Grid Federation Connection failure** für die gleiche Verbindung oder eine Warnung für einen Knoten **Unable to communicate with Node** hat. Diese Warnmeldung wird möglicherweise behoben, wenn Sie diese Warnungen beheben.
3. Weitere Informationen zum Fehler finden Sie in den Anweisungen unter "[Überwachen von Netzverbundverbindungen](#)". Um die Grid-übergreifenden Replizierungsmetriken zu überprüfen.
4. Wenn Sie die Warnmeldung nicht beheben können, wenden Sie sich an den technischen Support.

Die Grid-übergreifende Replizierung wird wie gewohnt ausgeführt, nachdem das Problem behoben wurde.

Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut

Nach dem Beheben der Warnung * Cross-Grid Replikation Permanent Failure* sollten Sie feststellen, ob Objekte oder Löschmarkierungen nicht in das andere Raster repliziert werden konnten. Sie können diese Objekte dann wieder aufnehmen oder die Grid Management API verwenden, um die Replikation erneut zu versuchen.

Die Warnung **Grid-übergreifende Replikation Permanent Failure** weist darauf hin, dass Tenant Objects nicht zwischen den Buckets auf zwei Grids repliziert werden können, aus einem Grund, der vom Benutzer behoben werden muss. Diese Warnmeldung wird in der Regel durch eine Änderung an der Quelle oder dem Ziel-Bucket verursacht. Weitere Informationen finden Sie unter "[Fehler beim Grid-Verbund beheben](#)".

Ermitteln Sie, ob Objekte nicht repliziert werden konnten

Um festzustellen, ob Objekte oder Löschmarkierungen nicht in das andere Raster repliziert wurden, können Sie das Überwachungsprotokoll nach durchsuchen "[CGRR \(Grid-übergreifende Replikationsanforderung\)](#)" Nachrichten. Diese Meldung wird dem Protokoll hinzugefügt, wenn StorageGRID ein Objekt, ein mehrteiliges Objekt oder eine Löschmarkierung nicht in den Ziel-Bucket repliziert.

Sie können das verwenden "[Audit-Explain-Tool](#)" Die Ergebnisse in ein leserliches Format zu übersetzen.

Bevor Sie beginnen

- Sie haben Root-Zugriffsberechtigung.
- Sie haben die `Passwords.txt` Datei:
- Sie kennen die IP-Adresse des primären Admin-Knotens.

Schritte

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Durchsuchen Sie `audit.log` nach CGRR-Meldungen, und formatieren Sie die Ergebnisse mit dem Audit-Explain-Tool.

Dieser Befehl gibt beispielsweise für alle CGRR-Meldungen in den letzten 30 Minuten eine abrüfungsfunktion ein und verwendet das Audit-Explain-Tool.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
```

Die Ergebnisse des Befehls sehen wie in diesem Beispiel aus, das Einträge für sechs CGRR-Meldungen enthält. In diesem Beispiel gaben alle Grid-übergreifenden Replikationsanforderungen einen allgemeinen Fehler zurück, da das Objekt nicht repliziert werden konnte. Die ersten drei Fehler gelten für die Vorgänge „Objekt replizieren“, und die letzten drei Fehler gelten für die Vorgänge „Markierung zum Löschen von Replikationen“.

```

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error

```

Jeder Eintrag enthält folgende Informationen:

Feld	Beschreibung
CGRR-Anforderung für Grid-übergreifende Replikation	Der Name der Anforderung
Mandant	Die Konto-ID des Mandanten
Verbindung	Die ID der Netzverbundverbindung
Betrieb	Der Typ des zu versuchenden Replikationsvorgangs: <ul style="list-style-type: none"> • Objekt replizieren • Löschmarkierung replizieren • Mehrteiliges Objekt replizieren
Eimer	Der Bucket-Name
Objekt	Der Objektname
Version	Die Versions-ID für das Objekt

Feld	Beschreibung
Fehler	Der Fehlertyp. Wenn die Grid-übergreifende Replikation fehlgeschlagen ist, lautet der Fehler „Allgemeiner Fehler“.

Wiederholen Sie fehlgeschlagene Replikationen

Nach dem Generieren einer Liste von Objekten und Löschen von Markierungen, die nicht in den Ziel-Bucket repliziert wurden, und dem Beheben der zugrunde liegenden Probleme können Sie die Replikation auf zwei Arten wiederholen:

- Nehmen Sie jedes Objekt erneut in den Quell-Bucket auf.
- Verwenden Sie die private Grid Management-API, wie beschrieben.

Schritte

1. Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
2. Wählen Sie **Gehe zu privater API-Dokumentation**.



Die mit „Privat“ gekennzeichneten StorageGRID API-Endpunkte können ohne Vorankündigung geändert werden. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

3. Wählen Sie im Abschnitt **Cross-Grid-Replication-Advanced** den folgenden Endpunkt aus:

```
POST /private/cross-grid-replication-retry-failed
```

4. Wählen Sie **Probieren Sie es aus**.
5. Ersetzen Sie im Textfeld **body** den Beispielintrag für **versionID** durch eine Versions-ID aus der audit.log, die einer fehlgeschlagenen Cross-Grid-Replikations-Anforderung entspricht.

Achten Sie darauf, dass die doppelten Anführungszeichen um die Zeichenfolge herum beibehalten werden.

6. Wählen Sie **Ausführen**.
7. Bestätigen Sie, dass der Server-Antwortcode **204** lautet. Dies bedeutet, dass das Objekt oder die Löschmarkierung als ausstehend für die Grid-übergreifende Replikation auf das andere Raster markiert wurde.



Ausstehend bedeutet, dass die Grid-übergreifende Replikationsanforderung zur Verarbeitung der internen Warteschlange hinzugefügt wurde.

Überwachen Sie Wiederholungen der Replikation

Sie sollten die Wiederholungen der Replikation überwachen, um sicherzustellen, dass sie abgeschlossen sind.



Es kann mehrere Stunden oder länger dauern, bis ein Objekt oder eine Löschmarkierung in das andere Raster repliziert wird.

Sie haben zwei Möglichkeiten, Wiederholungsoperationen zu überwachen:

- Verwenden Sie ein S3 ["HEAD Objekt"](#) Oder ["GET Objekt"](#) Anfrage. Die Antwort bezieht sich auf das StorageGRID-spezifische `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	<ul style="list-style-type: none"> • SUCCESS: Die Replikation war erfolgreich. • AUSSTEHEND: Das Objekt wurde noch nicht repliziert. • FAILURE: Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.
Ziel	REPLIKAT: Das Objekt wurde aus dem Quellraster repliziert.

- Verwenden Sie die private Grid Management-API, wie beschrieben.

Schritte

1. Wählen Sie im Abschnitt **Cross-Grid-Replication-Advanced** der privaten API-Dokumentation den folgenden Endpunkt aus:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Wählen Sie **Probieren Sie es aus.**
3. Geben Sie im Abschnitt Parameter die Versions-ID ein, die Sie in verwendet haben `cross-grid-replication-retry-failed` Anfrage.
4. Wählen Sie **Ausführen.**
5. Bestätigen Sie, dass der Server-Antwortcode **200** lautet.
6. Überprüfen Sie den Replikationsstatus. Dieser wird folgendermaßen lauten:
 - **AUSSTEHEND:** Das Objekt wurde noch nicht repliziert.
 - **ABGESCHLOSSEN:** Die Replikation war erfolgreich.
 - **FAILED:** Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.

Sicherheitsmanagement

Sicherheit managen: Übersicht

Sie können verschiedene Sicherheitseinstellungen über den Grid-Manager konfigurieren, um das StorageGRID-System zu sichern.

Verschlüsselung managen

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Sollten Sie ["Überprüfen Sie die verfügbaren Verschlüsselungsmethoden"](#) Ermitteln, welche die Anforderungen für die Datensicherung erfüllen

Verwalten von Zertifikaten

Das können Sie ["Konfigurieren und verwalten Sie die Serverzertifikate"](#) Wird für HTTP-Verbindungen oder die Clientzertifikate verwendet, mit denen eine Client- oder Benutzeridentität beim Server authentifiziert wird.

Konfigurieren von Verschlüsselungsmanagement-Servern

Mit einem "[Verschlüsselungsmanagement-Server](#)" Damit können Sie StorageGRID Daten selbst dann sichern, wenn eine Appliance aus dem Datacenter entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.



Um die Verschlüsselungsschlüsselverwaltung zu verwenden, müssen Sie während der Installation die Einstellung **Node Encryption** für jedes Gerät aktivieren, bevor das Gerät zum Grid hinzugefügt wird.

Proxy-Einstellungen verwalten

Wenn Sie S3-Platfomservices oder Cloud Storage Pools verwenden, können Sie ein konfigurieren "[Storage-Proxyserver](#)" Zwischen Storage-Nodes und den externen S3 -Endpunkten. Wenn Sie AutoSupport Meldungen mit HTTPS oder HTTP senden, können Sie ein konfigurieren "[Admin-Proxyserver](#)" Zwischen Admin-Knoten und technischem Support.

Kontrollieren Sie Firewalls

Um die Sicherheit Ihres Systems zu erhöhen, können Sie den Zugriff auf StorageGRID-Administratorknoten steuern, indem Sie bestimmte Ports am öffnen oder schließen "[Externe Firewall](#)". Sie können auch den Netzwerkzugriff auf jeden Node steuern, indem Sie dessen konfigurieren "[Interne Firewall](#)". Sie können den Zugriff auf alle Ports außer den für Ihre Bereitstellung benötigten verhindern.

Prüfen Sie die StorageGRID Verschlüsselungsmethoden

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Anhand der verfügbaren Methoden können Sie ermitteln, welche Methoden Ihre Datensicherungsanforderungen erfüllen.

Die Tabelle bietet eine allgemeine Zusammenfassung der in StorageGRID verfügbaren Verschlüsselungsmethoden.

Verschlüsselungsoption	So funktioniert es	Gilt für
Verschlüsselungsmanagement-Server (KMS) in Grid Manager	Du " Konfigurieren eines Verschlüsselungsmanagement-Servers " Auf der StorageGRID-Website und " Aktivieren Sie die Node-Verschlüsselung für die Appliance ". Anschließend stellt ein Appliance-Node eine Verbindung mit dem KMS her, um einen Schlüsselverschlüsselungsschlüssel (KEK) anzufordern. Dieser Schlüssel verschlüsselt und entschlüsselt den Datenverschlüsselungsschlüssel (DEK) auf jedem Volume.	Appliance-Knoten, deren Node Encryption während der Installation aktiviert ist. Alle Daten auf der Appliance sind gegen physischen Verlust oder aus dem Datacenter geschützt. Das Management von Verschlüsselungen mit einem KMS wird nur für Storage Nodes und Service-Appliances unterstützt.

Verschlüsselungsoption	So funktioniert es	Gilt für
Laufwerkssicherheit in SANtricity System Manager	Wenn die Laufwerkssicherheitsfunktion für eine SG5700- oder SG6000-Speicheranwendung aktiviert ist, können Sie diese verwenden "SANtricity System Manager" So erstellen und verwalten Sie den Sicherheitsschlüssel. Der Schlüssel ist erforderlich, um auf die Daten auf den gesicherten Laufwerken zuzugreifen.	Storage-Appliances mit Full Disk Encryption (FDE)-Laufwerken oder FIPS-Laufwerken. Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Kann nicht mit Storage Appliances oder Service-Appliances verwendet werden.
Verschlüsselung gespeicherter Objekte	Sie aktivieren die "Verschlüsselung gespeicherter Objekte" Im Grid-Manager. Wenn diese Option aktiviert ist, werden alle neuen Objekte, die nicht auf Bucket-Ebene oder Objektebene verschlüsselt sind, bei der Aufnahme verschlüsselt.	Neu aufgenommene S3- und Swift-Objektdaten Vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.
S3-Bucket-Verschlüsselung	Sie stellen eine PUT-Bucket-Verschlüsselungsanforderung bereit, um die Verschlüsselung für den Bucket zu aktivieren. Alle neuen Objekte, die nicht auf Objektebene verschlüsselt werden, werden bei der Aufnahme verschlüsselt.	Nur neu aufgenommene S3-Objektdaten Für den Bucket muss eine Verschlüsselung angegeben werden. Vorhandene Bucket-Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. "Operationen auf Buckets"
S3-Objektserverseitige Verschlüsselung (SSE)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und schließen das ein <code>x-amz-server-side-encryption</code> Kopfzeile der Anfrage.	Nur neu aufgenommene S3-Objektdaten Für das Objekt muss eine Verschlüsselung angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. StorageGRID verwaltet die Schlüssel. "Serverseitige Verschlüsselung"

Verschlüsselungsoption	So funktioniert es	Gilt für
<p>S3 Objektserverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)</p>	<p>Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und enthalten drei Anfrageheader.</p> <ul style="list-style-type: none"> • x-amz-server-side-encryption-customer-algorithm • x-amz-server-side-encryption-customer-key • x-amz-server-side-encryption-customer-key-MD5 	<p>Nur neu aufgenommene S3-Objektdaten</p> <p>Für das Objekt muss eine Verschlüsselung angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.</p> <p>Schlüssel werden außerhalb von StorageGRID gemanagt.</p> <p>"Serverseitige Verschlüsselung"</p>
<p>Externe Volume- oder Datastore-Verschlüsselung</p>	<p>Sofern die Implementierungsplattform sie unterstützt, verwenden Sie eine Verschlüsselungsmethode außerhalb von StorageGRID, um ein gesamtes Volume oder Datastore zu verschlüsseln.</p>	<p>Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, wobei jedes Volume oder jeder Datastore verschlüsselt ist</p> <p>Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.</p>
<p>Objektverschlüsselung außerhalb von StorageGRID</p>	<p>Dabei kommt eine Verschlüsselungsmethode außerhalb von StorageGRID zum Einsatz, um Objektdaten und Metadaten zu verschlüsseln, bevor sie in StorageGRID aufgenommen werden.</p>	<p>Nur Objektdaten und Metadaten (Systemkonfigurationsdaten sind nicht verschlüsselt).</p> <p>Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.</p> <p>"Amazon Simple Storage Service – Developer Guide: Schutz von Daten mit Client-seitiger Verschlüsselung"</p>

Verwendung mehrerer Verschlüsselungsmethoden

Je nach Ihren Anforderungen können Sie mehrere Verschlüsselungsmethoden gleichzeitig verwenden.
Beispiel:

- Mit einem KMS können Appliance-Nodes geschützt werden. Außerdem kann mithilfe der

Laufwerks sicherheitsfunktion in SANtricity System Manager die Daten „double verschlüsselte“ auf den Self-Encrypting Drives in denselben Appliances verschlüsselt werden.

- Sie können ein KMS verwenden, um Daten auf Appliance-Nodes zu sichern, und die Option gespeicherte Objektverschlüsselung verwenden, um alle Objekte bei der Aufnahme zu verschlüsseln.

Wenn nur ein kleiner Teil Ihrer Objekte eine Verschlüsselung erfordern, sollten Sie stattdessen die Verschlüsselung auf Bucket- oder Objektebene kontrollieren. Durch die Aktivierung diverser Verschlüsselungsstufen entstehen zusätzliche Performance-Kosten.

Verwalten von Zertifikaten

Sicherheitszertifikate verwalten: Übersicht

Sicherheitszertifikate sind kleine Datendateien, die zur Erstellung sicherer, vertrauenswürdiger Verbindungen zwischen StorageGRID-Komponenten und zwischen StorageGRID-Komponenten und externen Systemen verwendet werden.

StorageGRID verwendet zwei Arten von Sicherheitszertifikaten:

- **Serverzertifikate** sind erforderlich, wenn Sie HTTPS-Verbindungen verwenden. Serverzertifikate werden verwendet, um sichere Verbindungen zwischen Clients und Servern herzustellen, die Identität eines Servers bei seinen Clients zu authentifizieren und einen sicheren Kommunikationspfad für Daten bereitzustellen. Der Server und der Client verfügen jeweils über eine Kopie des Zertifikats.
- **Clientzertifikate** authentifizieren eine Client- oder Benutzeridentität auf dem Server und bieten eine sicherere Authentifizierung als Passwörter allein. Clientzertifikate verschlüsseln keine Daten.

Wenn ein Client über HTTPS eine Verbindung zum Server herstellt, antwortet der Server mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält. Der Client überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit dem Server, der denselben öffentlichen Schlüssel verwendet.

StorageGRID-Funktionen wie der Server für einige Verbindungen (z. B. den Endpunkt des Load Balancer) oder als Client für andere Verbindungen (z. B. den CloudMirror-Replikationsdienst).

Standard Grid CA-Zertifikat

StorageGRID enthält eine integrierte Zertifizierungsstelle (CA), die während der Systeminstallation ein internes Grid CA-Zertifikat generiert. Das Grid-CA-Zertifikat wird standardmäßig zum Schutz des internen StorageGRID-Datenverkehrs verwendet. Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die vollständig den Informationssicherheitsrichtlinien Ihres Unternehmens entsprechen. Sie können das Grid-CA-Zertifikat zwar für eine nicht-Produktionsumgebungen verwenden, jedoch empfiehlt es sich, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert sind. Ungesicherte Verbindungen ohne Zertifikat werden ebenfalls unterstützt, aber nicht empfohlen.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht, jedoch sollten die benutzerdefinierten Zertifikate für die Überprüfung der Serververbindungen angegeben sein.
- Alle benutzerdefinierten Zertifikate müssen den erfüllen "[Richtlinien für die Systemhärtung von Serverzertifikaten](#)".
- StorageGRID unterstützt das Bündeln von Zertifikaten aus einer Zertifizierungsstelle in einer einzelnen Datei (Bundle als CA-Zertifikat).



StorageGRID enthält auch CA-Zertifikate für das Betriebssystem, die in allen Grids identisch sind. Stellen Sie in Produktionsumgebungen sicher, dass Sie ein benutzerdefiniertes Zertifikat angeben, das von einer externen Zertifizierungsstelle anstelle des CA-Zertifikats des Betriebssystems signiert wurde.

Varianten der Server- und Client-Zertifikatstypen werden auf verschiedene Weise implementiert. Vor der Konfiguration des Systems sollten Sie alle erforderlichen Zertifikate für Ihre spezifische StorageGRID-Konfiguration bereithaben.

Greifen Sie auf Sicherheitszertifikate zu

Sie haben Zugriff auf Informationen zu allen StorageGRID-Zertifikaten an einer zentralen Stelle, zusammen mit Links zum Konfigurations-Workflow für jedes Zertifikat.

Schritte

1. Wählen Sie im Grid Manager **CONFIGURATION > Security > Certificates**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global Grid CA Client Load balancer endpoints Tenants Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type	Expiration date
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Wählen Sie auf der Seite Zertifikate eine Registerkarte aus, um Informationen zu den einzelnen Zertifikatkategorien zu erhalten und auf die Zertifikateinstellungen zuzugreifen. Sie können nur auf eine Registerkarte zugreifen, wenn Sie über die entsprechende Berechtigung verfügen.

- **Global:** Sichert den StorageGRID-Zugriff von Webbrowsern und externen API-Clients.
- **Raster CA:** Sichert internen StorageGRID-Datenverkehr.
- **Kunde:** Sichert Verbindungen zwischen externen Clients und der StorageGRID Prometheus Datenbank.
- **Load Balancer-Endpunkte:** Sichert Verbindungen zwischen S3- und Swift-Clients und dem StorageGRID Load Balancer.
- **Mandanten:** Sichert Verbindungen zu Identitäts-Federation-Servern oder von Plattform-Service-Endpunkten zu S3-Storage-Ressourcen.
- **Sonstiges:** Sichert StorageGRID-Verbindungen, die bestimmte Zertifikate erfordern.

Jede Registerkarte wird unten mit Links zu weiteren Zertifikatdetails beschrieben.

Weltweit

Die globalen Zertifikate sichern den StorageGRID-Zugriff über Webbrowser und externe S3 und Swift API-Clients. Zwei globale Zertifikate werden zunächst von der StorageGRID-Zertifizierungsstelle während der Installation generiert. Die beste Vorgehensweise für eine Produktionsumgebung besteht darin, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert wurden.

- **Zertifikat für die Managementoberfläche:** Sichert Client-Web-Browser-Verbindungen zu StorageGRID-Management-Schnittstellen.
- **S3- und Swift-API-Zertifikat:** Sichert Client-API-Verbindungen zu Storage-Nodes, Admin-Nodes und Gateway-Nodes, über die S3- und Swift-Client-Applikationen Objektdaten hochladen und herunterladen.

Informationen zu den installierten globalen Zertifikaten umfassen:

- **Name:** Zertifikatsname mit Link zur Verwaltung des Zertifikats.
- **Beschreibung**
- **Typ:** Benutzerdefiniert oder Standard. + Sie sollten immer ein benutzerdefiniertes Zertifikat verwenden, um die Netzsicherheit zu verbessern.
- **Ablaufdatum:** Bei Verwendung des Standardzertifikats wird kein Ablaufdatum angezeigt.

Ihre Vorteile:

- Ersetzen Sie die Standardzertifikate durch benutzerdefinierte Zertifikate, die von einer externen Zertifizierungsstelle signiert wurden, um eine verbesserte Grid-Sicherheit zu gewährleisten:
 - **"Ersetzen Sie das von StorageGRID generierte Standardzertifikat für die Managementoberfläche"** Wird für Grid Manager- und Tenant Manager-Verbindungen verwendet.
 - **"Das S3- und Swift-API-Zertifikat ersetzen"** Wird für Storage-Node- und Load Balancer-Endpunktverbindungen (optional) verwendet.
- **"Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her."**
- **"Stellen Sie das S3- und Swift-API-Standardzertifikat wieder her."**
- **"Erstellen Sie mit einem Skript ein neues Zertifikat für die selbstsignierte Managementoberfläche."**
- Kopieren Sie die, oder laden Sie sie herunter **"Zertifikat für die Managementoberfläche"** Oder **"S3- und Swift-API-Zertifikat"**.

Grid CA

Der **Grid-CA-Zertifikat**, Von der StorageGRID-Zertifizierungsstelle während der StorageGRID-Installation erzeugt, sichert den gesamten internen StorageGRID-Verkehr.

Zertifikatsinformationen umfassen das Ablaufdatum des Zertifikats und den Zertifikatsinhalt.

Das können Sie **"Kopieren oder laden Sie das Zertifikat der Grid-Zertifizierungsstelle herunter"**, Aber man kann es nicht ändern.

Client

Client-Zertifikate, Generiert von einer externen Zertifizierungsstelle, sichern Sie die Verbindungen zwischen externen Monitoring-Tools und der StorageGRID Prometheus Datenbank.

Die Zertifikatstabelle verfügt über eine Zeile für jedes konfigurierte Clientzertifikat und gibt an, ob das Zertifikat zusammen mit dem Ablaufdatum des Zertifikats für den Zugriff auf die Prometheus-Datenbank

verwendet werden kann.

Ihre Vorteile:

- ["Hochladen oder Generieren eines neuen Clientzertifikats"](#)
- Wählen Sie einen Zertifikatnamen aus, um die Zertifikatdetails anzuzeigen, in denen Sie:
 - ["Ändern Sie den Namen des Client-Zertifikats."](#)
 - ["Legen Sie die Zugriffsberechtigung für Prometheus fest."](#)
 - ["Laden Sie das Clientzertifikat hoch, und ersetzen Sie es."](#)
 - ["Kopieren Sie das Client-Zertifikat, oder laden Sie es herunter."](#)
 - ["Entfernen Sie das Clientzertifikat."](#)
- Wählen Sie **Actions**, um schnell zu reagieren ["Bearbeiten"](#), ["Anhängen"](#), Oder ["Entfernen"](#) Ein Client-Zertifikat. Sie können bis zu 10 Clientzertifikate auswählen und gleichzeitig mit **Actions > Remove** entfernen.

Load Balancer-Endpunkte

[Load Balancer-Endpunktzertifikate](#) Sichern der Verbindungen zwischen S3 und Swift Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes und Admin-Nodes

Die Endpunktstabelle für Load Balancer verfügt über eine Reihe für jeden konfigurierten Load Balancer-Endpunkt und gibt an, ob das globale S3- und Swift-API-Zertifikat oder ein benutzerdefiniertes Load Balancer-Endpoint-Zertifikat für den Endpunkt verwendet wird. Es wird auch das Ablaufdatum für jedes Zertifikat angezeigt.



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Ihre Vorteile:

- ["Anzeigen eines Endpunkts für die Lastverteilung"](#), Einschließlich der Zertifikatdetails.
- ["Geben Sie ein Endpoint-Zertifikat für den Load Balancer für FabricPool an."](#)
- ["Verwenden Sie das globale S3- und Swift-API-Zertifikat"](#) Statt ein neues Load Balancer-Endpoint-Zertifikat zu erstellen.

Mandanten

Die Mandanten nutzen können [Identity Federation Server-Zertifikate](#) Oder [Endpoint-Zertifikate für Plattformservice](#) Um ihre Verbindungen mit StorageGRID zu sichern.

Die Mandantentabelle verfügt über eine Zeile für jeden Mandanten und gibt an, ob jeder Mandant die Berechtigung hat, seine eigenen Identitätsquellen- oder Plattform-Services zu nutzen.

Ihre Vorteile:

- ["Wählen Sie einen Mandantennamen aus, um sich beim Mandanten-Manager anzumelden"](#)
- ["Wählen Sie einen Mandantennamen aus, um Details zur Identitätsföderation des Mandanten anzuzeigen"](#)
- ["Wählen Sie einen Mandantennamen aus, um Details zu den Services der Mandantenplattform anzuzeigen"](#)

- ["Festlegen eines Endpunktzertifikats für den Plattformservice während der Endpunkterstellung"](#)

Andere

StorageGRID verwendet andere Sicherheitszertifikate zu bestimmten Zwecken. Diese Zertifikate werden nach ihrem Funktionsnamen aufgelistet. Weitere Sicherheitszertifikate:

- [Cloud Storage Pool-Zertifikate](#)
- [Benachrichtigungszertifikate per E-Mail senden](#)
- [Externe Syslog-Server-Zertifikate](#)
- [Verbindungszertifikate für Grid Federation](#)
- [Zertifikate für Identitätsföderation](#)
- [KMS-Zertifikate \(Key Management Server\)](#)
- [Einzelanmelde-Zertifikate](#)

Informationen geben den Zertifikattyp an, den eine Funktion verwendet, sowie die Gültigkeitsdaten des Server- und Clientzertifikats. Wenn Sie einen Funktionsnamen auswählen, wird eine Browserregisterkarte geöffnet, auf der Sie die Zertifikatdetails anzeigen und bearbeiten können.



Sie können nur Informationen zu anderen Zertifikaten anzeigen und darauf zugreifen, wenn Sie über die entsprechende Berechtigung verfügen.

Ihre Vorteile:

- ["Festlegen eines Cloud-Storage-Pool-Zertifikats für S3, C2S S3 oder Azure"](#)
- ["Legen Sie ein Zertifikat für Benachrichtigungen per E-Mail fest"](#)
- ["Geben Sie ein externes Syslog-Serverzertifikat an"](#)
- ["Verbindungszertifikate für Netzverbund drehen"](#)
- ["Anzeigen und Bearbeiten eines Zertifikats für die Identitätsföderation"](#)
- ["Laden Sie den KMS-Server \(Key Management Server\) und die Clientzertifikate hoch"](#)
- ["Geben Sie manuell ein SSO-Zertifikat für eine vertrauenswürdige Partei an"](#)

Details zum Sicherheitszertifikat

Jede Art von Sicherheitszertifikat wird unten beschrieben, mit Links zu den Implementierungsanleitungen.

Zertifikat für die Managementoberfläche

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID-Managementoberfläche, sodass Benutzer ohne Sicherheitswarnungen auf Grid-Manager und Mandantenmanager zugreifen können.</p> <p>Dieses Zertifikat authentifiziert auch Grid Management-API- und Mandantenmanagement-API-Verbindungen.</p> <p>Sie können das bei der Installation erstellte Standardzertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.</p>	KONFIGURATION > Sicherheit > Zertifikate , wählen Sie die Registerkarte Global und wählen Sie dann Management Interface Certificate aus	"Konfigurieren Sie Zertifikate für die Managementoberfläche"

S3- und Swift-API-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>Authentifizierung von sicheren S3- oder Swift-Client-Verbindungen zu einem Storage Node und Load Balancer-Endpunkten (optional)</p>	KONFIGURATION > Sicherheit > Zertifikate , wählen Sie die Registerkarte Global und wählen Sie dann S3 und Swift API Zertifikat aus	"Konfigurieren von S3- und Swift-API-Zertifikaten"

Grid-CA-Zertifikat

Siehe [Beschreibung des Standard Grid CA-Zertifikats](#).

Administrator-Client-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Client	<p>Wird auf jedem Client installiert, sodass StorageGRID den externen Client-Zugriff authentifizieren kann.</p> <ul style="list-style-type: none"> • Ermöglicht autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank. • Ermöglicht die sichere Überwachung von StorageGRID mit externen Tools. 	<p>KONFIGURATION > Sicherheit > Zertifikate und dann die Registerkarte Client wählen</p>	<p>"Konfigurieren Sie Client-Zertifikate"</p>

Endpunkt-Zertifikat für Load Balancer

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>Authentifiziert die Verbindung zwischen S3- oder Swift-Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes und Admin-Nodes. Sie können ein Load Balancer-Zertifikat hochladen oder generieren, wenn Sie einen Load Balancer-Endpoint konfigurieren. Client-Applikationen verwenden das Load Balancer-Zertifikat, wenn Sie eine Verbindung zu StorageGRID herstellen, um Objektdaten zu speichern und abzurufen.</p> <p>Sie können auch eine benutzerdefinierte Version des globalen verwenden S3- und Swift-API-Zertifikat Zertifikat zur Authentifizierung von Verbindungen zum Lastverteilungsservice. Wenn das globale Zertifikat zur Authentifizierung von Load Balancer-Verbindungen verwendet wird, müssen Sie kein separates Zertifikat für jeden Load Balancer-Endpoint hochladen oder generieren.</p> <p>Hinweis: das Zertifikat, das für die Load Balancer Authentifizierung verwendet wird, ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID-Betriebs.</p>	KONFIGURATION > Netzwerk > Load Balancer-Endpunkte	<ul style="list-style-type: none"> • "Konfigurieren von Load Balancer-Endpunkten" • "Erstellen eines Load Balancer-Endpunkts für FabricPool"

Endpunkt-Zertifikat für Cloud Storage Pool

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung von einem StorageGRID Cloud Storage Pool auf einem externen Storage-Standort wie S3 Glacier oder Microsoft Azure Blob Storage. Für jeden Cloud-Provider-Typ ist ein anderes Zertifikat erforderlich.	ILM > Speicherpools	"Erstellen Sie einen Cloud-Storage-Pool"

Zertifikat für eine E-Mail-Benachrichtigung

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	<p>Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID, die für Benachrichtigungen verwendet werden.</p> <ul style="list-style-type: none">• Wenn die Kommunikation mit dem SMTP-Server TLS (Transport Layer Security) erfordert, müssen Sie das CA-Zertifikat für den E-Mail-Server angeben.• Geben Sie ein Clientzertifikat nur an, wenn für den SMTP-E-Mail-Server Clientzertifikate zur Authentifizierung erforderlich sind.	ALARME > E-Mail-Einrichtung	"Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"

Externes Syslog-Serverzertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>Authentifiziert die TLS- oder RELP/TLS-Verbindung zwischen einem externen Syslog-Server, der Ereignisse in StorageGRID protokolliert.</p> <p>Hinweis: für TCP-, RELP/TCP- und UDP-Verbindungen zu einem externen Syslog-Server ist kein externes Syslog-Serverzertifikat erforderlich.</p>	<p>KONFIGURATION > Überwachung > Audit- und Syslog-Server und dann externen Syslog-Server konfigurieren wählen</p>	<p>"Konfigurieren Sie einen externen Syslog-Server"</p>

Verbindungszertifikat für Grid Federation

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	<p>Authentifizieren und verschlüsseln Sie Informationen, die zwischen dem aktuellen StorageGRID-System und einem anderen Grid in einer Grid-Verbundverbindung gesendet werden.</p>	<p>KONFIGURATION > System > Grid Federation</p>	<ul style="list-style-type: none"> • "Erstellen von Grid Federation-Verbindungen" • "Verbindungszertifikate drehen"

Zertifikat für Identitätsföderation

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Identitäts-Provider, z. B. Active Directory, OpenLDAP oder Oracle Directory Server. Wird für Identitätsföderation verwendet, durch die Administratoren und Benutzer von einem externen System gemanagt werden können.	KONFIGURATION > Zugangskontrolle > Identitätsverbund	"Verwenden Sie den Identitätsverbund"

KMS-Zertifikat (Key Management Server)

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Verschlüsselungsmanagement-Server (KMS), der Verschlüsselungsschlüssel für die StorageGRID Appliance-Nodes bereitstellt.	KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Endpoint-Zertifikat für Plattform-Services

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung vom StorageGRID Plattform-Service zu einer S3-Storage-Ressource.	Tenant Manager > STORAGE (S3) > Plattform-Services-Endpunkte	"Endpunkt für Plattformservices erstellen" "Endpunkt der Plattfordienste bearbeiten"

SSO-Zertifikat (Single Sign On)

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen Services der Identitätsföderation, z. B. Active Directory Federation Services (AD FS) und StorageGRID, die für SSO-Anforderungen (Single Sign On) verwendet werden.	KONFIGURATION > Zugangskontrolle > Single Sign-On	"Konfigurieren Sie Single Sign-On"

Beispiele für Zertifikate

Beispiel 1: Load Balancer Service

In diesem Beispiel fungiert StorageGRID als Server.

1. Sie konfigurieren einen Load Balancer-Endpunkt und laden ein Serverzertifikat in StorageGRID hoch oder erstellen.
2. Sie konfigurieren eine S3- oder Swift-Client-Verbindung zum Endpunkt des Load Balancer und laden dasselbe Zertifikat auf den Client hoch.
3. Wenn der Client Daten speichern oder abrufen möchte, stellt er über HTTPS eine Verbindung zum Load Balancer-Endpunkt her.
4. StorageGRID antwortet mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält, und mit einer Signatur auf Grundlage des privaten Schlüssels.
5. Der Client überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit demselben öffentlichen Schlüssel.
6. Der Client sendet Objektdaten an StorageGRID.

Beispiel 2: Externer KMS (Key Management Server)

In diesem Beispiel fungiert StorageGRID als Client.

1. Mithilfe der Software für den externen Verschlüsselungsmanagement-Server konfigurieren Sie StorageGRID als KMS-Client und erhalten ein von einer Zertifizierungsstelle signiertes Serverzertifikat, ein öffentliches Clientzertifikat und den privaten Schlüssel für das Clientzertifikat.
2. Mit dem Grid Manager konfigurieren Sie einen KMS-Server und laden die Server- und Client-Zertifikate sowie den privaten Client-Schlüssel hoch.
3. Wenn ein StorageGRID-Node einen Verschlüsselungsschlüssel benötigt, fordert er den KMS-Server an, der Daten des Zertifikats enthält und eine auf dem privaten Schlüssel basierende Signatur.
4. Der KMS-Server validiert die Zertifikatsignatur und entscheidet, dass er StorageGRID vertrauen kann.
5. Der KMS-Server antwortet über die validierte Verbindung.

Konfigurieren Sie Serverzertifikate

Unterstützte Serverzertifikatstypen

Das StorageGRID-System unterstützt benutzerdefinierte Zertifikate, die mit RSA oder ECDSA (Algorithmus für digitale Signaturen der Elliptischen Kurve) verschlüsselt sind.



Der Verschlüsselungstyp für die Sicherheitsrichtlinie muss mit dem Serverzertifikattyp übereinstimmen. RSA-Chiffren erfordern beispielsweise RSA-Zertifikate, und ECDSA-Chiffren erfordern ECDSA-Zertifikate. Siehe "[Verwalten von Sicherheitszertifikaten](#)". Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfigurieren, die nicht mit dem Serverzertifikat kompatibel ist, können Sie dies tun "[Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie](#)".

Weitere Informationen darüber, wie StorageGRID Client-Verbindungen für die REST-API sichert, finden Sie unter "[Sicherheit für S3-REST-API konfigurieren](#)" Oder "[Konfigurieren Sie die Sicherheit für Swift REST API](#)".

Konfigurieren Sie Zertifikate für die Managementoberfläche

Sie können das Standardzertifikat für die Verwaltungsschnittstelle durch ein einzelnes benutzerdefiniertes Zertifikat ersetzen, das Benutzern den Zugriff auf den Grid Manager und den Tenant Manager ermöglicht, ohne dass Sicherheitswarnungen auftreten. Sie können auch das Standard-Zertifikat für die Managementoberfläche zurücksetzen oder ein neues erstellen.

Über diese Aufgabe

Standardmäßig wird jeder Admin-Node ein von der Grid-CA signiertes Zertifikat ausgestellt. Diese CA-signierten Zertifikate können durch ein einziges allgemeines Zertifikat für benutzerdefinierte Verwaltungsschnittstellen und einen entsprechenden privaten Schlüssel ersetzt werden.

Da für alle Admin-Nodes ein einzelnes Zertifikat für eine benutzerdefinierte Managementoberfläche verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multi-Domain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit Grid Manager und Tenant Manager überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Admin-Nodes im Raster übereinstimmt.

Sie müssen die Konfiguration auf dem Server abschließen. Je nach der von Ihnen verwendeten Root Certificate Authority (CA) müssen Benutzer möglicherweise auch das Grid CA-Zertifikat in den Webbrowser installieren, mit dem sie auf den Grid Manager und den Tenant Manager zugreifen können.



Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnmeldung **Ablauf des Serverzertifikats für die Managementoberfläche** ausgelöst, wenn dieses Serverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION > Sicherheit > Zertifikate** auswählen und das Ablaufdatum für das Zertifikat der Verwaltungsschnittstelle auf der Registerkarte Global anzeigen.



Wenn Sie mit einem Domännennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für die benutzerdefinierte Managementoberfläche läuft ab.
- Du [Zurücksetzen von einem Zertifikat der benutzerdefinierten Managementoberfläche auf das Standard-Serverzertifikat](#).

Fügen Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzu

Zum Hinzufügen eines Zertifikats einer benutzerdefinierten Managementoberfläche können Sie Ihr eigenes Zertifikat bereitstellen oder mit dem Grid Manager ein Zertifikat erstellen.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat:** Die benutzerdefinierte Server-Zertifikatdatei (PEM-codiert).
- **Zertifikat privater Schlüssel:** Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (.key).



Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket:** Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

c. Erweitern Sie **Zertifikatdetails**, um die Metadaten für jedes hochgeladene Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere Stelle zu kopieren.

d. Wählen Sie **Speichern**. + das Zertifikat der benutzerdefinierten Managementoberfläche wird für alle nachfolgenden neuen Verbindungen mit Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.



Die beste Vorgehensweise für eine Produktionsumgebung ist die Verwendung eines Zertifikats der benutzerdefinierten Management-Schnittstelle, das von einer externen Zertifizierungsstelle signiert wurde.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.

Feld	Beschreibung
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domännennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. Hinweis: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten für das generierte Zertifikat anzuzeigen.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an.
Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere Stelle zu kopieren.

e. Wählen Sie **Speichern**. + das Zertifikat der benutzerdefinierten Managementoberfläche wird für alle nachfolgenden neuen Verbindungen mit Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.



Nachdem Sie ein Zertifikat hochgeladen oder generiert haben, lassen Sie sich bis zu einem Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

6. Nachdem Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzugefügt haben, werden auf der Seite Zertifikat der Verwaltungsschnittstelle detaillierte Zertifikatsinformationen für die verwendeten Zertifikate angezeigt. + Sie können das PEM-Zertifikat nach Bedarf herunterladen oder kopieren.

Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her

Sie können das Standardzertifikat zur Managementoberfläche für Grid Manager- und Tenant-Manager-Verbindungen wiederherstellen.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie **Standard-Zertifikat verwenden**.

Wenn Sie das Standardzertifikat der Verwaltungsschnittstelle wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Das Standardzertifikat für die Verwaltungsschnittstelle wird für alle nachfolgenden neuen Clientverbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Erstellen Sie mit einem Skript ein neues Zertifikat für die selbstsignierte Managementoberfläche

Wenn eine strikte Host-Validierung erforderlich ist, können Sie das Zertifikat der Managementoberfläche mithilfe eines Skripts generieren.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Die beste Vorgehensweise für eine Produktionsumgebung ist die Verwendung eines Zertifikats, das von einer externen Zertifizierungsstelle signiert wurde.

Schritte

1. Ermitteln Sie den vollständig qualifizierten Domännennamen (FQDN) jedes Admin-Knotens.
2. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Für `--domains`, Verwenden Sie Platzhalter, um die vollständig qualifizierten Domännennamen aller Admin-Knoten darzustellen. Beispiel: `*.ui.storagegrid.example.com` Verwendet den Platzhalter `*` für die Darstellung `admin1.ui.storagegrid.example.com` Und `admin2.ui.storagegrid.example.com`.

- Einstellen `--type` Bis `management` Zum Konfigurieren des Zertifikats der Managementoberfläche, das von Grid Manager und Tenant Manager verwendet wird.
- Die erstellten Zertifikate sind standardmäßig für ein Jahr (365 Tage) gültig und müssen vor Ablauf neu erstellt werden. Sie können das verwenden `--days` Argument zum Überschreiben des standardmäßigen Gültigkeitszeitraums.



Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` Wird ausgeführt. Sie müssen sicherstellen, dass der Management-Client mit der gleichen Datenquelle wie StorageGRID synchronisiert wird. Andernfalls kann der Client das Zertifikat ablehnen.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

Die resultierende Ausgabe enthält das öffentliche Zertifikat, das vom Management-API-Client benötigt wird.

4. Wählen Sie das Zertifikat aus, und kopieren Sie es.

Geben Sie DIE START- und DAS ENDE-Tags in Ihre Auswahl ein.

5. Melden Sie sich von der Eingabeaufforderung-Shell ab. `$ exit`

6. Bestätigen Sie, dass das Zertifikat konfiguriert wurde:

a. Greifen Sie auf den Grid Manager zu.

b. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate**

c. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.

7. Konfigurieren Sie den Management-Client so, dass er das öffentliche Zertifikat verwendet, das Sie kopiert haben. Geben Sie DIE START- und END-Tags an.

Laden Sie das Zertifikat für die Managementoberfläche herunter oder kopieren Sie es

Sie können den Inhalt des Zertifikats der Managementoberfläche speichern oder kopieren, um ihn an einer anderen Stelle zu verwenden.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate**.

2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.

3. Wählen Sie die Registerkarte **Server** oder **CA Bundle** aus und laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

Laden Sie das Zertifikat oder das CA-Paket herunter .pem Datei: Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

- a. Wählen Sie **Zertifikat herunterladen** oder **CA-Paket herunterladen**.

Wenn Sie ein CA-Bundle herunterladen, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets als einzelne Datei heruntergeladen.

- b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen. Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

- a. Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM**.

Wenn Sie ein CA-Bundle kopieren, kopieren alle Zertifikate in den sekundären Registerkarten des CA-Bundles zusammen.

- b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
- c. Speichern Sie die Textdatei mit der Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Konfigurieren von S3- und Swift-API-Zertifikaten

Sie können das Serverzertifikat ersetzen oder wiederherstellen, das für S3- oder Swift-Clientverbindungen zu Storage Nodes oder zu Load Balancer-Endpunkten verwendet wird. Das benutzerdefinierte Ersatzserverzertifikat ist speziell für Ihr Unternehmen bestimmt.

Über diese Aufgabe

Standardmäßig wird jeder Speicherknoten ein X.509-Serverzertifikat ausgestellt, das von der Grid-CA signiert wurde. Diese CA-signierten Zertifikate können durch ein einziges allgemeines benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Für alle Speicherknoten wird ein einzelnes benutzerdefiniertes Serverzertifikat verwendet. Sie müssen daher das Zertifikat als Platzhalter- oder Multidomain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit dem Speicherendpunkt überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat, sodass es mit allen Speicherknoten im Raster übereinstimmt.

Nach Abschluss der Konfiguration auf dem Server müssen Sie möglicherweise auch das Grid CA-Zertifikat im S3- oder Swift-API-Client installieren, über den Sie je nach der von Ihnen verwendeten Root-Zertifizierungsstelle (CA) auf das System zugreifen können.



Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des globalen Serverzertifikats für S3 und Swift API** ausgelöst, wenn das Stammserverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION > Sicherheit > Zertifikate** und das Ablaufdatum für das S3- und Swift-API-Zertifikat auf der Registerkarte Global auswählen.

Sie können ein benutzerdefiniertes S3- und Swift-API-Zertifikat hochladen oder erstellen.

Fügen Sie ein benutzerdefiniertes S3- und Swift-API-Zertifikat hinzu

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat:** Die benutzerdefinierte Server-Zertifikatdatei (PEM-codiert).
- **Zertifikat privater Schlüssel:** Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (.key).



Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket:** Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

c. Wählen Sie die Zertifikatsdetails aus, um die Metadaten und PEM für jedes benutzerdefinierte S3- und Swift-API-Zertifikat anzuzeigen, das hochgeladen wurde. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere Stelle zu kopieren.

d. Wählen Sie **Speichern**.

Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen verwendet.

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.

Feld	Beschreibung
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domännennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. Hinweis: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten und das PEM für das benutzerdefinierte S3- und Swift-API-Zertifikat anzuzeigen, das erstellt wurde.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere Stelle zu kopieren.

e. Wählen Sie **Speichern**.

Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen verwendet.

5. Wählen Sie eine Registerkarte aus, um Metadaten für das Standard-StorageGRID-Serverzertifikat, ein Zertifikat mit einer Zertifizierungsstelle, das hochgeladen wurde, oder ein benutzerdefiniertes Zertifikat anzuzeigen, das erstellt wurde.



Nachdem Sie ein Zertifikat hochgeladen oder generiert haben, lassen Sie sich bis zu einem Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

6. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

7. Nachdem Sie ein benutzerdefiniertes S3- und Swift-API-Zertifikat hinzugefügt haben, zeigt die S3- und Swift-API-Zertifikatsseite detaillierte Zertifikatsinformationen für das verwendete S3- und Swift-API-

Zertifikat an. + Sie können das PEM-Zertifikat nach Bedarf herunterladen oder kopieren.

Stellen Sie das S3- und Swift-API-Standardzertifikat wieder her

Sie können die Wiederherstellung auf die Verwendung des standardmäßigen S3- und Swift-API-Zertifikats für S3- und Swift-Client-Verbindungen zu Storage Nodes durchführen. Sie können jedoch nicht das standardmäßige S3- und Swift-API-Zertifikat für einen Load Balancer-Endpoint verwenden.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie **Standard-Zertifikat verwenden**.

Wenn Sie die Standardversion des globalen S3- und Swift-API-Zertifikats wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Das standardmäßige S3- und Swift-API-Zertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen zu Storage-Nodes verwendet.

4. Wählen Sie **OK**, um die Warnung zu bestätigen und das Standard-S3- und Swift-API-Zertifikat wiederherzustellen.

Wenn Sie über Root-Zugriffsberechtigungen verfügen und das benutzerdefinierte S3- und Swift-API-Zertifikat für Endpoint-Verbindungen für den Load Balancer verwendet wurde, wird eine Liste mit Endpunkten für Load Balancer angezeigt, auf die über das Standard-S3- und Swift-API-Zertifikat nicht mehr zugegriffen werden kann. Gehen Sie zu "[Konfigurieren von Load Balancer-Endpunkten](#)" Zum Bearbeiten oder Entfernen der betroffenen Endpunkte.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Laden Sie das S3- und Swift-API-Zertifikat herunter oder kopieren Sie es

Sie können Inhalte des S3- und Swift-API-Zertifikats zur anderen Verwendung speichern oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie die Registerkarte **Server** oder **CA Bundle** aus und laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

Laden Sie das Zertifikat oder das CA-Paket herunter .pem Datei: Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

- a. Wählen Sie **Zertifikat herunterladen** oder **CA-Paket herunterladen**.

Wenn Sie ein CA-Bundle herunterladen, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets als einzelne Datei heruntergeladen.

- b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen. Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

- a. Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM**.

Wenn Sie ein CA-Bundle kopieren, kopieren alle Zertifikate in den sekundären Registerkarten des CA-Bundles zusammen.

- b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
- c. Speichern Sie die Textdatei mit der Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Verwandte Informationen

- ["S3-REST-API VERWENDEN"](#)
- ["Nutzen Sie die Swift REST API"](#)
- ["Konfigurieren Sie die Domännennamen des S3-Endpunkts"](#)

Kopieren Sie das Grid-CA-Zertifikat

StorageGRID verwendet eine interne Zertifizierungsstelle (Certificate Authority, CA) zum Schutz des internen Datenverkehrs. Dieses Zertifikat ändert sich nicht, wenn Sie Ihre eigenen Zertifikate hochladen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Client-Anwendungen den Server anhand des benutzerdefinierten Serverzertifikats überprüfen. Sie sollten das CA-Zertifikat nicht aus dem StorageGRID-System kopieren.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Raster CA** aus.
2. Laden Sie das Zertifikat im Abschnitt **Zertifikat PEM** herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei herunter

Laden Sie das Zertifikat herunter .pem Datei:

- a. Wählen Sie **Zertifikat herunterladen**.
- b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Zertifikat PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

- a. Wählen Sie **Zertifikat kopieren PEM**.
- b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
- c. Speichern Sie die Textdatei mit der Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie StorageGRID-Zertifikate für FabricPool

Für S3-Clients, die strenge Hostnamen-Validierungen durchführen und die eine strikte Hostname-Validierung nicht unterstützen, z. B. ONTAP-Clients mit FabricPool, können Sie beim Konfigurieren des Load Balancer-Endpunkts ein Serverzertifikat generieren oder hochladen.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

Wenn Sie einen Load Balancer-Endpunkt erstellen, können Sie ein selbstsigniertes Serverzertifikat generieren oder ein Zertifikat hochladen, das von einer bekannten Zertifizierungsstelle signiert ist. In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle signiert ist. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden. Sie sind außerdem sicherer, weil sie einen besseren Schutz vor man-in-the-Middle-Angriffen bieten.

In den folgenden Schritten finden Sie allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Weitere Informationen und Verfahren finden Sie unter "[Konfigurieren Sie StorageGRID für FabricPool](#)".

Schritte

1. Konfigurieren Sie optional eine HA-Gruppe (High Availability, Hochverfügbarkeit) für die Verwendung von FabricPool.

2. Einen S3-Load-Balancer-Endpoint für FabricPool erstellen.

Wenn Sie einen HTTPS-Load-Balancer-Endpoint erstellen, werden Sie aufgefordert, Ihr Serverzertifikat, den privaten Zertifikatschlüssel und das optionale CA-Bundle hochzuladen.

3. Fügen Sie StorageGRID als Cloud-Tier in ONTAP bei.

Geben Sie den Endpoint-Port des Load Balancer und den vollständig qualifizierten Domännennamen an, der im hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat ein.



Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zertifikat der Zwischenzertifizierungsstelle vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.

Konfigurieren Sie Client-Zertifikate

Mit Clientzertifikaten können autorisierte externe Clients auf die StorageGRID Prometheus-Datenbank zugreifen und externe Tools zur Überwachung von StorageGRID sicher einsetzen.

Wenn Sie mit einem externen Monitoring-Tool auf StorageGRID zugreifen müssen, müssen Sie mithilfe des Grid Managers ein Clientzertifikat hochladen oder generieren und die Zertifikatsinformationen in das externe Tool kopieren.

Siehe "[Verwalten von Sicherheitszertifikaten](#)" Und "[Konfigurieren Sie benutzerdefinierte Serverzertifikate](#)".



Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf von Client-Zertifikaten, die auf der Seite Zertifikate konfiguriert ist** ausgelöst, wenn dieses Serverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION > Sicherheit > Zertifikate** und das Ablaufdatum des Clientzertifikats auf der Registerkarte Client auswählen.



Wenn Sie zum Schutz der Daten auf speziell konfigurierten Appliance-Nodes einen Verschlüsselungsmanagement-Server (KMS) verwenden, lesen Sie die spezifischen Informationen zu "[Hochladen eines KMS-Clientzertifikats](#)".

Bevor Sie beginnen

- Sie haben Root-Zugriffsberechtigung.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- So konfigurieren Sie ein Clientzertifikat:
 - Sie haben die IP-Adresse oder den Domännennamen des Admin-Knotens.
 - Wenn Sie das Zertifikat für die StorageGRID-Managementoberfläche konfiguriert haben, verfügen Sie über die CA, das Client-Zertifikat und den privaten Schlüssel, mit dem Sie das Zertifikat für die Managementoberfläche konfigurieren können.
 - Um Ihr eigenes Zertifikat hochzuladen, steht der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer zur Verfügung.
 - Der private Schlüssel muss zum Zeitpunkt der Erstellung gespeichert oder aufgezeichnet worden sein. Wenn Sie nicht über den ursprünglichen privaten Schlüssel verfügen, müssen Sie einen neuen

erstellen.

- So bearbeiten Sie ein Clientzertifikat:
 - Sie haben die IP-Adresse oder den Domännennamen des Admin-Knotens.
 - Um Ihr eigenes Zertifikat oder ein neues Zertifikat hochzuladen, sind der private Schlüssel, das Clientzertifikat und die CA (sofern verwendet) auf Ihrem lokalen Computer verfügbar.

Fügen Sie Client-Zertifikate hinzu

Gehen Sie wie folgt vor, um das Clientzertifikat hinzuzufügen:

- [Das Zertifikat der Managementoberfläche ist bereits konfiguriert](#)
- [KANN Client-Zertifikat AUSGESTELLT haben](#)
- [Zertifikat vom Grid Manager generiert](#)

Das Zertifikat der Managementoberfläche ist bereits konfiguriert

Verwenden Sie diese Vorgehensweise, um ein Clientzertifikat hinzuzufügen, wenn bereits ein Zertifikat für eine Managementoberfläche mit einer vom Kunden bereitgestellten CA, einem Clientzertifikat und einem privaten Schlüssel konfiguriert wurde.

Schritte

1. Wählen Sie im Grid Manager die Option **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein.
4. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Laden Sie für den Schritt **Attach certificates** das Management Interface Zertifikat hoch.
 - a. Wählen Sie **Zertifikat hochladen**.
 - b. Wählen Sie **Browse** und wählen Sie die Zertifikatdatei der Verwaltungsschnittstelle aus (.pem).
 - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
 - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.
 - c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

7. [Konfiguration eines externen Überwachungstools](#), Wie Grafana.

KANN Client-Zertifikat AUSGESTELLT haben

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn ein Zertifikat der Verwaltungsschnittstelle nicht konfiguriert wurde und Sie planen, ein Client-Zertifikat für Prometheus hinzuzufügen, das ein vom Zertifizierungsstellen ausgestelltes Clientzertifikat und einen privaten Schlüssel verwendet.

Schritte

1. Führen Sie die Schritte zu aus "[Konfigurieren Sie ein Zertifikat für die Managementoberfläche](#)".
2. Wählen Sie im Grid Manager die Option **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Zertifikatnamen ein.
5. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
6. Wählen Sie **Weiter**.
7. Laden Sie für den Schritt **Attach certificates** das Clientzertifikat, den privaten Schlüssel und die CA-Bundle-Dateien hoch:
 - a. Wählen Sie **Zertifikat hochladen**.
 - b. Wählen Sie **Browse** aus, und wählen Sie das Clientzertifikat, den privaten Schlüssel und die CA-Paketdateien aus (.pem).
 - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
 - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.
 - c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Die neuen Zertifikate werden auf der Registerkarte Client angezeigt.

8. [Konfiguration eines externen Überwachungstools](#), Wie Grafana.

Zertifikat vom Grid Manager generiert

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn ein Zertifikat der Verwaltungsschnittstelle nicht konfiguriert wurde und Sie planen, ein Clientzertifikat für Prometheus hinzuzufügen, das die Funktion Zertifikat generieren in Grid Manager verwendet.

Schritte

1. Wählen Sie im Grid Manager die Option **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein.
4. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Wählen Sie für den Schritt **Zertifikate anhängen Zertifikat generieren** aus.
7. Geben Sie die Zertifikatsinformationen an:
 - **Subject** (optional): X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers.
 - **Tag gültig**: Die Anzahl der Tage, an denen das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt, an dem es generiert wird.
 - **Key-Usage-Erweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden Key-

Usage und erweiterte Key-Usage-Erweiterungen zum generierten Zertifikat hinzugefügt.

Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist.



Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, es treten Verbindungsprobleme mit älteren Clients auf, wenn diese Erweiterungen in Zertifikaten enthalten sind.

8. Wählen Sie **Erzeugen**.

9. Wählen Sie **Client-Zertifikatsdetails** aus, um die Zertifikatmetadaten und das PEM-Zertifikat anzuzeigen.



Nach dem Schließen des Dialogfelds können Sie den privaten Zertifikatschlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einem sicheren Ort.

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere Stelle zu kopieren.
- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Privatschlüssel kopieren**, um den privaten Zertifikatschlüssel zum Einfügen an andere Orte zu kopieren.
- Wählen Sie **privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

Geben Sie den Dateinamen des privaten Schlüssels und den Speicherort für den Download an.

10. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

11. Wählen Sie im Grid Manager die Option **KONFIGURATION > Sicherheit > Zertifikate** und wählen Sie dann die Registerkarte **Global** aus.

12. Wählen Sie **Management Interface Certificate** aus.

13. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.

14. Laden Sie die Dateien `Certificate.pem` und `private_key.pem` aus dem hoch [Details zum Clientzertifikat](#) Schritt: Es ist nicht erforderlich, das CA-Paket hochzuladen.

- Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
- Laden Sie jede Zertifikatsdatei hoch (`.pem`).
- Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

15. [Konfiguration eines externen Überwachungstools](#), Wie Grafana.

Konfigurieren Sie ein externes Monitoring-Tool

Schritte

1. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.

- a. **Name:** Geben Sie einen Namen für die Verbindung ein.

StorageGRID benötigt diese Informationen nicht, Sie müssen jedoch einen Namen angeben, um die Verbindung zu testen.

- b. **URL:** Geben Sie den Domain-Namen oder die IP-Adresse für den Admin-Node ein. Geben Sie HTTPS und Port 9091 an.

Beispiel: `https://admin-node.example.com:9091`

- c. Aktivieren Sie **TLS Client Auth** und **mit CA Cert**.

- d. Kopieren Sie unter TLS/SSL Auth Details und fügen Sie: + ein

- Das Management-Interface-CA-Zertifikat nach **CA-Zertifikat**
- Das Client-Zertifikat an **Client-Zertifikat**
- Der private Schlüssel zu **Client Key**

- e. **ServerName:** Geben Sie den Domainnamen des Admin-Knotens ein.

Servername muss mit dem Domännennamen übereinstimmen, wie er im Zertifikat der Verwaltungsschnittstelle angezeigt wird.

2. Speichern und testen Sie das Zertifikat und den privaten Schlüssel, das Sie aus StorageGRID oder einer lokalen Datei kopiert haben.

Sie können jetzt mit Ihrem externen Monitoring Tool auf die Prometheus Kennzahlen von StorageGRID zugreifen.

Weitere Informationen zu den Metriken finden Sie im "[Anweisungen zur Überwachung von StorageGRID](#)".

Client-Zertifikate bearbeiten

Sie können ein Administrator-Clientzertifikat bearbeiten, um seinen Namen zu ändern, Prometheus-Zugriff zu aktivieren oder zu deaktivieren oder ein neues Zertifikat hochzuladen, wenn das aktuelle Zertifikat abgelaufen ist.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.

In der Tabelle sind die Daten zum Ablauf des Zertifikats und die Zugriffsrechte für Prometheus aufgeführt. Wenn ein Zertifikat bald abläuft oder bereits abgelaufen ist, wird in der Tabelle eine Meldung angezeigt, und eine Warnmeldung wird ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.

3. Wählen Sie **Bearbeiten** und dann **Name und Berechtigung bearbeiten** aus

4. Geben Sie einen Zertifikatnamen ein.

5. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.

6. Wählen Sie **Weiter**, um das Zertifikat im Grid Manager zu speichern.

Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Verbinden Sie das neue Clientzertifikat

Sie können ein neues Zertifikat hochladen, wenn das aktuelle Zertifikat abgelaufen ist.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.

In der Tabelle sind die Daten zum Ablauf des Zertifikats und die Zugriffsrechte für Prometheus aufgeführt. Wenn ein Zertifikat bald abläuft oder bereits abgelaufen ist, wird in der Tabelle eine Meldung angezeigt, und eine Warnmeldung wird ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.

3. Wählen Sie **Bearbeiten** und dann eine Bearbeitungsoption aus.

Zertifikat hochladen

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

- a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
- b. Laden Sie den Namen des Clientzertifikats hoch (.pem).

Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung .pem.

Beispiel: storagegrid_certificate.pem

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.
- c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Zertifikat wird generiert

Generieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

- a. Wählen Sie **Zertifikat erstellen**.
- b. Geben Sie die Zertifikatsinformationen an:

- **Subject** (optional): X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers.
- **Tage gültig**: Die Anzahl der Tage, an denen das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt, an dem es generiert wird.
- **Key-Usage-Erweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden Key-Usage und erweiterte Key-Usage-Erweiterungen zum generierten Zertifikat hinzugefügt.

Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist.



Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, es treten Verbindungsprobleme mit älteren Clients auf, wenn diese Erweiterungen in Zertifikaten enthalten sind.

- c. Wählen Sie **Erzeugen**.
- d. Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.



Nach dem Schließen des Dialogfelds können Sie den privaten Zertifikatschlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einem sicheren Ort.

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine

andere Stelle zu kopieren.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an.
Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Privatschlüssel kopieren**, um den privaten Zertifikatschlüssel zum Einfügen an andere Orte zu kopieren.
- Wählen Sie **privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

Geben Sie den Dateinamen des privaten Schlüssels und den Speicherort für den Download an.

- e. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

Herunterladen oder Kopieren von Clientzertifikaten

Sie können ein Clientzertifikat zur Verwendung an anderer Stelle herunterladen oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie das Zertifikat aus, das Sie kopieren oder herunterladen möchten.
3. Laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei herunter

Laden Sie das Zertifikat herunter `.pem` Datei:

- a. Wählen Sie **Zertifikat herunterladen**.
- b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

- a. Wählen Sie **Zertifikat kopieren PEM**.
- b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
- c. Speichern Sie die Textdatei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

Entfernen Sie Client-Zertifikate

Wenn Sie kein Administrator-Clientzertifikat mehr benötigen, können Sie es entfernen.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie das Zertifikat aus, das Sie entfernen möchten.
3. Wählen Sie **Löschen** und bestätigen Sie dann.



Um bis zu 10 Zertifikate zu entfernen, wählen Sie auf der Registerkarte Client jedes zu entfernende Zertifikat aus und wählen dann **Aktionen > Löschen** aus.

Nachdem ein Zertifikat entfernt wurde, müssen Clients, die das Zertifikat verwendet haben, ein neues Clientzertifikat angeben, um auf die StorageGRID Prometheus-Datenbank zuzugreifen.

Konfigurieren Sie die Sicherheitseinstellungen

Verwalten Sie die TLS- und SSH-Richtlinie

Die TLS- und SSH-Richtlinie legt fest, welche Protokolle und Chiffren verwendet werden, um sichere TLS-Verbindungen mit Clientanwendungen und sichere SSH-Verbindungen zu internen StorageGRID-Diensten herzustellen.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten in Bewegung verschlüsseln. Verwenden Sie im Allgemeinen die moderne Kompatibilitätsrichtlinie (Standard), es sei denn, Ihr System muss Common Criteria-konform sein oder Sie müssen andere Chiffren verwenden.



Einige StorageGRID-Dienste wurden nicht aktualisiert, um die Chiffren in diesen Richtlinien zu verwenden.

Bevor Sie beginnen

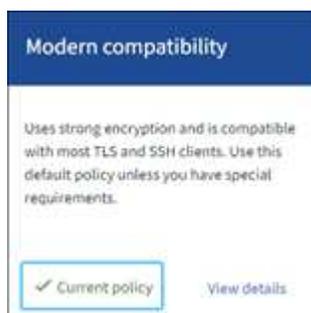
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Root-Zugriffsberechtigung](#)".

Wählen Sie eine Sicherheitsrichtlinie aus

Schritte

1. Wählen Sie **CONFIGURATION > Security > Security settings**.

Auf der Registerkarte **TLS und SSH Policies** werden die verfügbaren Richtlinien angezeigt. Die derzeit aktive Richtlinie wird durch ein grünes Häkchen auf der Kachel „Richtlinie“ gekennzeichnet.



2. Lesen Sie die Kacheln, um mehr über die verfügbaren Richtlinien zu erfahren.

Richtlinie	Beschreibung
Moderne Kompatibilität (Standard)	Verwenden Sie die Standardrichtlinie, wenn Sie eine starke Verschlüsselung benötigen und wenn Sie keine besonderen Anforderungen haben. Diese Richtlinie ist mit den meisten TLS- und SSH-Clients kompatibel.
Kompatibilität mit älteren Systemen	Verwenden Sie diese Richtlinie, wenn Sie zusätzliche Kompatibilitätsoptionen für ältere Clients benötigen. Die zusätzlichen Optionen in dieser Richtlinie machen sie möglicherweise weniger sicher als die moderne Kompatibilitätsrichtlinie.
Gemeinsame Kriterien	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen.
FIPS-strikt	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen und das NetApp Cryptographic Security Module 3.0.0 für externe Client-Verbindungen zu Load Balancer-Endpunkten, Tenant Manager und Grid Manager verwenden müssen. Die Verwendung dieser Richtlinie kann die Performance beeinträchtigen.
Individuell	Erstellen Sie eine benutzerdefinierte Richtlinie, wenn Sie Ihre eigenen Chiffren anwenden müssen.

3. Um Details zu den Chiffren, Protokollen und Algorithmen der einzelnen Richtlinien anzuzeigen, wählen Sie **Details anzeigen**.

4. Um die aktuelle Richtlinie zu ändern, wählen Sie **Richtlinie verwenden**.

Ein grünes Häkchen erscheint neben **Aktuelle Richtlinie** auf der Policy-Kachel.

Erstellen Sie eine benutzerdefinierte Sicherheitsrichtlinie

Sie können eine benutzerdefinierte Richtlinie erstellen, wenn Sie Ihre eigenen Chiffren anwenden müssen.

Schritte

1. Wählen Sie auf der Kachel der Richtlinie, die der benutzerdefinierten Richtlinie, die Sie erstellen möchten, am ähnlichsten ist, **Details anzeigen** aus.
2. Wählen Sie **in Zwischenablage kopieren**, und wählen Sie dann **Abbrechen**.



3. Wählen Sie in der Kachel **Benutzerdefinierte Richtlinie** die Option **Konfigurieren und Verwenden** aus.
4. Fügen Sie die JSON ein, die Sie kopiert haben, und nehmen Sie alle erforderlichen Änderungen vor.
5. Wählen Sie **Richtlinie verwenden**.

Auf der Kachel „Benutzerdefinierte Richtlinie“ wird ein grünes Häkchen neben **Aktuelle Richtlinie** angezeigt.

6. Wählen Sie optional **Konfiguration bearbeiten**, um weitere Änderungen an der neuen benutzerdefinierten Richtlinie vorzunehmen.

Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfiguriert haben, können Sie sich möglicherweise nicht beim Grid Manager anmelden, wenn die konfigurierte TLS-Richtlinie nicht mit dem kompatibel ist ["Serverzertifikat konfiguriert"](#).

Sie können vorübergehend auf die Standard-Sicherheitsrichtlinie zurücksetzen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

2. Führen Sie den folgenden Befehl aus:

```
restore-default-cipher-configurations
```

3. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Node zu.
4. Befolgen Sie die Schritte unter [Wählen Sie eine Sicherheitsrichtlinie aus](#) Um die Richtlinie erneut zu

konfigurieren.

Konfigurieren Sie die Netzwerk- und Objektsicherheit

Sie können die Netzwerk- und Objektsicherheit so konfigurieren, dass gespeicherte Objekte verschlüsselt, bestimmte S3- und Swift-Anforderungen verhindert oder Client-Verbindungen zu Storage-Nodes HTTP anstelle von HTTPS verwenden.

Verschlüsselung gespeicherter Objekte

Die gespeicherte Objektverschlüsselung ermöglicht die Verschlüsselung aller Objektdaten bei der Aufnahme über S3. Gespeicherte Objekte werden standardmäßig nicht verschlüsselt, aber Sie können Objekte mit dem AES-128- oder AES-256-Verschlüsselungsalgorithmus verschlüsseln. Wenn Sie die Einstellung aktivieren, werden alle neu aufgenommenen Objekte verschlüsselt, aber es werden keine Änderungen an vorhandenen gespeicherten Objekten vorgenommen. Wenn Sie die Verschlüsselung deaktivieren, bleiben derzeit verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

Die Einstellung für die Verschlüsselung gespeicherter Objekte ist nur für S3-Objekte anwendbar, die nicht durch Verschlüsselung auf Bucket-Ebene oder Objekt-Ebene verschlüsselt wurden.

Weitere Informationen zu Verschlüsselungsmethoden von StorageGRID finden Sie unter "[Prüfen Sie die StorageGRID Verschlüsselungsmethoden](#)".

Client-Änderung verhindern

Die Einstellung „Client-Änderung verhindern“ ist eine systemweite Einstellung. Wenn die Option **Client-Änderung verhindern** ausgewählt ist, werden die folgenden Anfragen abgelehnt.

S3-REST-API

- Bucket-Anforderungen löschen
- Alle Anforderungen, die das Ändern von Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging zum Einsatz kommen

Swift REST API

- Container-Anforderungen löschen
- Anträge zum Ändern vorhandener Objekte. Beispielsweise werden folgende Vorgänge verweigert: Put Overwrite, Delete, Metadata Update usw.

Aktivieren Sie HTTP für Storage Node-Verbindungen

Standardmäßig verwenden Clientanwendungen das HTTPS-Netzwerkprotokoll für alle direkten Verbindungen zu Storage-Nodes. Optional können Sie HTTP für diese Verbindungen aktivieren, z. B. beim Testen eines nicht produktiven Grids.

Verwenden Sie HTTP für Storage-Node-Verbindungen nur, wenn S3- und Swift-Clients HTTP-Verbindungen direkt zu Storage-Nodes herstellen müssen. Sie müssen diese Option nicht für Clients verwenden, die nur HTTPS-Verbindungen verwenden, oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (weil Sie dies können "[Konfigurieren Sie jeden Endpunkt der Lastverteilung](#)" Zur Verwendung von HTTP oder HTTPS).

Siehe "[Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen](#)" Um zu erfahren, welche Ports S3

und Swift-Clients bei der Verbindung zu Storage-Nodes über HTTP oder HTTPS verwenden.

Wählen Sie Optionen aus

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **CONFIGURATION > Security > Security settings**.
2. Wählen Sie die Registerkarte **Netzwerk und Objekte**.
3. Verwenden Sie für die Verschlüsselung gespeicherter Objekte die Einstellung **None** (Standard), wenn Sie keine Verschlüsselung gespeicherter Objekte wünschen, oder wählen Sie **AES-128** oder **AES-256**, um gespeicherte Objekte zu verschlüsseln.
4. Wählen Sie optional **Client-Änderung verhindern**, wenn Sie S3- und Swift-Clients daran hindern möchten, spezifische Anforderungen zu stellen.



Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

5. Wählen Sie optional **HTTP für Storage Node-Verbindungen aktivieren**, wenn Clients direkt mit Storage Nodes verbunden sind und Sie HTTP-Verbindungen verwenden möchten.



Gehen Sie vorsichtig vor, wenn Sie HTTP für ein Produktions-Grid aktivieren, da die Anforderungen unverschlüsselt gesendet werden.

6. Wählen Sie **Speichern**.

Zeitlimit für Inaktivität des Browsers ändern

Sie können steuern, ob Grid Manager und Tenant Manager-Benutzer abgemeldet werden, wenn sie länger als eine bestimmte Zeit inaktiv sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben Root-Zugriffsberechtigung.

Über diese Aufgabe

Das Zeitlimit für die Inaktivität des Browsers beträgt standardmäßig 15 Minuten. Wenn der Browser eines Benutzers für diese Zeit nicht aktiv ist, wird der Benutzer abgemeldet.

Bei Bedarf können Sie die Sperrzeit erhöhen oder verringern, indem Sie die Option * Inaktive Benutzer abmelden nach* einstellen.

Das Zeitlimit für die Inaktivität des Browsers wird auch durch Folgendes gesteuert:

- Ein separater, nicht konfigurierbarer StorageGRID-Timer, der für die Systemsicherheit enthalten ist. Standardmäßig läuft das Authentifizierungs-Token jedes Benutzers 16 Stunden nach der Anmeldung des Benutzers ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch

abgemeldet, auch wenn das Zeitlimit für die Inaktivität des Browsers deaktiviert ist oder der Wert für das Browsertimeout nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.

- Timeout-Einstellungen für den Identitäts-Provider, vorausgesetzt, Single Sign-On (SSO) ist für StorageGRID aktiviert.

Wenn SSO aktiviert ist und der Browser eines Benutzers eine Zeitdauer ausläuft, muss der Benutzer seine SSO-Anmeldeinformationen erneut eingeben, um erneut auf StorageGRID zuzugreifen. Siehe ["Konfigurieren Sie Single Sign-On"](#).

Schritte

1. Wählen Sie **CONFIGURATION > Security > Security settings**.
2. Wählen Sie die Registerkarte **Browser Inaktivität Timeout**.
3. Geben Sie im Feld **Abmelden inaktiver Benutzer nach** einen Browser-Timeout-Zeitraum zwischen 60 Sekunden und 7 Tagen an.

Sie können die Zeitüberschreitung des Browsers in Sekunden, Minuten, Stunden oder Tagen angeben.

4. Wählen Sie **Speichern**. Wenn ein Browser für die angegebene Zeit inaktiv ist, wird der Benutzer vom Grid Manager oder Tenant Manager abgemeldet.

Die neue Einstellung hat keine Auswirkung auf die derzeit angemeldeten Benutzer. Benutzer müssen sich erneut anmelden oder ihre Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

Konfigurieren von Verschlüsselungsmanagement-Servern

Key Management-Server konfigurieren: Übersicht

Sie können einen oder mehrere externe Verschlüsselungsmanagement-Server (KMS) konfigurieren, um die Daten auf speziell konfigurierten Appliance-Nodes zu schützen.

Was ist ein KMS (Key Management Server)?

Ein Verschlüsselungsmanagement-Server (KMS) ist ein externes Drittanbietersystem, das mithilfe des Key Management Interoperability Protocol (KMIP) Verschlüsselungen für die StorageGRID Appliance-Nodes am zugehörigen StorageGRID Standort bereitstellt.

Sie können einen oder mehrere Schlüsselverwaltungsserver verwenden, um die Knotenverschlüsselungsschlüssel für alle StorageGRID Appliance-Knoten zu verwalten, deren **Node-Verschlüsselung**-Einstellung während der Installation aktiviert ist. Durch den Einsatz von Verschlüsselungsmanagement-Servern mit diesen Appliance-Nodes können Sie Ihre Daten selbst dann schützen, wenn eine Appliance aus dem Datacenter entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.

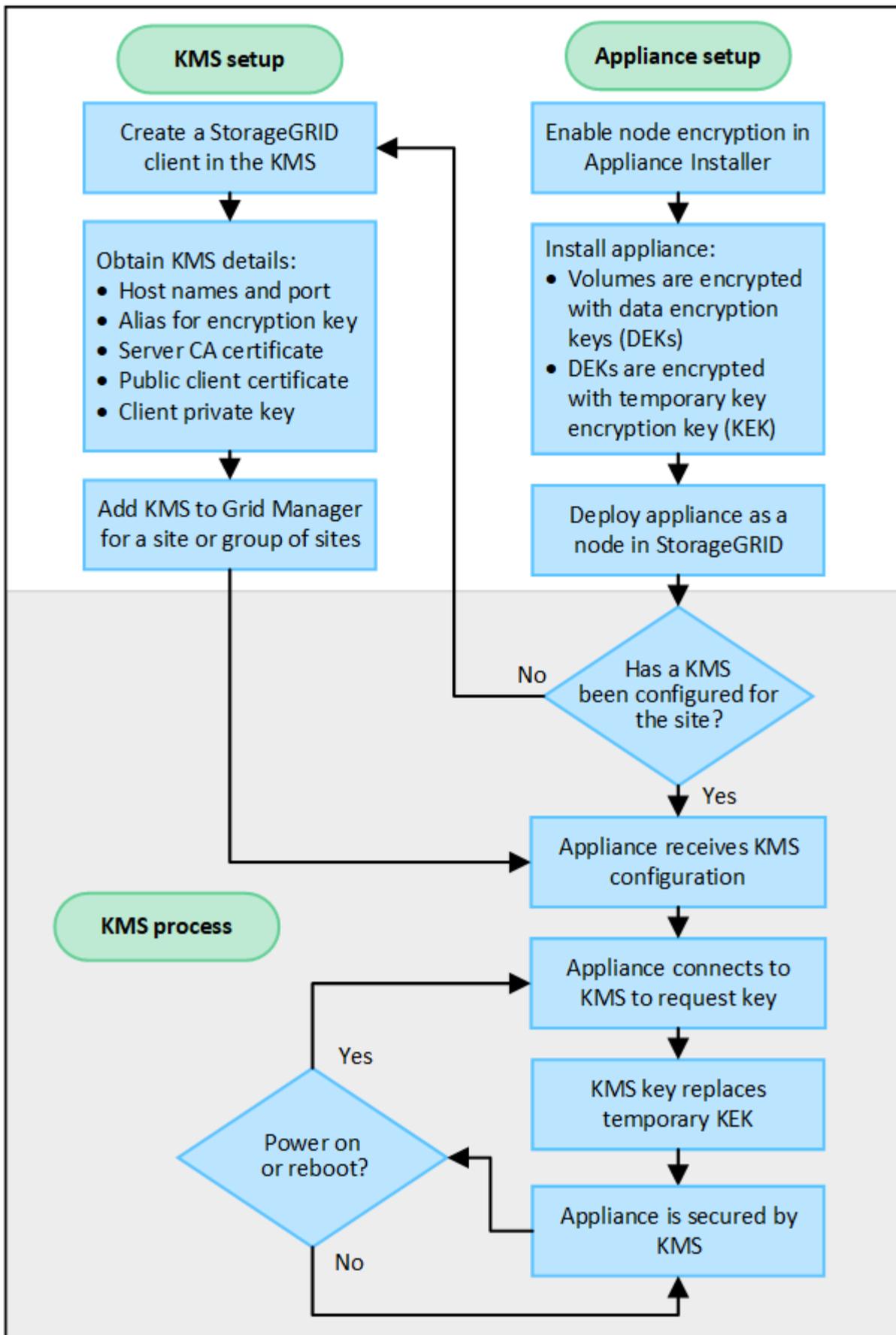


StorageGRID erstellt oder verwaltet keine externen Schlüssel, die zur Verschlüsselung und Entschlüsselung von Appliance-Nodes verwendet werden. Wenn Sie Vorhaben, einen externen Verschlüsselungsmanagementserver zum Schutz von StorageGRID-Daten zu verwenden, müssen Sie wissen, wie Sie diesen Server einrichten, und wissen, wie Sie die Verschlüsselungsschlüssel managen. Die Ausführung wichtiger Managementaufgaben geht über diesen Anweisungen hinaus. Wenn Sie Hilfe benötigen, lesen Sie die Dokumentation für Ihren zentralen Managementserver, oder wenden Sie sich an den technischen Support.

Überblick über die KMS- und Appliance-Konfiguration

Bevor der Verschlüsselungsmanagement-Server (KMS) die StorageGRID-Daten auf Appliance-Nodes sichern kann, müssen zwei Konfigurationsaufgaben durchgeführt werden: Ein oder mehrere KMS-Server einrichten und die Node-Verschlüsselung für die Appliance-Nodes aktivieren. Wenn diese beiden Konfigurationsaufgaben abgeschlossen sind, erfolgt automatisch der Verschlüsselungsmanagementprozess.

Das Flussdiagramm zeigt die grundlegenden Schritte bei der Verwendung eines KMS zur Sicherung von StorageGRID-Daten auf Appliance-Nodes.



Das Flussdiagramm zeigt die parallele Einrichtung von KMS und die Einrichtung der Appliance. Sie können

jedoch die Verschlüsselungsmanagement-Server je nach Ihren Anforderungen vor oder nach Aktivierung der Node-Verschlüsselung für neue Appliance-Nodes einrichten.

Einrichten des Verschlüsselungsmanagement-Servers (KMS)

Die Einrichtung eines Schlüsselverwaltungsservers umfasst die folgenden grundlegenden Schritte.

Schritt	Siehe
Greifen Sie auf die KMS-Software zu und fügen Sie jedem KMS- oder KMS-Cluster einen Client für StorageGRID hinzu.	"Konfigurieren Sie StorageGRID als Client im KMS"
Erhalten Sie die erforderlichen Informationen für den StorageGRID-Client auf dem KMS.	"Konfigurieren Sie StorageGRID als Client im KMS"
Fügen Sie den KMS dem Grid Manager hinzu, weisen Sie ihn einer einzelnen Site oder einer Standardgruppe von Standorten zu, laden Sie die erforderlichen Zertifikate hoch und speichern Sie die KMS-Konfiguration.	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Richten Sie das Gerät ein

Die Einrichtung eines Appliance-Nodes für die KMS-Nutzung umfasst die folgenden grundlegenden Schritte.

1. Verwenden Sie während der Hardware-Konfigurationsphase der Appliance-Installation das Installationsprogramm von StorageGRID Appliance, um die Einstellung **Node-Verschlüsselung** für die Appliance zu aktivieren.



Sie können die Einstellung **Node Encryption** nicht aktivieren, nachdem eine Appliance zum Grid hinzugefügt wurde, und Sie können keine externe Schlüsselverwaltung für Geräte verwenden, für die keine Knotenverschlüsselung aktiviert ist.

2. Führen Sie das Installationsprogramm für die StorageGRID-Appliance aus. Während der Installation wird jedem Appliance-Volume ein zufälliger Datenverschlüsselungsschlüssel (random Data Encryption Key, DEK) zugewiesen:
 - Die DEKs werden verwendet, um die Daten auf jedem Volume zu verschlüsseln. Diese Schlüssel werden mit der Linux Unified Key Setup (LUKS)-Festplattenverschlüsselung im Betriebssystem der Appliance generiert und können nicht geändert werden.
 - Jede einzelne DEK wird durch einen Master Key Encryption Key (KEK) verschlüsselt. Bei der ersten KEK handelt es sich um einen temporären Schlüssel, der die DEKs verschlüsselt, bis das Gerät eine Verbindung mit dem KMS herstellen kann.
3. Fügen Sie den Appliance-Node StorageGRID hinzu.

Siehe ["Aktivieren Sie die Node-Verschlüsselung"](#) Entsprechende Details.

Verschlüsselungsmanagementprozess (wird automatisch durchgeführt)

Die Verschlüsselung des Verschlüsselungsmanagement umfasst die folgenden grundlegenden Schritte, die automatisch durchgeführt werden.

1. Wenn Sie eine Appliance installieren, bei der die Node-Verschlüsselung im Grid aktiviert ist, bestimmt StorageGRID, ob für den Standort, der den neuen Node enthält, eine KMS-Konfiguration vorhanden ist.
 - Wenn bereits ein KMS für den Standort konfiguriert wurde, erhält die Appliance die KMS-Konfiguration.
 - Wenn ein KMS für den Standort noch nicht konfiguriert wurde, werden die Daten auf der Appliance weiterhin durch die temporäre KEK verschlüsselt, bis Sie einen KMS für den Standort konfigurieren und die Appliance die KMS-Konfiguration erhält.
2. Die Appliance verwendet die KMS-Konfiguration, um eine Verbindung zum KMS herzustellen und einen Verschlüsselungsschlüssel anzufordern.
3. Der KMS sendet einen Verschlüsselungsschlüssel an die Appliance. Der neue Schlüssel des KMS ersetzt die temporäre KEK und wird nun zur Verschlüsselung und Entschlüsselung der DEKs für die Appliance-Volumes verwendet.



Alle Daten, die vor der Verbindung des verschlüsselten Appliance-Nodes mit dem konfigurierten KMS vorhanden sind, werden mit einem temporären Schlüssel verschlüsselt. Die Appliance-Volumes sollten jedoch erst dann als vor Entfernung aus dem Datacenter geschützt betrachtet werden, wenn der temporäre Schlüssel durch den KMS-Schlüssel ersetzt wird.

4. Wenn die Appliance eingeschaltet oder neu gestartet wird, stellt sie eine Verbindung zum KMS her, um den Schlüssel anzufordern. Der Schlüssel, der im flüchtigen Speicher gespeichert ist, kann einen Stromausfall oder einen Neustart nicht überleben.

Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers

Bevor Sie einen externen KMS (Key Management Server) konfigurieren, müssen Sie die Überlegungen und Anforderungen verstehen.

Was sind die KMIP-Anforderungen?

StorageGRID unterstützt KMIP Version 1.4.

["Spezifikation Des Key Management Interoperability Protocol Version 1.4"](#)

Für die Kommunikation zwischen den Appliance-Nodes und dem konfigurierten KMS werden sichere TLS-Verbindungen verwendet. StorageGRID unterstützt die folgenden TLS v1.2-Chiffren für KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Sie müssen sicherstellen, dass jeder Appliance-Node, der Node-Verschlüsselung verwendet, Netzwerkzugriff auf den für den Standort konfigurierten KMS- oder KMS-Cluster hat.

Die Netzwerk-Firewall-Einstellungen müssen es jedem Appliance-Node ermöglichen, über den Port zu kommunizieren, der für KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet wird. Der KMIP-Standardport ist 5696.

Welche Appliances werden unterstützt?

Sie können einen Schlüsselverwaltungsserver (KMS) verwenden, um Verschlüsselungsschlüssel für jede StorageGRID-Appliance in Ihrem Grid zu verwalten, auf der die Einstellung **Node-Verschlüsselung** aktiviert ist. Diese Einstellung kann nur während der Hardware-Konfigurationsphase der Appliance-Installation mithilfe des StorageGRID Appliance Installer aktiviert werden.



Nach dem Hinzufügen einer Appliance zum Grid kann die Node-Verschlüsselung nicht aktiviert werden. Zudem kann kein externes Verschlüsselungsmanagement für Appliances verwendet werden, bei denen die Node-Verschlüsselung nicht aktiviert ist.

Sie können das konfigurierte KMS für StorageGRID-Appliances und Appliance-Nodes verwenden.

Sie können das konfigurierte KMS nicht für softwarebasierte (nicht-Appliance-)Knoten verwenden, einschließlich der folgenden:

- Als Virtual Machines (VMs) implementierte Nodes
- Nodes, die in Container-Engines auf Linux Hosts implementiert sind

Auf diesen anderen Plattformen implementierte Nodes können Verschlüsselung außerhalb von StorageGRID auf Datenspeicher- oder Festplattenebene verwenden.

Wann sollte ich wichtige Management-Server konfigurieren?

Bei einer neuen Installation sollten Sie in der Regel einen oder mehrere Schlüsselverwaltungsserver im Grid Manager einrichten, bevor Sie Mandanten erstellen. Diese Reihenfolge stellt sicher, dass die Nodes geschützt sind, bevor Objektdaten auf ihnen gespeichert werden.

Sie können die Schlüsselverwaltungsserver im Grid Manager vor oder nach der Installation der Appliance-Knoten konfigurieren.

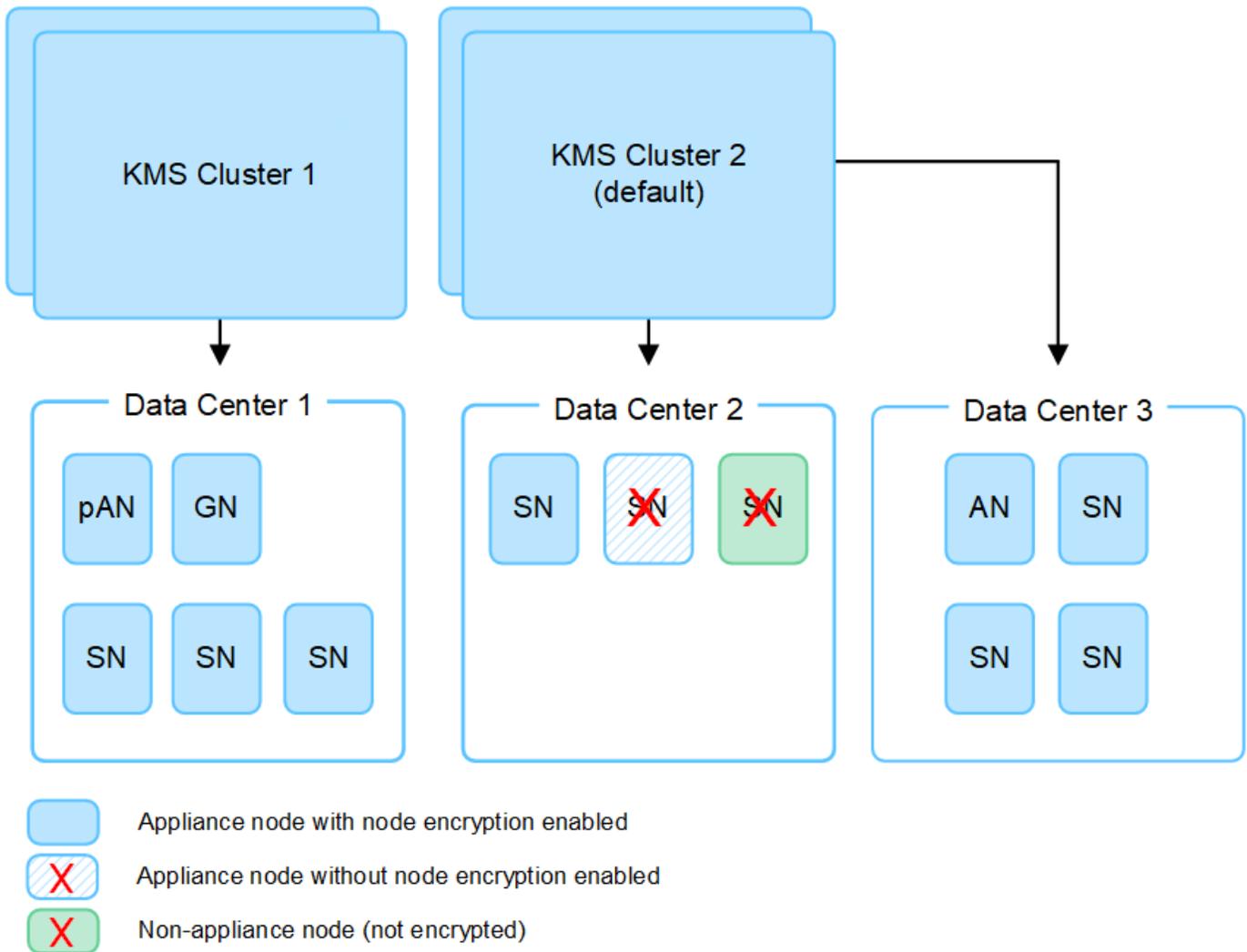
Wie viele wichtige Management Server brauche ich?

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver konfigurieren, um die Appliance-Nodes in Ihrem StorageGRID-System Verschlüsselungen bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel zur Verfügung.

StorageGRID unterstützt die Verwendung von KMS-Clustern. Jeder KMS-Cluster enthält mehrere replizierte Verschlüsselungsmanagement-Server, die Konfigurationseinstellungen und Verschlüsselungen teilen. Die Verwendung von KMS-Clustern für das Verschlüsselungsmanagement wird empfohlen, da dadurch die Failover-Funktionen einer Hochverfügbarkeitskonfiguration verbessert werden.

Nehmen Sie beispielsweise an, Ihr StorageGRID System verfügt über drei Datacenter-Standorte. Sie können ein KMS-Cluster konfigurieren, um allen Appliance-Nodes in Datacenter 1 und einem zweiten KMS-Cluster einen Schlüssel für alle Appliance-Nodes an allen anderen Standorten bereitzustellen. Wenn Sie den zweiten KMS-Cluster hinzufügen, können Sie einen Standard-KMS für Datacenter 2 und Datacenter 3 konfigurieren.

Beachten Sie, dass Sie kein KMS für nicht-Appliance-Knoten oder für alle Appliance-Knoten verwenden können, für die die Einstellung **Node Encryption** während der Installation nicht aktiviert war.



Was passiert, wenn eine Taste gedreht wird?

Als bewährte Sicherheitsmethode sollten Sie den Verschlüsselungsschlüssel, der von jedem konfigurierten KMS verwendet wird, regelmäßig drehen.

Wenn Sie den Verschlüsselungsschlüssel drehen, verwenden Sie die KMS-Software, um von der letzten verwendeten Version des Schlüssels auf eine neue Version desselben Schlüssels zu drehen. Drehen Sie nicht zu einer ganz anderen Taste.



Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS im Grid Manager ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Verwenden Sie denselben Schlüssel-Alias für neue Schlüssel, wie sie für vorherige Schlüssel verwendet wurden. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.

Wenn die neue Schlüsselversion verfügbar ist:

- Die Appliance wird automatisch auf die verschlüsselten Appliance-Nodes am Standort oder an den dem KMS zugeordneten Standorten verteilt. Die Verteilung sollte innerhalb einer Stunde erfolgen, wenn der Schlüssel gedreht wird.

- Wenn der Node der verschlüsselten Appliance offline ist, wenn die neue Schlüsselversion verteilt ist, erhält der Node den neuen Schlüssel, sobald er neu gebootet wird.
- Wenn die neue Schlüsselversion aus irgendeinem Grund nicht zur Verschlüsselung von Appliance-Volumes verwendet werden kann, wird der Alarm **KMS-Schlüsselrotation fehlgeschlagen** für den Appliance-Knoten ausgelöst. Möglicherweise müssen Sie sich an den technischen Support wenden, um Hilfe bei der Lösung dieses Alarms zu erhalten.

Kann ich einen Appliance-Knoten nach der Verschlüsselung wiederverwenden?

Wenn Sie eine verschlüsselte Appliance in einem anderen StorageGRID System installieren müssen, müssen Sie zuerst den Grid-Node außer Betrieb nehmen, um Objektdaten auf einen anderen Node zu verschieben. Anschließend können Sie das Installationsprogramm der StorageGRID-Appliance für verwenden "[Löschen Sie die KMS-Konfiguration](#)". Durch das Löschen der KMS-Konfiguration wird die **Node Encryption**-Einstellung deaktiviert und die Zuordnung zwischen dem Appliance-Knoten und der KMS-Konfiguration für den StorageGRID-Standort wird aufgehoben.



Der Zugriff auf den KMS-Verschlüsselungsschlüssel ist ausgeschlossen, dass alle Daten, die auf der Appliance verbleiben, nicht mehr zugänglich sind und dauerhaft gesperrt werden.

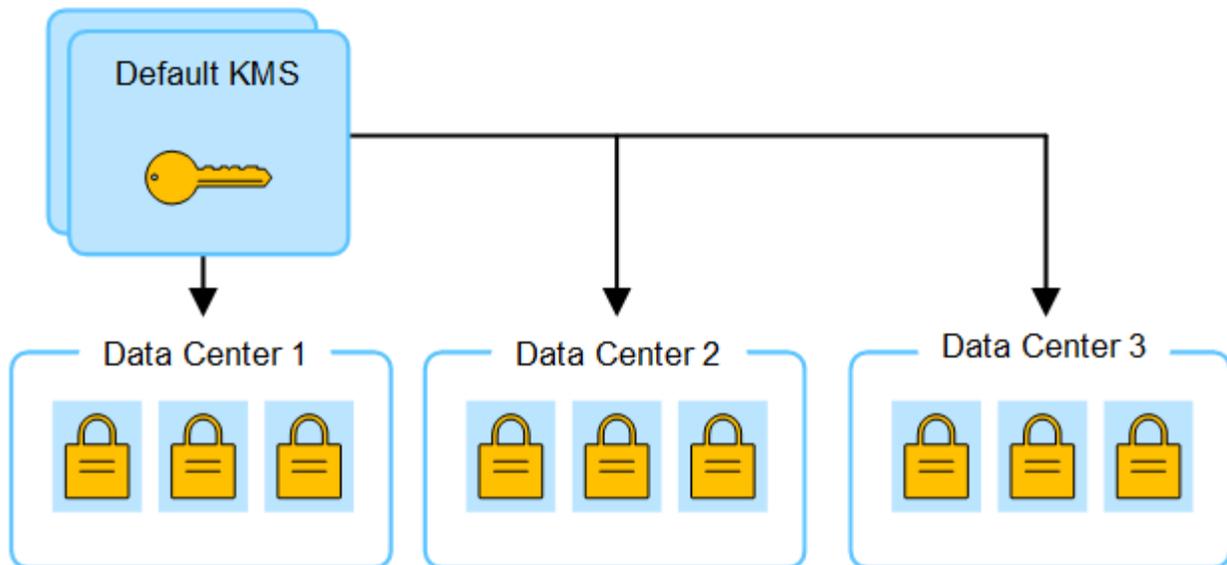
Überlegungen für das Ändern des KMS für einen Standort

Jeder Verschlüsselungsmanagement-Server (KMS) oder KMS-Cluster gewährt allen Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen Verschlüsselungsschlüssel. Wenn Sie ändern müssen, welcher KMS für einen Standort verwendet wird, müssen Sie den Verschlüsselungsschlüssel möglicherweise von einem KMS auf einen anderen kopieren.

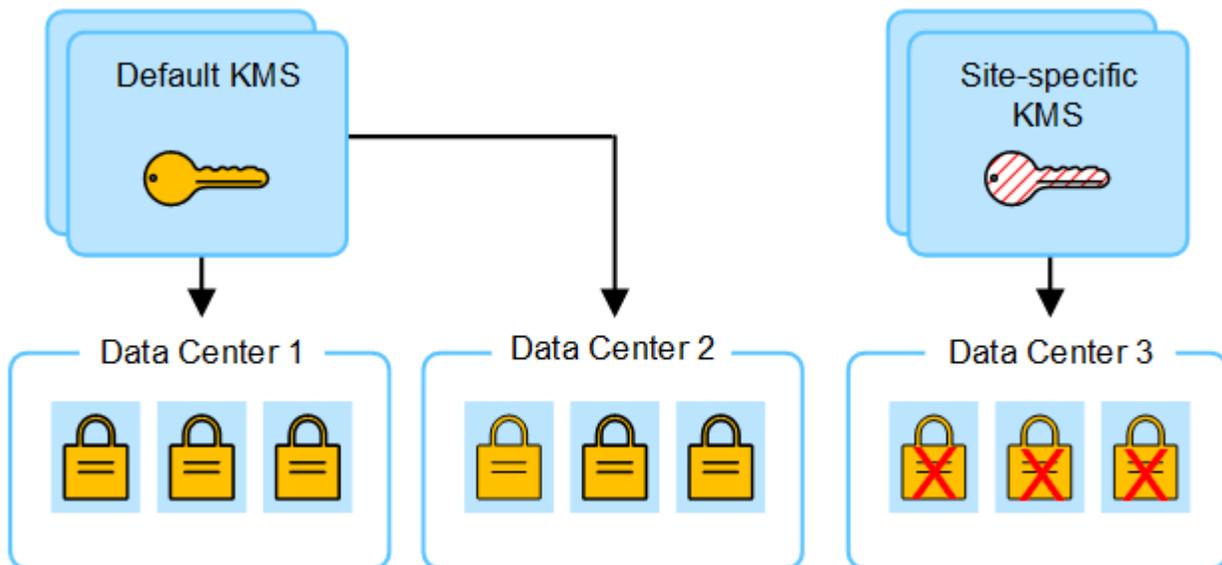
Wenn Sie den KMS ändern, der für einen Standort verwendet wird, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Nodes an diesem Standort mit dem auf dem neuen KMS gespeicherten Schlüssel entschlüsselt werden können. In einigen Fällen müssen Sie möglicherweise die aktuelle Version des Verschlüsselungsschlüssels vom ursprünglichen KMS auf den neuen KMS kopieren. Sie müssen sicherstellen, dass der KMS über den richtigen Schlüssel verfügt, um die verschlüsselten Appliance-Nodes am Standort zu entschlüsseln.

Beispiel:

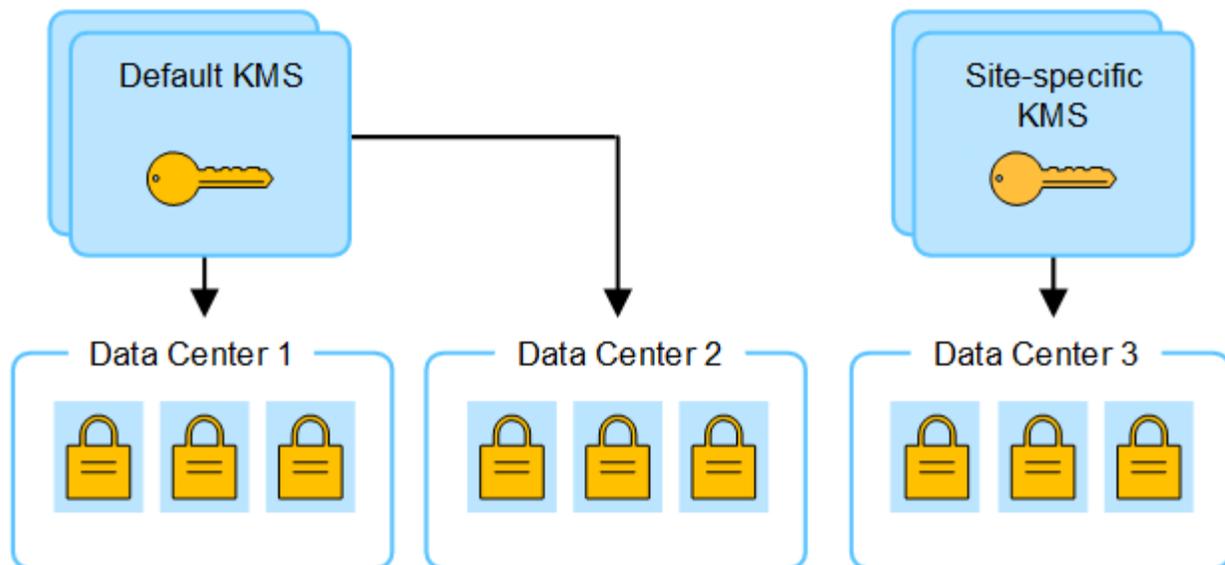
1. Sie konfigurieren zunächst ein Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben.
2. Wenn der KMS gespeichert wird, stellen alle Appliance-Nodes, deren **Node Encryption**-Einstellung aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel wird verwendet, um die Appliance-Nodes an allen Standorten zu verschlüsseln. Dieser Schlüssel muss auch verwendet werden, um diese Geräte zu entschlüsseln.



3. Sie entscheiden, einen standortspezifischen KMS für einen Standort hinzuzufügen (Datacenter 3 in der Abbildung). Da die Appliance-Nodes jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für den standortspezifischen KMS zu speichern. Der Fehler tritt auf, weil der standortspezifische KMS nicht über den korrekten Schlüssel verfügt, um die Knoten an diesem Standort zu entschlüsseln.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS. (Technisch kopieren Sie den Originalschlüssel in einen neuen Schlüssel mit dem gleichen Alias. Der ursprüngliche Schlüssel wird zu einer früheren Version des neuen Schlüssels.) Der standortspezifische KMS hat jetzt den richtigen Schlüssel zur Entschlüsselung der Appliance-Nodes in Datacenter 3, sodass er in StorageGRID gespeichert werden kann.



Anwendungsfälle für die Änderung, welcher KMS für eine Site verwendet wird

Die Tabelle fasst die erforderlichen Schritte für die häufigsten Fälle zur Änderung des KMS für einen Standort zusammen.

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie haben einen oder mehrere Site-spezifische KMS-Einträge, und Sie möchten einen von ihnen als Standard-KMS verwenden.	<p>Bearbeiten Sie den Site-spezifischen KMS. Wählen Sie im Feld verwaltet Schlüssel für die Option Sites, die nicht von einem anderen KMS verwaltet werden (Standard KMS). Der Site-spezifische KMS wird jetzt als Standard-KMS verwendet. Sie gilt für alle Standorte, die kein dediziertes KMS haben.</p> <p>"Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)"</p>
Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten nicht das Standard-KMS für den neuen Standort verwenden.	<ol style="list-style-type: none"> 1. Wenn die Appliance-Nodes auf dem neuen Standort bereits durch den Standard-KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf einen neuen KMS. 2. Fügen Sie mithilfe des Grid-Managers den neuen KMS hinzu und wählen Sie die Site aus. <p>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"</p>
Sie möchten, dass der KMS für eine Site einen anderen Server verwendet.	<ol style="list-style-type: none"> 1. Wenn die Appliance-Nodes am Standort bereits durch den vorhandenen KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom bestehenden KMS auf den neuen KMS. 2. Bearbeiten Sie mithilfe des Grid Manager die bestehende KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein. <p>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"</p>

Konfigurieren Sie StorageGRID als Client im KMS

Sie müssen StorageGRID als Client für jeden externen Verschlüsselungsmanagement-Server oder KMS-Cluster konfigurieren, bevor Sie den KMS StorageGRID hinzufügen können.

Über diese Aufgabe

Diese Anweisungen gelten für Thales CipherTrust Manager. Eine Liste der unterstützten Versionen finden Sie unter "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)".

Schritte

1. Erstellen Sie von der KMS-Software einen StorageGRID-Client für jeden KMS- oder KMS-Cluster, den Sie verwenden möchten.

Jeder KMS managt einen einzelnen Verschlüsselungsschlüssel für die Nodes der StorageGRID Appliances an einem einzelnen Standort oder einer Gruppe von Standorten.

2. Erstellen Sie von der KMS-Software einen AES-Verschlüsselungsschlüssel für jedes KMS- oder KMS-Cluster.

Der Verschlüsselungsschlüssel muss mindestens 2,048 Bit haben und exportierbar sein.

3. Notieren Sie die folgenden Informationen für jeden KMS- oder KMS-Cluster.

Diese Informationen benötigen Sie, wenn Sie den KMS StorageGRID hinzufügen.

- Host-Name oder IP-Adresse für jeden Server.
- Der vom KMS verwendete KMIP-Port.
- Schlüsselalias für den Verschlüsselungsschlüssel im KMS.



Der Verschlüsselungsschlüssel muss bereits im KMS vorhanden sein. StorageGRID erstellt oder managt keine KMS-Schlüssel.

4. Beziehen Sie für jeden KMS- oder KMS-Cluster ein Serverzertifikat, das von einer Zertifizierungsstelle (CA) signiert wurde, oder ein Zertifikatbündel, das jede der PEM-kodierten CA-Zertifikatdateien enthält, die in der Reihenfolge der Zertifikatskette verkettet sind.

Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

- Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.
- Das Feld für alternativen Servernamen (SAN) in jedem Serverzertifikat muss den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse enthalten, mit der StorageGRID eine Verbindung herstellt.



Wenn Sie den KMS in StorageGRID konfigurieren, müssen Sie dieselben FQDNs oder IP-Adressen im Feld **Hostname** eingeben.

- Das Serverzertifikat muss mit dem Zertifikat übereinstimmen, das von der KMIP-Schnittstelle des KMS verwendet wird. In der Regel wird Port 5696 verwendet.
5. Holen Sie sich das öffentliche Clientzertifikat, das vom externen KMS an StorageGRID ausgestellt wurde, und den privaten Schlüssel für das Clientzertifikat.

Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)

Mithilfe des Assistenten für den StorageGRID-Verschlüsselungsmanagement-Server können Sie jeden KMS- oder KMS-Cluster hinzufügen.

Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers](#)".
- Das ist schon "[StorageGRID wurde als Client im KMS konfiguriert](#)", Und Sie haben die erforderlichen Informationen für jeden KMS- oder KMS-Cluster.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Konfigurieren Sie, falls möglich, Site-spezifische Verschlüsselungsmanagement-Server, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS gemanagt werden. Wenn Sie zuerst den Standard-KMS erstellen, werden alle Node-verschlüsselten Appliances im Grid durch den Standard-KMS verschlüsselt. Wenn Sie später einen Site-spezifischen KMS erstellen möchten, müssen Sie zuerst die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS kopieren. Siehe "[Überlegungen für das Ändern des KMS für einen Standort](#)" Entsprechende Details.

Schritt 1: KM Details

In Schritt 1 (KMS-Details) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers geben Sie Details zum KMS- oder KMS-Cluster an.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt, und die Registerkarte Configuration Details ist ausgewählt.

Key management server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration details

Encrypted nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [Configure key management servers](#).

Create
Actions ▾

Displaying one result

<input type="checkbox"/>	KMS name	Key name	Manages keys for	Hostname	Certificate expiration
<input type="checkbox"/>	KMS	SG-Global	nmakmipdc1	thales1.vtc.englab.netapp.com and 2 others	✓ All certificates are valid

← Previous **1** Next →

2. Wählen Sie **Erstellen**.

Schritt 1 (KMS-Details) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird angezeigt.

Add a Key Management Server ✕

1 KMS Details
 2 Upload server certificate
 3 Upload client certificates

KMS details

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster select **Add another hostname** to add a hostname for each server in the cluster.

KMS name ?

Key name ?

Manages keys for ?

▼

Port ?

Hostname ?

[Add another hostname](#)

Cancel
Continue

3. Geben Sie die folgenden Informationen für den KMS und den StorageGRID-Client ein, den Sie in diesem KMS konfiguriert haben.

Feld	Beschreibung
KMS-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.
Schlüsselname	Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.

Feld	Beschreibung
Verwaltet Schlüssel für	<p>Der StorageGRID-Site, die diesem KMS zugeordnet wird. Wenn möglich, sollten Sie alle standortspezifischen Verschlüsselungsmanagement-Server konfigurieren, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden.</p> <ul style="list-style-type: none"> • Wählen Sie einen Standort aus, wenn dieser KMS Verschlüsselungen für die Appliance-Nodes an einem bestimmten Standort managt. • Wählen Sie Sites Not Managed by another KMS (default KMS) aus, um ein Standard-KMS zu konfigurieren, das für alle Sites gilt, die kein dediziertes KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. <p>Hinweis: beim Speichern der KMS-Konfiguration tritt Ein Validierungsfehler auf, wenn Sie eine Site auswählen, die zuvor durch den Standard-KMS verschlüsselt wurde, aber Sie haben die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels nicht dem neuen KMS zur Verfügung gestellt.</p>
Port	<p>Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.</p>
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.</p> <p>Hinweis: das Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.</p>

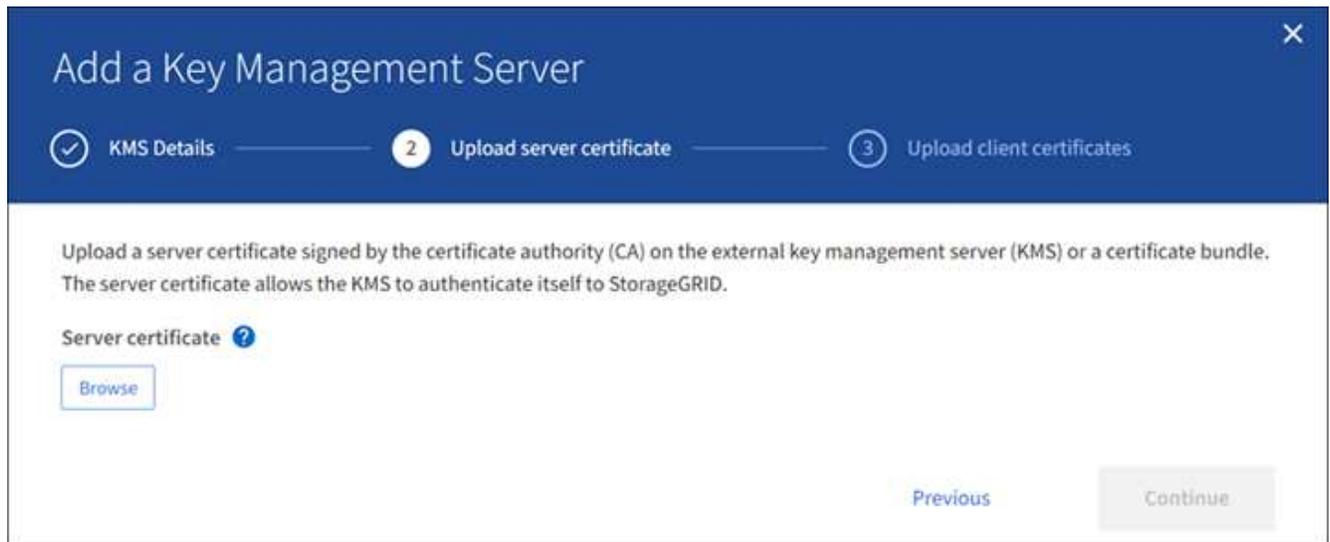
4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt 2: Serverzertifikat hochladen

In Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Serverzertifikat (oder Zertifikatpaket) für das KMS hoch. Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

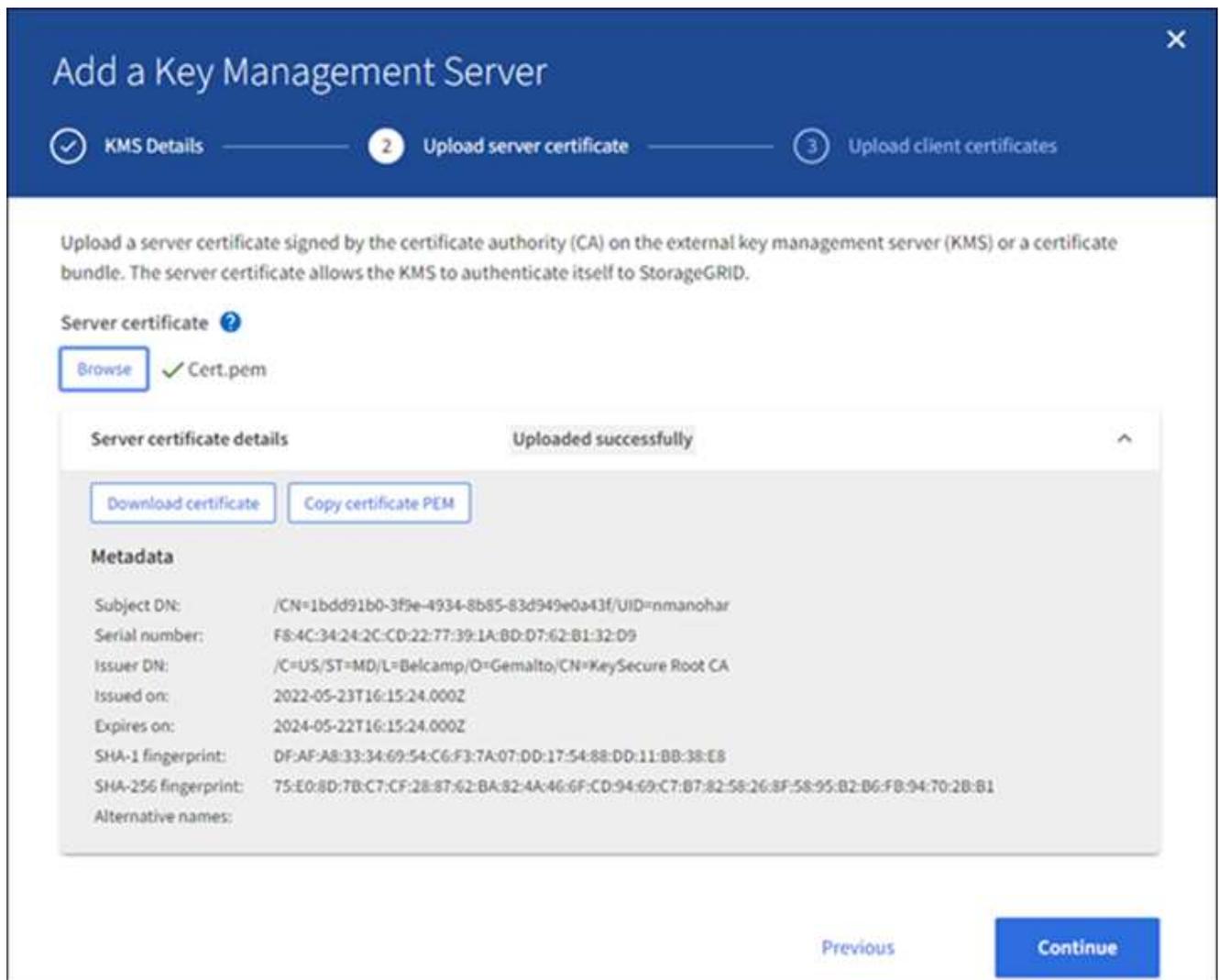
Schritte

1. Navigieren Sie aus **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatbündels.



2. Laden Sie die Zertifikatdatei hoch.

Die Metadaten des Serverzertifikats werden angezeigt.





Wenn Sie ein Zertifikatbündel hochgeladen haben, werden die Metadaten für jedes Zertifikat auf der eigenen Registerkarte angezeigt.

3. Wählen Sie **Weiter**.

Schritt 3: Laden Sie Clientzertifikate hoch

In Schritt 3 (Clientzertifikate hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Schritte

1. Navigieren Sie unter **Schritt 3 (Client-Zertifikate hochladen)** zum Speicherort des Client-Zertifikats.

The screenshot shows a wizard window titled "Add a Key Management Server". The progress bar at the top indicates three steps: "KMS Details" (completed), "Upload server certificate" (completed), and "3 Upload client certificates" (current step). The main content area contains the following text: "Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS." Below this text are two sections: "Client certificate" with a "Browse" button, and "Client certificate private key" with a "Browse" button. At the bottom right, there are two buttons: "Previous" and "Test and save".

2. Laden Sie die Clientzertifikatdatei hoch.

Die Metadaten des Client-Zertifikats werden angezeigt.

3. Navigieren Sie zum Speicherort des privaten Schlüssels für das Clientzertifikat.

4. Laden Sie die Datei mit dem privaten Schlüssel hoch.

5. Wählen Sie **Test und Speichern**.

Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und den Appliance-Nodes werden getestet. Wenn alle Verbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.



Unmittelbar nach dem Hinzufügen eines KMS wird der Zertifikatsstatus auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

6. Wenn bei der Auswahl von **Test und Speichern** eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie dann **OK** aus.

Beispiel: Wenn ein Verbindungstest fehlgeschlagen ist, können Sie einen Fehler bei unbearbeitbarer Einheit mit 422: Nicht verarbeitbarer Einheit erhalten.

7. Wenn Sie die aktuelle Konfiguration speichern müssen, ohne die externe Verbindung zu testen, wählen Sie **Speichern erzwingen**.



Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

- Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.

Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

KMS-Details anzeigen

Sie können Informationen zu jedem Schlüsselverwaltungsserver (KMS) in Ihrem StorageGRID-System anzeigen, einschließlich des aktuellen Status des Servers und der Clientzertifikate.

Schritte

- Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.

- Überprüfen Sie die Informationen in der Tabelle für jeden KMS.

Feld	Beschreibung
KMS-Name	Der beschreibende Name des KMS.
Schlüsselname	Der Schlüsselalias für den StorageGRID-Client im KMS.
Verwaltet Schlüssel für	Der dem KMS zugeordnete StorageGRID-Site. Dieses Feld zeigt den Namen einer bestimmten StorageGRID-Site oder Sites an, die nicht von einem anderen KMS verwaltet werden (Standard-KMS) .

Feld	Beschreibung
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse des KMS.</p> <p>Wenn ein Cluster von zwei Schlüsselverwaltungsservern vorhanden ist, werden der vollständig qualifizierte Domänenname oder die IP-Adresse beider Server aufgelistet. Wenn mehr als zwei Schlüsselverwaltungsserver in einem Cluster vorhanden sind, wird der vollständig qualifizierte Domänenname oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Schlüsselverwaltungsserver im Cluster aufgelistet.</p> <p>Beispiel: 10.10.10.10 and 10.10.10.11 Oder 10.10.10.10 and 2 others.</p> <p>Um alle Hostnamen in einem Cluster anzuzeigen, öffnen Sie ein KMS und wählen Bearbeiten oder Aktionen > Bearbeiten.</p>
Ablauf des Zertifikats	<p>Aktueller Status des Serverzertifikats, des optionalen CA-Zertifikats und des Client-Zertifikats: Gültig, abgelaufen, bald abgelaufen oder unbekannt.</p> <p>Hinweis: Es kann StorageGRID so lange wie 30 Minuten dauern, bis Updates zum Ablauf des Zertifikats erhalten. Sie müssen Ihren Webbrowser aktualisieren, um die aktuellen Werte anzuzeigen.</p>

3. Wenn der Ablauf des Zertifikats unbekannt ist, warten Sie bis zu 30 Minuten, und aktualisieren Sie dann Ihren Webbrowser.



Unmittelbar nach dem Hinzufügen eines KMS wird der Ablauf des Zertifikats auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

4. Wenn in der Spalte Zertifikatablauf angezeigt wird, dass ein Zertifikat abgelaufen ist oder kurz vor dem Ablaufdatum steht, beheben Sie das Problem so schnell wie möglich.

Wenn die Warnungen **KMS CA Certificate Expiration**, **KMS Client Certificate Expiration** und **KMS Server Certificate Expiration** ausgelöst werden, notieren Sie sich die Beschreibung der einzelnen Warnungen und führen Sie die empfohlenen Aktionen durch.



Sie müssen Probleme mit dem Zertifikat so schnell wie möglich beheben, um den Datenzugriff aufrechtzuerhalten.

5. Um die Zertifikatdetails für dieses KMS anzuzeigen, wählen Sie den KMS-Namen aus der Tabelle aus.
6. Überprüfen Sie auf der KMS-Übersichtsseite die Metadaten und das Zertifikat-PEM sowohl für das Serverzertifikat als auch für das Clientzertifikat. Wählen Sie bei Bedarf **Zertifikat bearbeiten**, um ein Zertifikat durch ein neues zu ersetzen.

Verschlüsselte Nodes anzeigen

Sie können Informationen zu den Appliance-Knoten in Ihrem StorageGRID-System anzeigen, bei denen die Einstellung **Node-Verschlüsselung** aktiviert ist.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.

2. Wählen Sie oben auf der Seite die Registerkarte **verschlüsselte Knoten** aus.

Auf der Registerkarte Verschlüsselte Knoten werden die Geräteknoten in Ihrem StorageGRID-System aufgelistet, für die die Einstellung **Knotenverschlüsselung** aktiviert ist.

3. Überprüfen Sie die Informationen in der Tabelle für jeden Appliance-Node.

Spalte	Beschreibung
Node-Name	Der Name des Appliance-Node.
Node-Typ	Der Node-Typ: Storage, Admin oder Gateway.
Standort	Der Name der StorageGRID-Site, auf der der Node installiert ist.
KMS-Name	Der beschreibende Name des für den Knoten verwendeten KMS. Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte Konfigurationsdetails aus, um ein KMS hinzuzufügen. "Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"
Schlüssel-UID	Die eindeutige ID des Verschlüsselungsschlüssels, der zur Verschlüsselung und Entschlüsselung von Daten auf dem Appliance-Node verwendet wird. Um eine gesamte Schlüssel-UID anzuzeigen, setzen Sie den Cursor über die Zelle. Ein Bindestrich (-) gibt an, dass die Schlüssel-UID unbekannt ist, möglicherweise wegen eines Verbindungsproblem zwischen dem Appliance-Node und dem KMS.
Status	Der Status der Verbindung zwischen dem KMS und dem Appliance-Node. Wenn der Knoten verbunden ist, wird der Zeitstempel alle 30 Minuten aktualisiert. Nach einer Änderung der KMS-Konfiguration kann es mehrere Minuten dauern, bis der Verbindungsstatus aktualisiert wird. Hinweis: Sie müssen Ihren Webbrowser aktualisieren, um die neuen Werte zu sehen.

4. Wenn in der Spalte Status ein KMS-Problem angezeigt wird, beheben Sie das Problem sofort.

Während normaler KMS-Vorgänge wird der Status **mit KMS** verbunden. Wenn ein Knoten von der Tabelle getrennt wird, wird der Verbindungsstatus des Knotens angezeigt (administrativ ausgefallen oder unbekannt).

Andere Statusmeldungen entsprechen StorageGRID Meldungen mit denselben Namen:

- KMS-Konfiguration konnte nicht geladen werden
- KMS-Verbindungsfehler
- DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden
- DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen
- KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
- KM ist nicht konfiguriert

Führen Sie die empfohlenen Aktionen für diese Warnmeldungen aus.



Sämtliche Probleme müssen sofort behoben werden, um einen vollständigen Schutz Ihrer Daten zu gewährleisten.

Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)

Möglicherweise müssen Sie die Konfiguration eines Schlüsselverwaltungsservers bearbeiten, z. B. wenn ein Zertifikat kurz vor dem Ablauf steht.

Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers](#)".
- Wenn Sie die für einen KMS ausgewählte Site aktualisieren möchten, haben Sie die geprüft "[Überlegungen für das Ändern des KMS für einen Standort](#)".
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Key Management Server an.

2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **actions > Edit**.

Sie können einen KMS auch bearbeiten, indem Sie den KMS-Namen in der Tabelle auswählen und auf der KMS-Detailseite **Bearbeiten** auswählen.

3. Aktualisieren Sie optional die Details in **Schritt 1 (KMS-Details)** des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers.

Feld	Beschreibung
KMS-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.

Feld	Beschreibung
Schlüsselname	<p>Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.</p> <p>In seltenen Fällen müssen Sie nur den Schlüsselnamen bearbeiten. Sie müssen beispielsweise den Schlüsselnamen bearbeiten, wenn der Alias im KMS umbenannt wird oder alle Versionen des vorherigen Schlüssels in die Versionsgeschichte des neuen Alias kopiert wurden.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Für StorageGRID müssen alle zuvor verwendeten Schlüsselversionen (sowie zukünftige Versionen) vom KMS mit demselben Schlüsselalias zugänglich sein. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.</p> <p>"Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"</p> </div>
Verwaltet Schlüssel für	<p>Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS haben, wählen Sie optional Sites Not Managed by another KMS (default KMS) aus. Diese Auswahl konvertiert ein standortspezifisches KMS in das Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben, und für alle Sites, die in einer Erweiterung hinzugefügt wurden.</p> <p>Hinweis: Wenn Sie eine Site-spezifische KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie das Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.</p>
Port	<p>Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.</p>
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.</p> <p>Hinweis: das Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.</p>

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers wird angezeigt.

6. Wenn Sie das Serverzertifikat ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neue Datei hoch.

7. Wählen Sie **Weiter**.

Schritt 3 (Client-Zertifikate hochladen) des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers wird angezeigt.

8. Wenn Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neuen Dateien hoch.

9. Wählen Sie **Test und Speichern**.

Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und allen Node-verschlüsselten Appliance-Nodes an den betroffenen Standorten werden getestet. Wenn alle Knotenverbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

10. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails, und wählen Sie **OK**.

Sie können beispielsweise einen Fehler bei der nicht verarbeitbaren Einheit von 422 erhalten, wenn die für diesen KMS ausgewählte Site bereits von einem anderen KMS verwaltet wird oder wenn ein Verbindungstest fehlgeschlagen ist.

11. Wenn Sie die aktuelle Konfiguration speichern müssen, bevor Sie die Verbindungsfehler beheben, wählen Sie **Speichern erzwingen**.



Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

Die KMS-Konfiguration wird gespeichert.

12. Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.

Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

Entfernen eines Verschlüsselungsmanagement-Servers (KMS)

In einigen Fällen möchten Sie einen Schlüsselverwaltungsserver entfernen. Sie können beispielsweise einen standortspezifischen KMS entfernen, wenn Sie den Standort deaktiviert haben.

Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers](#)".
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

In diesen Fällen können Sie einen KMS entfernen:

- Wenn der Standort außer Betrieb genommen wurde oder wenn der Standort keine Appliance-Nodes mit aktivierter Node-Verschlüsselung enthält, können Sie einen standortspezifischen KMS entfernen.
- Der Standard-KMS kann entfernt werden, wenn für jeden Standort bereits ein standortspezifischer KMS vorhanden ist, bei dem Appliance-Nodes mit aktivierter Node-Verschlüsselung vorhanden sind.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Key Management Server an.

2. Wählen Sie den KMS aus, den Sie entfernen möchten, und wählen Sie **Aktionen > Entfernen**.

Sie können KMS auch entfernen, indem Sie den KMS-Namen in der Tabelle auswählen und auf der KMS-Detailseite **Entfernen** auswählen.

3. Bestätigen Sie, dass Folgendes zutrifft:

- Sie entfernen ein standortspezifisches KMS für einen Standort, der keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
- Sie entfernen den Standard-KMS, aber für jeden Standort mit Knotenverschlüsselung ist bereits ein standortspezifisches KMS vorhanden.

4. Wählen Sie **Ja**.

Die KMS-Konfiguration wurde entfernt.

Proxy-Einstellungen verwalten

Konfigurieren Sie Speicher-Proxy-Einstellungen

Wenn Sie Plattform-Services oder Cloud Storage-Pools verwenden, können Sie einen nicht transparenten Proxy zwischen Storage Nodes und den externen S3-Endpunkten konfigurieren. Beispielsweise benötigen Sie einen nicht transparenten Proxy, um Meldungen von Plattformdiensten an externe Endpunkte, z. B. einen Endpunkt im Internet, zu senden.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

Sie können die Einstellungen für einen einzelnen Speicherproxy konfigurieren.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Proxy-Einstellungen**.

Die Seite Speicher-Proxy-Einstellungen wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.

Proxy Settings
Storage
Admin

2. Aktivieren Sie das Kontrollkästchen **Speicher-Proxy aktivieren**.

Die Felder zum Konfigurieren eines Speicher-Proxys werden angezeigt.

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy

Protocol HTTP SOCKS5

Hostname

Port (optional)

3. Wählen Sie das Protokoll für den nicht-transparenten Speicher-Proxy aus.
4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie optional den Port ein, der für die Verbindung mit dem Proxyserver verwendet wird.

Sie können dieses Feld leer lassen, wenn Sie den Standardport für das Protokoll verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. Wählen Sie **Speichern**.

Nach dem Speichern des Storage-Proxy können neue Endpunkte für Plattformservices oder Cloud-Storage-Pools konfiguriert und getestet werden.



Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

7. Überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass für den Plattformdienst bezogene Nachrichten von StorageGRID nicht blockiert werden.

Nachdem Sie fertig sind

Wenn Sie einen Speicher-Proxy deaktivieren müssen, deaktivieren Sie das Kontrollkästchen **Speicher-Proxy aktivieren**, und wählen Sie **Speichern** aus.

Verwandte Informationen

- ["Netzwerk und Ports für Plattformservices"](#)
- ["Objektmanagement mit ILM"](#)

Konfigurieren Sie die Administrator-Proxy-Einstellungen

Wenn Sie AutoSupport-Meldungen über HTTP oder HTTPS senden (siehe ["Konfigurieren"](#)

Sie AutoSupport") Können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und technischem Support (AutoSupport) konfigurieren.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

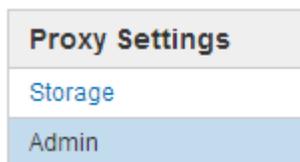
Sie können die Einstellungen für einen einzigen Admin-Proxy konfigurieren.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Proxy-Einstellungen**.

Die Seite Admin Proxy Settings wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.

2. Wählen Sie im Sidebar-Menü die Option **Admin**.



3. Aktivieren Sie das Kontrollkästchen **Admin-Proxy aktivieren**.

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy

Hostname

Port

Username (optional)

Password (optional)

4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie den Port ein, der für die Verbindung mit dem Proxy-Server verwendet wird.
6. Geben Sie optional den Proxy-Benutzernamen ein.

Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server keinen Benutzernamen benötigt.

7. Geben Sie optional das Proxy-Kennwort ein.

Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server kein Passwort benötigt.

8. Wählen Sie **Speichern**.

Nachdem der Admin-Proxy gespeichert wurde, wird der Proxy-Server zwischen Admin-Nodes und dem technischen Support konfiguriert.



Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

9. Wenn Sie den Proxy deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Admin Proxy aktivieren**, und wählen Sie **Save** aus.

Kontrollieren Sie Firewalls

Kontrolle des Zugriffs über externe Firewall

Sie können bestimmte Ports an der externen Firewall öffnen oder schließen.

Sie können den Zugriff auf die Benutzeroberflächen und APIs auf StorageGRID-Administratorknoten steuern, indem Sie bestimmte Ports an der externen Firewall öffnen oder schließen. Beispielsweise möchten Sie verhindern, dass Mandanten sich an der Firewall mit dem Grid Manager verbinden können, und zwar zusätzlich über andere Methoden zur Steuerung des Systemzugriffs.

Informationen zum Konfigurieren der internen StorageGRID-Firewall finden Sie unter "[Konfigurieren Sie die interne Firewall](#)".

Port	Beschreibung	Port offen...
443	Standard-HTTPS-Port für Admin-Nodes	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Mandanten-Manager und die Mandanten-Management-API zugreifen. Hinweis: Port 443 wird auch für einen internen Verkehr genutzt.
8443	Eingeschränkter Grid Manager-Port an Admin-Nodes	<ul style="list-style-type: none">• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Grid Manager und die Grid Management API zugreifen.• Webbrowser und Management-API-Clients können nicht auf den Tenant Manager oder die Mandanten-Management-API zugreifen.• Anfragen nach internen Inhalten werden abgelehnt.

Port	Beschreibung	Port offen...
9443	Eingeschränkter Mandantenmanager-Port an Admin-Nodes	<ul style="list-style-type: none"> • Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Mandanten-Manager und die Mandanten-Management-API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid-Management-API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.



Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

Verwandte Informationen

- ["Melden Sie sich beim Grid Manager an"](#)
- ["Erstellen eines Mandantenkontos"](#)
- ["Externe Kommunikation"](#)

Interne Firewall-Kontrollen verwalten

StorageGRID verfügt über eine interne Firewall auf jedem Node, die die Sicherheit Ihres Grids erhöht, indem Sie den Netzwerkzugriff auf den Node kontrollieren können. Verwenden Sie die Firewall, um den Netzwerkzugriff auf allen Ports zu verhindern, außer den für Ihre spezifische Grid-Bereitstellung erforderlichen Ports. Die Konfigurationsänderungen, die Sie auf der Seite Firewall-Steuerung vornehmen, werden für jeden Knoten bereitgestellt.

Verwenden Sie die drei Registerkarten auf der Seite „Firewall-Steuerung“, um den für Ihr Raster erforderlichen Zugriff anzupassen.

- **Privilegierte Adressliste:** Verwenden Sie diese Registerkarte, um ausgewählten Zugriff auf geschlossene Ports zu ermöglichen. Sie können IP-Adressen oder Subnetze in CIDR-Notation hinzufügen, die über die Registerkarte externen Zugriff managen auf geschlossene Ports zugreifen können.
- **Externen Zugriff verwalten:** Verwenden Sie diese Registerkarte, um Ports zu schließen, die standardmäßig geöffnet sind, oder um zuvor geschlossene Ports wieder zu öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk:** Verwenden Sie diese Registerkarte, um anzugeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut.

Auf dieser Registerkarte können Sie auch zusätzliche Ports angeben, die geöffnet werden sollen, wenn das nicht vertrauenswürdige Clientnetzwerk konfiguriert ist. Diese Ports können Zugriff auf den Grid Manager, den Tenant Manager oder beide ermöglichen.

Die Einstellungen auf dieser Registerkarte überschreiben die Einstellungen auf der Registerkarte externen Zugriff verwalten.

- Ein Knoten mit einem nicht vertrauenswürdigen Client-Netzwerk akzeptiert nur Verbindungen auf den

an diesem Knoten konfigurierten Load-Balancer-Endpunktports (global, Knotenschnittstelle und Knotentyp gebundene Endpunkte).

- Zusätzliche Ports, die auf der Registerkarte nicht vertrauenswürdiger Client-Netzwerk geöffnet werden, sind in allen nicht vertrauenswürdigen Client-Netzwerken geöffnet, auch wenn keine Load Balancer-Endpunkte konfiguriert sind.
- Load Balancer-Endpunkt-Ports und ausgewählte zusätzliche Ports *sind die einzigen offenen Ports* in nicht vertrauenswürdigen Client-Netzwerken, unabhängig von den Einstellungen auf der Registerkarte Externe Netzwerke verwalten.
- Wenn vertrauenswürdig, sind alle Ports, die auf der Registerkarte externen Zugriff managen geöffnet sind, sowie alle im Client-Netzwerk geöffneten Load Balancer-Endpunkte zugänglich.



Die Einstellungen, die Sie auf einer Registerkarte vornehmen, können sich auf die Zugriffsänderungen auswirken, die Sie auf einer anderen Registerkarte vornehmen. Überprüfen Sie die Einstellungen auf allen Registerkarten, um sicherzustellen, dass sich Ihr Netzwerk wie erwartet verhält.

Informationen zum Konfigurieren der internen Firewall-Steuerelemente finden Sie unter "[Konfigurieren Sie die Firewall-Steuerelemente](#)".

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter "[Kontrolle des Zugriffs über externe Firewall](#)".

Liste privilegierter Adressen und Verwaltung externer Zugriffsregisterkarten

Auf der Registerkarte Liste der privilegierten Adressen können Sie eine oder mehrere IP-Adressen registrieren, denen Zugriff auf geschlossene Grid-Ports gewährt wird. Auf der Registerkarte externen Zugriff verwalten können Sie den externen Zugriff auf ausgewählte externe Ports oder alle offenen externen Ports schließen (externe Ports sind Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können). Diese beiden Registerkarten können häufig zusammen verwendet werden, um den genauen Netzwerkzugriff anzupassen, den Sie für Ihr Raster benötigen.



Privilegierte IP-Adressen haben standardmäßig keinen internen Grid-Port-Zugriff.

Beispiel 1: Verwenden Sie einen Jump-Host für Wartungsaufgaben

Angenommen, Sie möchten einen Jump-Host (einen sicherheitsgesicherten Host) für die Netzwerkadministration verwenden. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um die IP-Adresse des Jump-Hosts hinzuzufügen.
2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.



Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie Ihre Konfiguration gespeichert haben, werden alle externen Ports auf dem Admin-Knoten in Ihrem Grid für alle Hosts außer dem Jump-Host gesperrt. Sie können dann den Jump-Host verwenden, um Wartungsarbeiten am Grid sicherer durchzuführen.

Beispiel 2: Beschränken Sie den Zugriff auf den Grid-Manager und den Tenant Manager

Angenommen, Sie möchten den Zugriff auf den Grid-Manager und den Mandantenmanager aus Sicherheitsgründen einschränken. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 443 zu blockieren.
2. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 8443 zu ermöglichen.
3. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 9443 zu ermöglichen.

Nachdem Sie Ihre Konfiguration gespeichert haben, können Hosts nicht auf Port 443 zugreifen, aber sie können dennoch über Port 8443 und den Tenant Manager über Port 9443 auf den Grid Manager zugreifen.

Beispiel 3: Sperren sensibler Ports

Angenommen, Sie möchten sensible Ports und den Dienst auf diesem Port sperren (z. B. SSH an Port 22). Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um nur den Hosts Zugriff zu gewähren, die Zugriff auf den Dienst benötigen.
2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.



Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie die Konfiguration gespeichert haben, stehen den Hosts auf der Liste der privilegierten Adressen Port 22 und SSH-Dienst zur Verfügung. Allen anderen Hosts wird der Zugriff auf den Dienst verweigert, unabhängig davon, von welcher Schnittstelle die Anforderung stammt.

Beispiel 4: Deaktivieren Sie den Zugriff auf nicht verwendete Dienste

Auf Netzwerkebene können Sie einige Dienste deaktivieren, die Sie nicht verwenden möchten. Wenn Sie beispielsweise keinen Swift-Zugriff bereitstellen, führen Sie die folgenden allgemeinen Schritte aus:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18083 zu blockieren.
2. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18085 zu blockieren.

Nachdem Sie die Konfiguration gespeichert haben, lässt der Storage Node die Swift-Konnektivität nicht mehr zu, erlaubt aber weiterhin den Zugriff auf andere Dienste auf nicht blockierten Ports.

Registerkarte nicht vertrauenswürdige Client-Netzwerke

Wenn Sie ein Clientnetzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Clientverkehr nur an explizit konfigurierten Endpunkten oder zusätzlichen Ports akzeptieren, die Sie auf dieser Registerkarte auswählen.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *Trusted*. Das heißt, standardmäßig vertraut

StorageGRID eingehende Verbindungen zu jedem Grid-Knoten auf allen "[Verfügbare externe Ports](#)".

Sie können die Bedrohung durch feindliche Angriffe auf Ihrem StorageGRID-System verringern, indem Sie angeben, dass das Client-Netzwerk auf jedem Knoten *unvertrauenswürdig* ist. Wenn das Client-Netzwerk eines Knotens nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind, und alle zusätzlichen Ports, die Sie über die Registerkarte nicht vertrauenswürdiges Client-Netzwerk auf der Seite Firewall-Steuerung festlegen. Siehe "[Konfigurieren von Load Balancer-Endpunkten](#)" Und "[Konfigurieren Sie die Firewall-Steuerelemente](#)".

Beispiel 1: Der Gateway-Node akzeptiert nur HTTPS-S3-Anforderungen

Angenommen, ein Gateway-Node soll den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anforderungen ablehnen. Sie würden folgende allgemeine Schritte durchführen:

1. Von "[Load Balancer-Endpunkte](#)" Konfigurieren Sie einen Load Balancer-Endpunkt für S3 über HTTPS an Port 443.
2. Wählen Sie auf der Seite Firewall-Steuerung die Option nicht vertrauenswürdig aus, um anzugeben, dass das Client-Netzwerk auf dem Gateway-Knoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, wird der gesamte eingehende Datenverkehr im Client-Netzwerk des Gateway-Knotens außer HTTPS-S3-Anfragen auf Port 443- und ICMP-Echo-(Ping-)Anfragen verworfen.

Beispiel 2: Storage-Node sendet Anforderungen von S3-Plattform-Services

Angenommen, Sie möchten den ausgehenden Datenverkehr der S3-Plattformdienste von einem Storage-Node aktivieren, möchten jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Registerkarte nicht vertrauenswürdige Client-Netzwerke der Seite Firewall-Steuerung an, dass das Client-Netzwerk auf dem Storage Node nicht vertrauenswürdig ist.

Nachdem Sie die Konfiguration gespeichert haben, akzeptiert der Storage Node keinen eingehenden Datenverkehr mehr im Client-Netzwerk, erlaubt jedoch weiterhin ausgehende Anfragen an konfigurierte Plattformdienstziele.

Beispiel 3: Zugriff auf Grid Manager auf ein Subnetz beschränken

Angenommen, Sie möchten den Zugriff des Grid-Managers nur auf ein bestimmtes Subnetz zulassen. Führen Sie die folgenden Schritte aus:

1. Verbinden Sie das Client-Netzwerk Ihrer Admin-Knoten mit dem Subnetz.
2. Verwenden Sie die Registerkarte nicht vertrauenswürdiges Clientnetzwerk, um das Clientnetzwerk als nicht vertrauenswürdig zu konfigurieren.
3. Fügen Sie im Abschnitt **zusätzliche Ports auf nicht vertrauenswürdigem Client-Netzwerk öffnen** der Registerkarte Port 443 oder 8443 hinzu.
4. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle externen Ports zu blockieren (mit oder ohne privilegierte IP-Adressen für Hosts außerhalb dieses Subnetzes).

Nachdem Sie die Konfiguration gespeichert haben, können nur Hosts in dem von Ihnen angegebenen Subnetz auf den Grid Manager zugreifen. Alle anderen Hosts sind blockiert.

Konfigurieren Sie die interne Firewall

Sie können die StorageGRID Firewall konfigurieren, um den Netzwerkzugriff auf bestimmte Ports auf Ihren StorageGRID Nodes zu steuern.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Das ist schon ["Bestimmte Zugriffsberechtigungen"](#).
- Sie haben die Informationen in geprüft ["Management der Firewall-Kontrollen"](#) Und ["Netzwerkrichtlinien"](#).
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.



Wenn Sie die Konfiguration des Client-Netzwerks ändern, können bestehende Clientverbindungen fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Über diese Aufgabe

StorageGRID verfügt über eine interne Firewall auf jedem Node, über die Sie einige Ports an den Nodes des Grids öffnen oder schließen können. Sie können die Registerkarten für die Firewall-Steuerung verwenden, um Ports zu öffnen oder zu schließen, die standardmäßig im Grid-Netzwerk, im Admin-Netzwerk und im Client-Netzwerk geöffnet sind. Sie können auch eine Liste mit privilegierten IP-Adressen erstellen, die auf gesperrte Grid-Ports zugreifen können. Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut, und Sie können den Zugriff bestimmter Ports auf dem Client-Netzwerk konfigurieren.

Die Beschränkung der Anzahl der offenen Ports auf IP-Adressen außerhalb Ihres Grids auf nur die absolut notwendigen Ports erhöht die Sicherheit Ihres Grids. Mithilfe der Einstellungen auf den drei Registerkarten für die Firewall-Steuerung stellen Sie sicher, dass nur die erforderlichen Ports geöffnet sind.

Weitere Informationen zur Verwendung von Firewall-Kontrollen, einschließlich Beispiele, finden Sie unter ["Management der Firewall-Kontrollen"](#).

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter ["Kontrolle des Zugriffs über externe Firewall"](#).

Firewall-Kontrollen für den Zugriff

Schritte

1. Wählen Sie **CONFIGURATION > Security > Firewall Control**.

Die drei Registerkarten auf dieser Seite werden unter beschrieben ["Management der Firewall-Kontrollen"](#).

2. Wählen Sie eine beliebige Registerkarte aus, um die Firewall-Steuerelemente zu konfigurieren.

Sie können diese Registerkarten in beliebiger Reihenfolge verwenden. Die Konfigurationen, die Sie auf einer Registerkarte festlegen, beschränken nicht, was Sie auf den anderen Registerkarten tun können. Konfigurationsänderungen, die Sie auf einer Registerkarte vornehmen, können jedoch das Verhalten der auf anderen Registerkarten konfigurierten Ports ändern.

Liste privilegierter Adressen

Sie verwenden die Registerkarte Liste der privilegierten Adressen, um Hosts Zugriff auf Ports zu gewähren, die standardmäßig geschlossen oder durch Einstellungen auf der Registerkarte externen Zugriff verwalten geschlossen sind.

Privilegierte IP-Adressen und Subnetze haben standardmäßig keinen internen Grid-Zugriff. Zudem sind die Load Balancer-Endpunkte und zusätzliche Ports, die auf der Registerkarte „privilegierte Adressen“ geöffnet wurden, auch dann verfügbar, wenn sie auf der Registerkarte „externen Zugriff verwalten“ gesperrt sind.



Einstellungen auf der Registerkarte „Liste privilegierter Adressen“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdigen Clientnetzwerk“ nicht außer Kraft setzen.

Schritte

1. Geben Sie auf der Registerkarte Liste der privilegierten Adressen die Adresse oder das IP-Subnetz ein, die Sie Zugriff auf geschlossene Ports gewähren möchten.
2. Wählen Sie optional **Add another IP address or subnet in CIDR Notation** aus, um weitere privilegierte Clients hinzuzufügen.



Fügen Sie so wenig Adressen wie möglich zur Liste der privilegierten Adressen hinzu.

3. Wählen Sie optional **privilegierten IP-Adressen erlauben, auf interne StorageGRID-Ports zuzugreifen**. Siehe "[Interne StorageGRID-Ports](#)".



Diese Option entfernt einige Schutzmaßnahmen für interne Dienste. Lassen Sie sie nach Möglichkeit deaktiviert.

4. Wählen Sie **Speichern**.

Management des externen Zugriffs

Wenn ein Port auf der Registerkarte externen Zugriff verwalten geschlossen wird, kann keine IP-Adresse ohne Grid auf den Port zugegriffen werden, es sei denn, Sie fügen die IP-Adresse der Liste privilegierter Adressen hinzu. Sie können nur Ports schließen, die standardmäßig geöffnet sind, und Sie können nur Ports öffnen, die Sie geschlossen haben.



Einstellungen auf der Registerkarte „externen Zugriff verwalten“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdigen Clientnetzwerk“ nicht außer Kraft setzen. Wenn ein Knoten beispielsweise nicht vertrauenswürdig ist, wird Port SSH/22 im Client-Netzwerk gesperrt, selbst wenn er auf der Registerkarte externen Zugriff verwalten geöffnet ist. Die Einstellungen auf der Registerkarte nicht vertrauenswürdiger Client-Netzwerk überschreiben geschlossene Ports (z. B. 443, 8443, 9443) im Client-Netzwerk.

Schritte

1. Wählen Sie **externen Zugriff verwalten**. Auf der Registerkarte wird eine Tabelle mit allen externen Ports (Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können) für die Nodes in Ihrem Grid angezeigt.
2. Konfigurieren Sie die Ports, die geöffnet und geschlossen werden sollen, mithilfe der folgenden Optionen:
 - Verwenden Sie den Umschalter neben jedem Port, um den ausgewählten Port zu öffnen oder zu schließen.
 - Wählen Sie **Alle angezeigten Ports öffnen**, um alle in der Tabelle aufgeführten Ports zu öffnen.

- Wählen Sie **Alle angezeigten Ports schließen**, um alle in der Tabelle aufgeführten Ports zu schließen.



Wenn Sie die Grid-Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port verbunden sind, einschließlich Ihnen, den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.



Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Ports angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für einen externen Port zu finden, indem Sie eine Portnummer eingeben. Sie können einen Teil der Portnummer eingeben. Wenn Sie beispielsweise einen **2** eingeben, werden alle Ports angezeigt, die den String "2" als Teil ihres Namens haben.

3. Wählen Sie **Speichern**

Nicht Vertrauenswürdiges Client-Netzwerk

Wenn das Client-Netzwerk für einen Knoten nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehenden Datenverkehr an Ports, die als Load Balancer-Endpunkte konfiguriert sind, und optional zusätzliche Ports, die Sie auf dieser Registerkarte auswählen. Auf dieser Registerkarte können Sie auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt wurden.



Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Die Konfigurationsänderungen, die Sie auf der Registerkarte **nicht vertrauenswürdiges Client-Netzwerk** vornehmen, überschreiben die Einstellungen auf der Registerkarte **externen Zugriff verwalten**.

Schritte

1. Wählen Sie **Nicht Vertrauenswürdiges Client-Netzwerk**.
2. Geben Sie im Abschnitt „Standard für neuen Knoten festlegen“ an, welche Standardeinstellung verwendet werden soll, wenn in einem Erweiterungsverfahren neue Knoten zum Raster hinzugefügt werden.
 - **Trusted** (Standard): Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird sein Client-Netzwerk vertrauenswürdig.
 - **UnTrusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig.

Bei Bedarf können Sie zu dieser Registerkarte zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.



Diese Einstellung hat keine Auswirkung auf die vorhandenen Nodes im StorageGRID System.

3. Verwenden Sie die folgenden Optionen, um die Knoten auszuwählen, die Clientverbindungen nur an explizit konfigurierten Endpunkten des Lastausgleichs oder zusätzlichen ausgewählten Ports zulassen sollen:
 - Wählen Sie **Untrust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten zur Liste UnTrusted Client Network hinzuzufügen.
 - Wählen Sie **Trust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten aus der Liste

UnTrusted Client Network zu entfernen.

- Verwenden Sie den Umschalter neben den einzelnen Ports, um das Client-Netzwerk für den ausgewählten Knoten als vertrauenswürdig oder nicht vertrauenswürdig festzulegen.

Sie können beispielsweise **Untrust on displayed Nodes** auswählen, um alle Knoten zur Liste UnTrusted Client Network hinzuzufügen, und dann den Umschalter neben einem einzelnen Knoten verwenden, um diesen einzelnen Knoten zur Liste Trusted Client Network hinzuzufügen.



Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Knoten angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für jeden Knoten durch Eingabe des Knotennamens zu suchen. Sie können einen Teilnamen eingeben. Wenn Sie beispielsweise einen **GW** eingeben, werden alle Knoten angezeigt, die den String "GW" als Teil ihres Namens haben.

4. Wählen Sie optional alle zusätzlichen Ports aus, die im nicht vertrauenswürdigem Client-Netzwerk geöffnet werden sollen. Diese Ports können Zugriff auf den Grid Manager, den Tenant Manager oder beide ermöglichen.

Sie können z. B. mit dieser Option sicherstellen, dass der Grid-Manager im Client-Netzwerk zu Wartungszwecken aufgerufen werden kann.



Diese zusätzlichen Ports sind im Client-Netzwerk geöffnet, unabhängig davon, ob sie auf der Registerkarte externen Zugriff verwalten geschlossen sind.

5. Wählen Sie **Speichern**.

Die neuen Firewall-Einstellungen werden sofort angewendet und durchgesetzt. Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Verwalten von Mandanten

Mandanten managen: Übersicht

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3 und Swift-Clients zum Speichern und Abrufen von Objekten verwenden.



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Was sind Mandantenkonten?

Ein Mandantenkonto ermöglicht Ihnen, entweder die Simple Storage Service (S3) REST-API oder die Swift REST-API zu verwenden, um Objekte in einem StorageGRID System zu speichern und abzurufen.

Jedes Mandantenkonto verfügt über föderierte oder lokale Gruppen, Benutzer, S3 Buckets oder Swift Container und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte durch verschiedene Einheiten zu trennen. Beispielsweise können für einen der folgenden Anwendungsfälle mehrere Mandantenkonten verwendet werden:

- **Anwendungsbeispiel für Unternehmen:** Wenn Sie ein StorageGRID-System in einer Enterprise-

Anwendung verwalten, sollten Sie den Objekt-Storage des Grid möglicherweise von den verschiedenen Abteilungen Ihres Unternehmens trennen. In diesem Fall können Sie Mandantenkonten für die Marketingabteilung, die Kundenbetreuung, die Personalabteilung usw. erstellen.



Wenn Sie das S3-Client-Protokoll verwenden, können Sie S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen eines Unternehmens zu trennen. Sie müssen keine Mandantenkonten verwenden. Siehe Anweisungen zur Implementierung "[S3-Buckets und Bucket-Richtlinien](#)" Finden Sie weitere Informationen.

- **Anwendungsbeispiel Service Provider:** Wenn Sie ein StorageGRID-System als Service-Provider verwalten, können Sie den Objekt-Storage des Grid durch die verschiedenen Entitäten verteilen, die den Storage auf Ihrem Grid leasen. In diesem Fall würden Sie Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. erstellen.

Weitere Informationen finden Sie unter "[Verwenden Sie ein Mandantenkonto](#)".

Wie erstelle ich ein Mandantenkonto?

Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Grundlegende Informationen, einschließlich Mandantename, Client-Typ (S3 oder Swift) und optionalem Storage-Kontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformservices verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Verbundverbindung verwenden kann.
- Der erste Root-Zugriff für den Mandanten basiert darauf, ob das StorageGRID System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign On (SSO) verwendet.

Darüber hinaus können Sie die S3-Objektsperre für das StorageGRID-System aktivieren, wenn S3-Mandantenkonten gesetzliche Vorgaben erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und managen.

Wofür wird Tenant Manager verwendet?

Nachdem Sie das Mandantenkonto erstellt haben, können sich Mandantenbenutzer beim Tenant Manager anmelden, um Aufgaben wie die folgenden auszuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Grid-Verbund für Account-Klone und Grid-übergreifende Replizierung verwenden
- Managen von S3-Zugriffsschlüsseln
- S3 Buckets erstellen und managen
- Verwenden Sie S3-Plattformservices
- Verwenden Sie S3 Select
- Monitoring der Storage-Auslastung



Benutzer von S3-Mandanten können mit dem Tenant Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen, müssen jedoch Objekte mit einer S3-Client-Applikation aufnehmen und managen. Siehe "[S3-REST-API VERWENDEN](#)" Entsprechende Details.



Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Berechtigung Root-Zugriff erlaubt Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

Erstellen Sie ein Mandantenkonto

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Storage in Ihrem StorageGRID-System zu kontrollieren.

Die Schritte zum Erstellen eines Mandantenkontos variieren je nachdem, ob ["Identitätsföderation"](#) und ["Single Sign On"](#) sind konfiguriert und ob das Grid Manager-Konto, das Sie zum Erstellen des Mandantenkontos verwenden, einer Admin-Gruppe mit Root-Zugriffsberechtigung angehört.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie verfügen über die Berechtigung Root-Zugriff oder Mandantenkonten.
- Wenn das Mandantenkonto die für den Grid Manager konfigurierte Identitätsquelle verwendet und Sie einer föderierten Gruppe Root-Zugriffsberechtigungen für das Mandantenkonto gewähren möchten, haben Sie diese föderierte Gruppe in den Grid Manager importiert. Sie müssen dieser Administratorgruppe keine Grid Manager-Berechtigungen zuweisen. Siehe ["Managen von Admin-Gruppen"](#).
- Wenn Sie einem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in einem anderen Grid über eine Grid-Federation-Verbindung ermöglichen möchten:
 - Das ist schon ["Grid Federation-Verbindung konfiguriert"](#).
 - Der Status der Verbindung lautet **connected**.
 - Sie haben Root-Zugriffsberechtigung.
 - Sie haben die Überlegungen für überprüft ["Verwalten der zulässigen Mandanten für den Grid-Verbund"](#).
 - Wenn das Mandantenkonto die Identitätsquelle verwendet, die für Grid Manager konfiguriert wurde, haben Sie dieselbe Verbundgruppe in Grid Manager auf beiden Grids importiert.

Wenn Sie den Mandanten erstellen, wählen Sie diese Gruppe aus, um die anfängliche Root-Zugriffsberechtigung für die Quell- und Zielmandantenkonten zu erhalten.



Wenn diese Administratorgruppe vor dem Erstellen des Mandanten nicht auf beiden Grids vorhanden ist, wird der Mandant nicht am Ziel repliziert.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen**.

Geben Sie Details ein

Schritte

1. Geben Sie Details für die Serviceeinheit ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, 20-stellige Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten. Wenn Sie einen Mandanten erstellen, der eine Grid-Federation-Verbindung verwendet, können Sie optional mithilfe dieses Felds ermitteln, welcher der Quell-Tenant ist und welcher der Zielmandant ist. Beispielsweise wird diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den Mandanten angezeigt, der in Grid 2 repliziert wurde: „Dieser Mandant wurde in Grid 1 erstellt.“
Client-Typ	Der Typ des Client-Protokolls, das dieser Mandant verwendet, entweder S3 oder Swift . Hinweis: Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.
Storage-Kontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent, einen numerischen Wert für das Kontingent und die Einheiten verfügt.

2. Wählen Sie **Weiter**.

Wählen Sie Berechtigungen aus

Schritte

1. Wählen Sie optional alle Berechtigungen aus, die dieser Tenant haben soll.



Einige dieser Berechtigungen haben zusätzliche Anforderungen. Für Details wählen Sie das Hilfesymbol für jede Berechtigung aus.

Berechtigung	Wenn ausgewählt...
Unterstützung von Plattform-Services	Der Mandant kann S3-Plattformservices wie CloudMirror verwenden. Siehe "Management von Plattform-Services für S3-Mandantenkonten" .
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für verbundene Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie dies haben "SSO konfiguriert" Für Ihr StorageGRID-System.
S3 Select zulassen	Der Mandant kann S3 SelectObjectContent API-Anforderungen ausgeben, um Objektdaten zu filtern und abzurufen. Siehe "Management von S3 Select für Mandantenkonten" . Wichtig: SelectObjectContent Requests können die Load Balancer Performance für alle S3 Clients und alle Tenants verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Berechtigung	Wenn ausgewählt...
Netzverbundverbindung verwenden	<p>Der Mandant kann eine Grid Federation-Verbindung verwenden.</p> <p>Auswahl dieser Option:</p> <ul style="list-style-type: none"> • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer aus diesem Raster (das <i>source Grid</i>) in das andere Raster der ausgewählten Verbindung (das <i>Destination Grid</i>) geklont werden. • Ermöglicht diesem Mandanten, die Grid-übergreifende Replizierung zwischen entsprechenden Buckets in jedem Grid zu konfigurieren. <p>Siehe "Verwalten Sie die zulässigen Mandanten für den Grid-Verbund".</p> <p>Hinweis: Sie können nur Grid Federation connection verwenden auswählen, wenn Sie einen neuen S3-Mandanten erstellen; Sie können diese Berechtigung nicht für einen vorhandenen Mandanten auswählen.</p>

2. Wenn Sie **Grid Federation connection** verwenden ausgewählt haben, wählen Sie eine der verfügbaren Grid Federation-Verbindungen aus.

Use grid federation connection ?

Connection name ? ⇅	Remote grid hostname ? ⇅	Connection status ? ⇅
Grid A-Grid B	10.96.104.230	Connected

3. Wählen Sie **Weiter**.

Root-Zugriff definieren und Mandanten erstellen

Schritte

1. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System Identitätsföderation, Single Sign-On (SSO) oder beides verwendet.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	<ol style="list-style-type: none"> Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.

Option	Tun Sie das
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

2. Wählen Sie **Create Tenant**.

Eine Erfolgsmeldung wird angezeigt, und die neue Serviceeinheit wird auf der Seite „Serviceeinheiten“ aufgeführt. Informationen zum Anzeigen von Mandantendetails und zum Überwachen der Mandantenaktivität finden Sie unter ["Überwachen Sie die Mandantenaktivität"](#).

3. Wenn Sie die Berechtigung **Grid Federation connection** für den Mieter verwenden ausgewählt haben:

- Vergewissern Sie sich, dass ein identischer Mandant auf das andere Grid in der Verbindung repliziert wurde. Die Mandanten in beiden Grids haben die gleiche 20-stellige Konto-ID, den gleichen Namen, die gleiche Beschreibung, das gleiche Kontingent und die gleichen Berechtigungen.



Wenn die Fehlermeldung „Tenant created without a Clone,“ angezeigt wird, lesen Sie die Anweisungen in ["Fehler beim Grid-Verbund beheben"](#).

- Wenn Sie beim Definieren des Root-Zugriffs ein lokales Root-Benutzerpasswort angegeben haben, ["Ändern Sie das Passwort für den lokalen Root-Benutzer"](#) Für den replizierten Mandanten.



Ein lokaler Root-Benutzer kann sich erst bei Tenant Manager im Zielraster anmelden, wenn das Passwort geändert wurde.

Beim Mandanten anmelden (optional)

Sie können sich nach Bedarf jetzt beim neuen Mandanten anmelden, um die Konfiguration abzuschließen, oder sich später beim Mandanten anmelden. Die Schritte zur Anmeldung hängen davon ab, ob Sie über den Standardport (443) oder einen eingeschränkten Port beim Grid Manager angemeldet sind. Siehe ["Kontrolle des Zugriffs über externe Firewall"](#).

Jetzt anmelden

Sie verwenden...	Tun Sie das...
Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	<ol style="list-style-type: none"> Wählen Sie als root anmelden. Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets, Identitätsverbänden, Gruppen und Benutzern angezeigt. Wählen Sie die Links aus, um das Mandantenkonto zu konfigurieren. Jeder Link öffnet die entsprechende Seite im Tenant Manager. Informationen zum Ausfüllen der Seite finden Sie im "Anweisungen zur Verwendung von Mandantenkonten".

Sie verwenden...	Tun Sie das...
Port 443 und Sie haben kein Passwort für den lokalen Root-Benutzer festgelegt	Wählen Sie Anmelden , und geben Sie die Anmeldeinformationen für einen Benutzer in der Gruppe Root Access Federated ein.
Ein eingeschränkter Port	<ol style="list-style-type: none"> 1. Wählen Sie Fertig Stellen 2. Wählen Sie eingeschränkt in der Tabelle Tenant aus, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren. <p>Die URL für den Tenant Manager weist folgendes Format auf:</p> <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ <i>port</i> Ist der reine Mandantenport ◦ <i>20-digit-account-id</i> Die eindeutige Account-ID des Mandanten

Melden Sie sich später an

Sie verwenden...	Führen Sie eine dieser...
Port 443	<ul style="list-style-type: none"> • Wählen Sie im Grid Manager MIETERS aus und wählen Sie Anmelden rechts neben dem Mieternamen aus. • Geben Sie die URL des Mandanten in einen Webbrowser ein: <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ <i>20-digit-account-id</i> Die eindeutige Account-ID des Mandanten
Ein eingeschränkter Port	<ul style="list-style-type: none"> • Wählen Sie im Grid Manager die Option MITERS aus, und wählen Sie eingeschränkt. • Geben Sie die URL des Mandanten in einen Webbrowser ein: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ <i>port</i> Ist der ausschließlich auf Mandanten beschränkte Port ◦ <i>20-digit-account-id</i> Die eindeutige Account-ID des Mandanten

Konfigurieren Sie den Mandanten

Befolgen Sie die Anweisungen unter "[Verwenden Sie ein Mandantenkonto](#)" Zum Management von Mandantengruppen und -Benutzern managen Sie S3-Zugriffsschlüssel, Buckets, Plattform-Services sowie Konto-Klone und Grid-Replizierung.

Mandantenkonto bearbeiten

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen, das Speicherkontingent oder die Berechtigungen für Mandanten zu ändern.



Wenn ein Mandant über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Mandantendetails von beiden Rastergittern in der Verbindung bearbeiten. Änderungen, die Sie an einem Raster in der Verbindung vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Details der Serviceeinheit zwischen den Rastern exakt synchronisieren möchten, nehmen Sie die gleichen Änderungen an beiden Rastern vor. Siehe "[Verwalten Sie die zulässigen Mandanten für die Grid Federation-Verbindung](#)".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung Root-Zugriff oder Mandantenkonten.

Schritte

1. Wählen Sie **MIETER**.

The screenshot shows the 'Tenants' management page. At the top, there's a title 'Tenants' and a subtitle: 'View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.' Below this are controls: 'Create', 'Export to CSV', 'Actions' dropdown, and a search bar 'Search tenants by name or ID'. On the right, it says 'Displaying 5 results'. The main content is a table with the following data:

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;"></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;"></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;"></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;"></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Suchen Sie das Mandantenkonto, das Sie bearbeiten möchten.

Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Wählen Sie den Mandanten aus. Sie können eine der folgenden Aktionen ausführen:

- Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **actions > Edit**.

- Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Bearbeiten**.
4. Ändern Sie optional die Werte für diese Felder:
- **Name**
 - **Beschreibung**
 - **Speicherquote**
5. Wählen Sie **Weiter**.
6. Wählen oder deaktivieren Sie die Berechtigungen für das Mandantenkonto.
- Wenn Sie **Platform Services** für einen Mandanten deaktivieren, der diese bereits nutzt, werden die Dienste, die er für seine S3-Buckets konfiguriert hat, nicht mehr funktionieren. Es wird keine Fehlermeldung an den Mandanten gesendet. Wenn der Mandant beispielsweise die Replizierung von CloudMirror für einen S3-Bucket konfiguriert hat, können sie Objekte weiterhin im Bucket speichern, doch werden Kopien dieser Objekte nicht mehr im externen S3-Bucket erstellt, den sie als Endpunkt konfiguriert haben. Siehe "[Management von Plattform-Services für S3-Mandantenkonten](#)".
 - Ändern Sie die Einstellung **verwendet eigene Identitätsquelle**, um zu bestimmen, ob das Mandantenkonto seine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

Wenn **eigene Identitätsquelle verwendet** ist:

- Deaktiviert und ausgewählt, hat der Mandant bereits seine eigene Identitätsquelle aktiviert. Ein Mandant muss seine Identitätsquelle deaktivieren, bevor er die für den Grid Manager konfigurierte Identitätsquelle verwenden kann.
 - Deaktiviert und nicht ausgewählt, SSO ist für das StorageGRID-System aktiviert. Der Mandant muss die Identitätsquelle verwenden, die für den Grid Manager konfiguriert wurde.
- Wählen oder deaktivieren Sie die Berechtigung **allow S3 Select** nach Bedarf. Siehe "[Management von S3 Select für Mandantenkonten](#)".
 - Um die Berechtigung **use Grid Federation connection** zu entfernen, folgen Sie den Anweisungen für "[Entfernen der Berechtigung eines Mandanten zur Verwendung des Grid-Verbunds](#)".

Ändern Sie das Passwort für den lokalen Root-Benutzer des Mandanten

Möglicherweise müssen Sie das Passwort für den lokalen Root-Benutzer eines Mandanten ändern, wenn der Root-Benutzer aus dem Konto gesperrt ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandanten-Konto anmelden. Um Root-Benutzeraufgaben auszuführen, müssen Benutzer einer föderierten Gruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. Wählen Sie **MIETER**.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;"></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;"></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;"></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;"></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	–	–	500	→ 📄

2. Wählen Sie das Mandantenkonto aus. Sie können eine der folgenden Aktionen ausführen:
 - Aktivieren Sie das Kontrollkästchen für den Mandanten, und wählen Sie **actions > root-Passwort ändern**.
 - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **actions > root password ändern**.
3. Geben Sie das neue Kennwort für das Mandantenkonto ein.
4. Wählen Sie **Speichern**.

Mandantenkonto löschen

Sie können ein Mandantenkonto löschen, wenn Sie den Zugriff des Mandanten auf das System dauerhaft entfernen möchten.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben alle Buckets (S3), Container (Swift) und Objekte entfernt, die dem Mandantenkonto zugeordnet sind.
- Wenn der Mandant eine Grid Federation-Verbindung verwenden darf, haben Sie die Überlegungen für geprüft "[Löschen eines Mandanten mit der Berechtigung Grid Federation verwenden](#)".

Schritte

1. Wählen Sie **MIETER**.
2. Suchen Sie das oder die Konten, die Sie löschen möchten.

Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Um mehrere Mandanten zu löschen, aktivieren Sie die Kontrollkästchen und wählen **Aktionen > Löschen**.

4. Führen Sie einen der folgenden Schritte aus, um eine einzelne Serviceeinheit zu löschen:
 - Aktivieren Sie das Kontrollkästchen, und wählen Sie **Aktionen > Löschen**.
 - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie dann **actions > Delete** aus.
5. Wählen Sie **Ja**.

Management von Plattform-Services

Verwaltung von Plattformservices für Mandanten: Übersicht

Wenn Sie Plattformservices für S3-Mandantenkonten aktivieren, müssen Sie Ihr Grid so konfigurieren, dass Mandanten auf die externen Ressourcen zugreifen können, die für die Nutzung dieser Services erforderlich sind.

Was sind Plattform-Services?

Zu den Plattform-Services zählen die CloudMirror-Replizierung, Ereignisbenachrichtigungen und der Such-Integrationservice.

Dank dieser Services können Mandanten die folgenden Funktionen mit ihren S3 Buckets nutzen:

- **CloudMirror Replikation:** Der StorageGRID CloudMirror Replikationsservice wird verwendet, um bestimmte Objekte von einem StorageGRID-Bucket auf ein bestimmtes externes Ziel zu spiegeln.

So können Sie beispielsweise CloudMirror Replizierung verwenden, um spezifische Kundendaten in Amazon S3 zu spiegeln und anschließend AWS Services für Analysen Ihrer Daten nutzen.



Die CloudMirror-Replizierung weist einige wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter "[Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung](#)".



Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

- **Benachrichtigungen:** Pro Bucket werden Ereignisbenachrichtigungen verwendet, um Benachrichtigungen über bestimmte Aktionen zu senden, die an Objekte an einen bestimmten externen Amazon Simple Notification Service™ (Amazon SNS) durchgeführt werden.

Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.



Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

- **Suchintegrationsdienst:** Der Suchintegrationsdienst dient dazu, S3-Objektmetadaten an einen bestimmten Elasticsearch-Index zu senden, in dem die Metadaten mit dem externen Dienst durchsucht oder analysiert werden können.

Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.



Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperre-Metadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

Dank Plattform-Services können Mandanten externe Storage-Ressourcen, Benachrichtigungsservices und Such- oder Analyseservices für ihre Daten nutzen. Da sich der Zielstandort für Plattformservices in der Regel außerhalb Ihrer StorageGRID-Implementierung befindet, müssen Sie entscheiden, ob die Nutzung dieser Services durch Mandanten gestattet werden soll. Wenn Sie dies tun, müssen Sie die Verwendung von Plattform-Services aktivieren, wenn Sie Mandantenkonten erstellen oder bearbeiten. Sie müssen auch Ihr Netzwerk so konfigurieren, dass die von Mandanten generierten Plattformservices-Meldungen ihre Ziele erreichen können.

Empfehlungen für die Nutzung von Plattform-Services

Vor der Verwendung von Plattform-Services sollten Sie sich der folgenden Empfehlungen bewusst sein:

- Wenn in einem S3-Bucket im StorageGRID System sowohl die Versionierung als auch die CloudMirror-Replizierung aktiviert sind, sollten Sie für den Zielendpunkt auch die S3-Bucket-Versionierung aktivieren. So kann die CloudMirror-Replizierung ähnliche Objektversionen auf dem Endpunkt generieren.
- Sie sollten nicht mehr als 100 aktive Mandanten mit S3-Anfragen verwenden, die CloudMirror-Replizierung, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren S3-Client-Performance führen.
- Anforderungen an einen Endpunkt, die nicht abgeschlossen werden können, werden in die Warteschlange für maximal 500,000 Anfragen gestellt. Dieses Limit wird gleich von aktiven Mandanten gemeinsam genutzt. Neue Mandanten dürfen dieses Limit von 500,000 vorübergehend überschreiten, sodass neu erstellte Mandanten nicht unfair bestraft werden.

Verwandte Informationen

- ["Verwenden Sie ein Mandantenkonto"](#)
- ["Konfigurieren Sie Speicher-Proxy-Einstellungen"](#)
- ["Monitoring von StorageGRID"](#)

Netzwerk und Ports für Plattformservices

Wenn ein S3-Mandant Plattformservices verwendet, müssen Sie das Netzwerk für das Grid konfigurieren, um sicherzustellen, dass Plattformservices-Meldungen an seine Ziele gesendet werden können.

Sie können Plattformservices für ein S3-Mandantenkonto aktivieren, wenn Sie das Mandantenkonto erstellen oder aktualisieren. Wenn Plattformservices aktiviert sind, kann der Mandant Endpunkte erstellen, die als Ziel für die CloudMirror-Replizierung, Ereignisbenachrichtigungen oder Integrationsmeldungen aus seinen S3-Buckets dienen. Diese Plattform-Services-Meldungen werden von Storage-Nodes gesendet, die den ADC-Service an die Ziel-Endpunkte ausführen.

Beispielsweise können Mandanten die folgenden Typen von Ziel-Endpunkten konfigurieren:

- Ein lokal gehostetes Elasticsearch-Cluster ausführen
- Eine lokale Anwendung, die den Empfang von Amazon SNS-Nachrichten (Simple Notification Service) unterstützt
- Ein lokal gehosteter S3-Bucket auf derselben oder einer anderen Instanz von StorageGRID
- Einem externen Endpunkt wie einem Endpunkt auf Amazon Web Services

Um sicherzustellen, dass Meldungen von Plattformservices bereitgestellt werden können, müssen Sie das Netzwerk oder die Netzwerke mit den ADC-Speicherknoten konfigurieren. Sie müssen sicherstellen, dass die folgenden Ports zum Senden von Plattformservices-Meldungen an die Ziel-Endpunkte verwendet werden können.

Standardmäßig werden Plattform-Services-Meldungen an die folgenden Ports gesendet:

- **80**: Für Endpunkt-URIs, die mit http beginnen
- **443**: Für Endpunkt-URIs, die mit https beginnen

Mandanten können bei der Erstellung oder Bearbeitung eines Endpunkts einen anderen Port angeben.



Wenn eine StorageGRID-Bereitstellung als Ziel für die CloudMirror-Replikation verwendet wird, können Replikationsmeldungen auf einem anderen Port als 80 oder 443 empfangen werden. Vergewissern Sie sich, dass der von der Ziel-StorageGRID-Implementierung für S3 verwendete Port im Endpunkt angegeben ist.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch "[Konfigurieren Sie Speicher-Proxy-Einstellungen](#)" Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

Verwandte Informationen

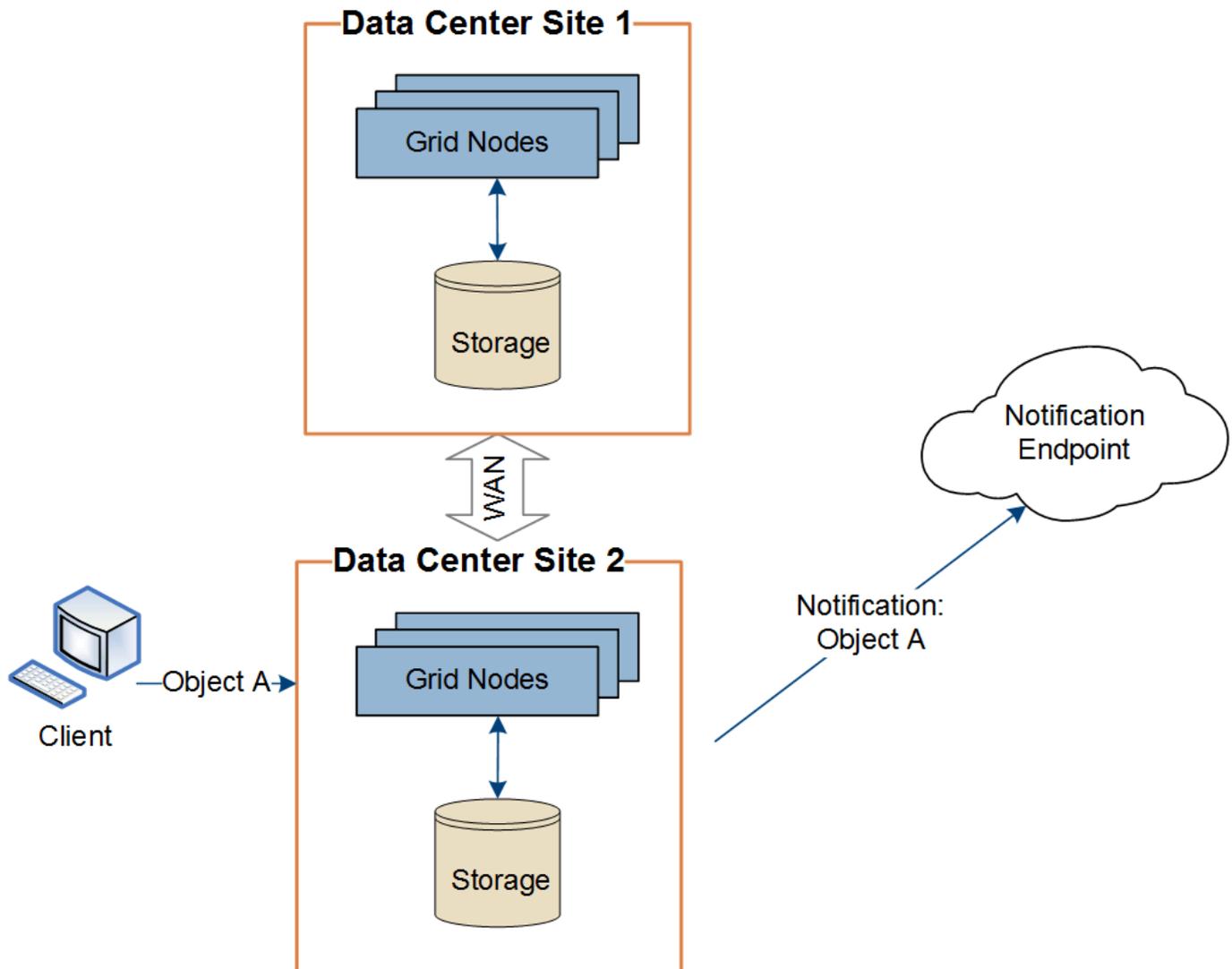
- "[Verwenden Sie ein Mandantenkonto](#)"

Bereitstellung von Plattform-Services am Standort

Alle Vorgänge von Plattform-Services werden am Standort durchgeführt.

Wenn ein Mandant einen Client verwendet, um einen S3 API Create-Vorgang für ein Objekt durch eine Verbindung zu einem Gateway-Node an Datacenter Standort 1 durchzuführen, wird die Benachrichtigung über diese Aktion von Datacenter Standort 1 ausgelöst und gesendet.

Wenn der Client anschließend einen S3-API-Löschvorgang auf demselben Objekt von Data Center Site 2 aus durchführt, wird die Benachrichtigung über die Löschaktion ausgelöst und von Data Center Site 2 gesendet.



Stellen Sie sicher, dass das Netzwerk an jedem Standort so konfiguriert ist, dass Plattformdienste-Meldungen an ihre Ziele gesendet werden können.

Fehlerbehebung bei Plattform-Services

Die in Plattform-Services verwendeten Endpunkte werden von Mandantenbenutzern im Mandanten-Manager erstellt und gewartet. Falls jedoch Probleme bei der Konfiguration oder Verwendung von Plattformservices bei einem Mandanten auftreten, können Sie das Problem mithilfe des Grid Manager beheben.

Probleme mit neuen Endpunkten

Bevor ein Mandant Plattform-Services nutzen kann, muss er mithilfe des Mandanten-Manager einen oder mehrere Endpunkte erstellen. Jeder Endpunkt stellt ein externes Ziel für einen Plattform-Service dar, wie einen StorageGRID S3 Bucket, einen Amazon Web Services Bucket, ein Thema „Simple Notification Service“ oder ein Elasticsearch-Cluster, der lokal oder in AWS gehostet wird. Jeder Endpunkt umfasst sowohl den Standort der externen Ressource als auch die für den Zugriff auf diese Ressource erforderlichen Zugangsdaten.

Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID System, ob der Endpunkt vorhanden ist und ob er mit den angegebenen Zugangsdaten erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Wenn die Endpoint-Validierung fehlschlägt, erklärt eine Fehlermeldung, warum die Endpoint-Validierung fehlgeschlagen ist. Der Mandantenbenutzer sollte das Problem lösen, und versuchen Sie dann erneut, den Endpunkt zu erstellen.



Die Erstellung von Endpunkten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn ein Fehler auftritt, wenn StorageGRID versucht, einen vorhandenen Endpunkt zu erreichen, wird im Mandantenmanager eine Meldung auf dem Dashboard angezeigt.



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Mandantenbenutzer können auf der Seite Endpunkte die aktuellste Fehlermeldung für jeden Endpunkt lesen und herausfinden, wie lange der Fehler bereits aufgetreten ist. Die Spalte **Letzter Fehler** zeigt die aktuellste Fehlermeldung für jeden Endpunkt an und gibt an, wie lange der Fehler aufgetreten ist. Fehler, die das Symbol enthalten, traten innerhalb der letzten 7 Tage auf.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.



One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3	3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
<input type="checkbox"/>	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



Einige Fehlermeldungen in der Spalte **Letzter Fehler** können eine LOGID in Klammern enthalten. Ein Grid-Administrator oder technischer Support kann diese ID verwenden, um ausführlichere Informationen über den Fehler im bycast.log zu finden.

Probleme im Zusammenhang mit Proxy-Servern

Wenn Sie einen konfiguriert haben "[Storage-Proxy](#)" Zwischen Storage-Nodes und Plattform-Service-Endpunkten können Fehler auftreten, wenn Ihr Proxy-Service keine Meldungen von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass keine Nachrichten im Zusammenhang mit dem Plattformdienst blockiert werden.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Endpunktfehler aufgetreten sind, zeigt das Dashboard im Tenant Manager eine Warnmeldung an. Sie können die Seite Endpoints aufrufen, um weitere Details über den Fehler zu sehen.

Client-Betrieb schlägt fehl

Einige Probleme bei Plattform-Services können zum Ausfall von Client-Operationen auf dem S3-Bucket führen. Beispielsweise schlägt der S3-Client-Betrieb fehl, wenn der interne RSM-Service (Replicated State Machine) ausfällt oder es zu viele Plattformservices-Nachrichten in Warteschlange für die Lieferung gibt.

So überprüfen Sie den Status der Dienste:

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **site > Storage Node > SSM > Services** aus.

Behebbarer und nicht wiederherstellbarer Endpunktfehler

Nach der Erstellung von Endpunkten können Fehler bei Plattformservice-Anfragen aus verschiedenen Gründen auftreten. Einige Fehler lassen sich durch Benutzereingriffe wiederherstellen. Beispielsweise können behebbare Fehler aus den folgenden Gründen auftreten:

- Die Anmeldedaten des Benutzers wurden gelöscht oder abgelaufen.
- Der Ziel-Bucket ist nicht vorhanden.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn bei StorageGRID ein wiederherstellbarer Fehler auftritt, wird die Serviceanfrage für die Plattform erneut versucht, bis sie erfolgreich ist.

Andere Fehler können nicht behoben werden. Beispielsweise tritt ein nicht behebbarer Fehler auf, wenn der Endpunkt gelöscht wird.

Wenn bei StorageGRID ein nicht behebbarer Endpunktfehler auftritt, wird im Grid Manager der alte Alarm „Total Events“ (SMTT) ausgelöst. So zeigen Sie den alten Alarm „Ereignisse insgesamt“ an:

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **site > Node > SSM > Events** aus.
3. Letztes Ereignis oben in der Tabelle anzeigen.

Ereignismeldungen sind auch in `aufgeführt /var/local/log/bycast-err.log`.

4. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
5. Wählen Sie die Registerkarte **Konfiguration**, um die Ereignisanzahl zurückzusetzen.
6. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.

7. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts erneut auszulösen.

Der Mieter kann die vorhandenen Werte erneut einreichen, um unerwünschte Änderungen zu vermeiden.

Nachrichten zu Plattform-Services können nicht bereitgestellt werden

Wenn im Ziel ein Problem auftritt, das verhindert, dass Plattformdienste-Meldungen akzeptiert werden, wird der Client-Vorgang auf dem Bucket erfolgreich ausgeführt, die Plattform-Services-Meldung wird jedoch nicht geliefert. Dieser Fehler kann z. B. auftreten, wenn die Anmeldeinformationen auf dem Ziel aktualisiert werden, sodass sich StorageGRID nicht mehr beim Ziel-Service authentifizieren kann.

Wenn Meldungen zu Plattformdiensten aufgrund eines nicht behebbaren Fehlers nicht zugestellt werden können, wird der Legacy-Alarm „Total Events (SMTT)“ im Grid Manager ausgelöst.

Langsamere Performance für Plattform-Service-Anfragen

StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielpunkt warten.

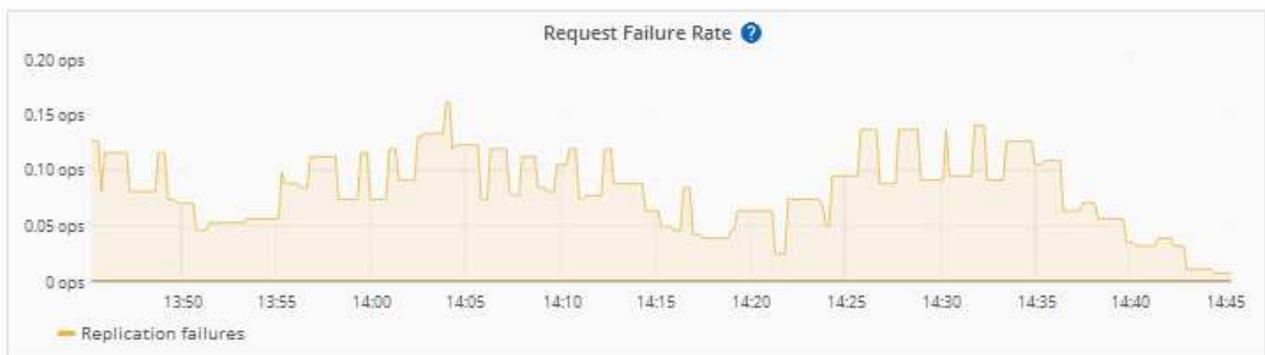
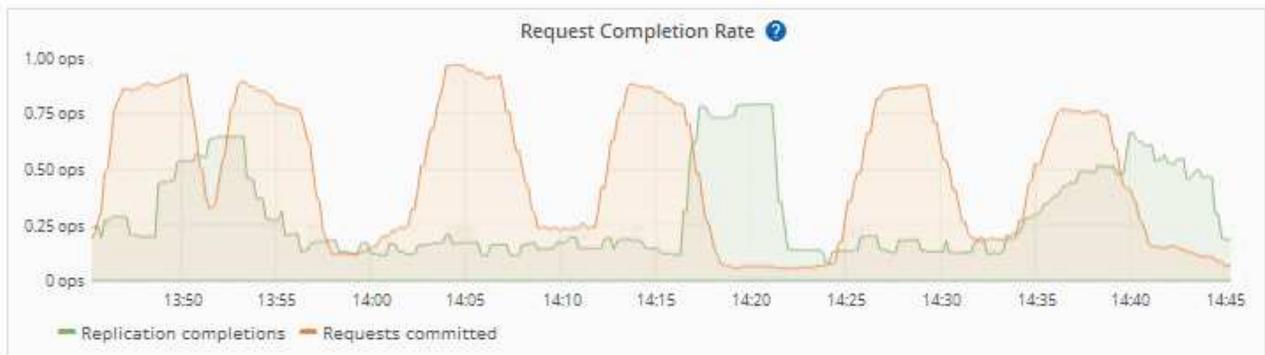
Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahme rate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie z. B. PUT-Anforderungen) letztendlich.

CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Plattformdienstanfragen schlagen fehl

So zeigen Sie die Ausfallrate der Anfrage für Plattformdienste an:

1. Wählen Sie **KNOTEN**.
2. Wählen Sie **site > Platform Services**.
3. Zeigen Sie das Diagramm Fehlerrate anfordern an.



Plattformdienste – Warnung nicht verfügbar

Die Warnmeldung **Platform Services nicht verfügbar** zeigt an, dass an einem Standort keine Plattformservicevorgänge ausgeführt werden können, da zu wenige Speicherknoten mit dem RSM-Dienst ausgeführt oder verfügbar sind.

Der RSM-Dienst stellt sicher, dass Plattformserviceanforderungen an die jeweiligen Endpunkte gesendet werden.

Um diese Warnmeldung zu beheben, legen Sie fest, welche Speicherknoten am Standort den RSM-Service enthalten. (Der RSM-Service ist auf Speicherknoten vorhanden, die auch den ADC-Service enthalten.) Stellen Sie anschließend sicher, dass ein einfacher Großteil dieser Speicherknoten ausgeführt und verfügbar ist.



Wenn mehr als ein Speicherknoten, der den RSM-Dienst enthält, an einem Standort ausfällt, verlieren Sie alle ausstehenden Plattformserviceanforderungen für diesen Standort.

Zusätzliche Anleitung zur Fehlerbehebung für Endpunkte von Plattformservices

Weitere Informationen finden Sie unter [Verwenden Sie ein Mandantenkonto](#) > [Troubleshooting der Endpunkte für Plattformservices](#).

Verwandte Informationen

- ["Fehlerbehebung für das StorageGRID-System"](#)

Management von S3 Select für Mandantenkonten

Bestimmte S3-Mandanten können S3 Select verwenden, um SelectObjectContent-Anfragen für einzelne Objekte auszulösen.

S3 Select bietet eine effiziente Möglichkeit, große Datenmengen zu durchsuchen, ohne eine Datenbank und zugehörige Ressourcen bereitstellen zu müssen, um die Suche zu ermöglichen. Es senkt auch die Kosten und die Latenz beim Abrufen der Daten.

Was ist S3 Select?

Mit S3 Select können S3-Clients SelectObjectContent-Anfragen verwenden, um nur die von einem Objekt benötigten Daten zu filtern und abzurufen. Die StorageGRID Implementierung von S3 Select enthält eine Untergruppe von S3 Select-Befehlen und -Funktionen.

Überlegungen und Anforderungen bei der Verwendung von S3 Select

Grid-Administrationsanforderungen

Der Grid-Administrator muss Mandanten die Möglichkeit S3 Select erteilen. Wählen Sie **S3-Auswahl zulassen** aus, wann ["Erstellen eines Mandanten"](#) Oder ["Bearbeiten eines Mandanten"](#).

Anforderungen an das Objektformat

Das Objekt, das Sie abfragen möchten, muss eines der folgenden Formate aufweisen:

- **CSV**. Kann wie ist verwendet oder in GZIP- oder BZIP2-Archiven komprimiert werden.
- **Parkett**. Zusätzliche Anforderungen an Parkett-Objekte:
 - S3 Select unterstützt nur Spaltenkomprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Komprimierung ganzer Objekte für Parkett-Objekte.
 - S3 Select unterstützt keine Parkett-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
 - Die maximale Größe der nicht komprimierten Zeilengruppe beträgt 512 MB.
 - Sie müssen die im Objektschema angegebenen Datentypen verwenden.
 - Sie können KEINE logischen TYPEN VON INTERVALL, JSON, LISTE, ZEIT oder UUID verwenden.

Anforderungen an Endpunkte

Die SelectObjectContent-Anforderung muss an ein gesendet werden ["Endpunkt des StorageGRID-Load-](#)

Balancer".

Die vom Endpunkt verwendeten Admin- und Gateway-Nodes müssen einen der folgenden sein:

- Ein SG100- oder SG1000-Appliance-Node
- Ein auf VMware basierender Software-Node
- Ein Bare-Metal-Knoten, auf dem ein Kernel mit aktivierter cgroup v2 ausgeführt wird

Allgemeine Überlegungen

Abfragen können nicht direkt an Storage-Nodes gesendet werden.



SelectObjectContent-Anforderungen können die Load Balancer-Performance für alle S3-Clients und alle Mandanten reduzieren. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Siehe "[Anweisungen zur Verwendung von S3 Select](#)".

Um sie anzuzeigen "[Grafana-Diagramme](#)" Für S3 Wählen Sie im Grid Manager Operationen über die Zeit aus, wählen Sie im Grid Manager * SUPPORT* > **Tools** > **Metriken**.

Client-Verbindungen konfigurieren

Konfigurieren Sie S3- und Swift-Client-Verbindungen: Übersicht

Als Grid-Administrator managen Sie die Konfigurationsoptionen, die steuern, wie sich S3 und Swift Client-Applikationen mit dem StorageGRID System verbinden, um Daten zu speichern und abzurufen.

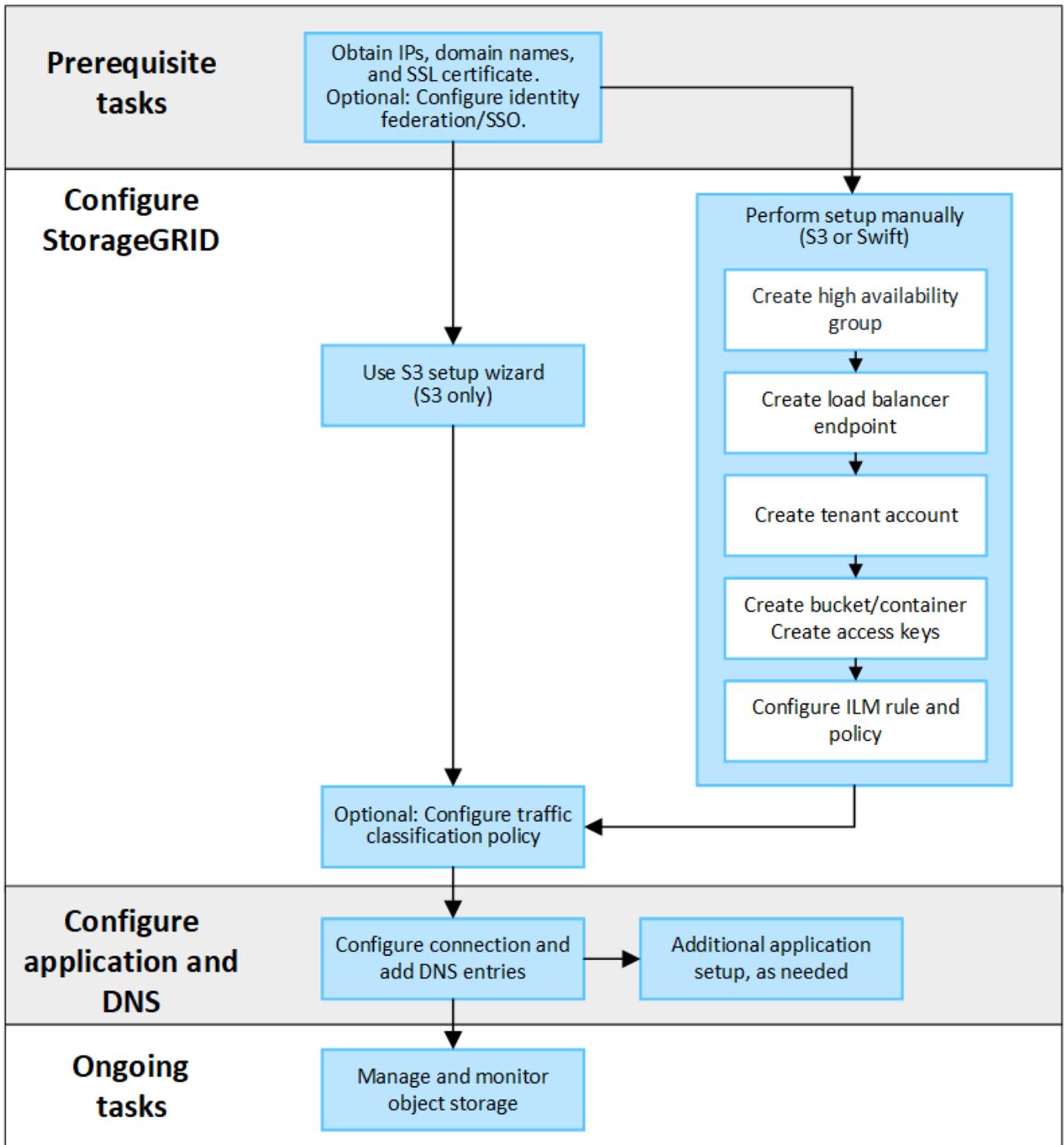


Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Konfigurationsworkflow

Wie im Workflow-Diagramm dargestellt, gibt es vier primäre Schritte für die Verbindung von StorageGRID mit einer beliebigen S3- oder Swift-Applikation:

1. Führen Sie erforderliche Aufgaben in StorageGRID aus, je nachdem, wie die Clientanwendung eine Verbindung zu StorageGRID herstellt.
2. Verwenden Sie StorageGRID, um die Werte abzurufen, die die Anwendung für die Verbindung mit dem Grid benötigt. Sie können entweder den S3-Einrichtungsassistenten verwenden oder jede StorageGRID-Einheit manuell konfigurieren.
3. Verwenden Sie die S3- oder Swift-Applikation, um die Verbindung zu StorageGRID abzuschließen. Erstellen Sie DNS-Einträge, um IP-Adressen mit beliebigen Domännennamen zu verknüpfen, die Sie verwenden möchten.
4. Laufende Aufgaben in der Applikation und in StorageGRID werden durchgeführt, um Objekt-Storage über einen längeren Zeitraum zu managen und zu überwachen.



Informationen, die zum Anhängen von StorageGRID an eine Client-Applikation erforderlich sind

Bevor Sie StorageGRID an eine S3- oder Swift-Client-Applikation anhängen können, müssen Sie die Konfigurationsschritte in StorageGRID ausführen und einen bestimmten Wert erhalten.

Welche Werte brauche ich?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen und wo diese Werte von der S3- oder Swift-Anwendung und dem DNS-Server verwendet werden.

Wert	Wobei der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
SSL-Zertifikat	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
Servername (FQDN)	StorageGRID > Endpunkt des Load Balancer	<ul style="list-style-type: none"> • Client-Anwendung • DNS-Eintrag
S3 Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	Client-Anwendung
Bucket/Container-Name	StorageGRID > Mandant und Bucket	Client-Anwendung

Wie erhalte ich diese Werte?

Je nach Ihren Anforderungen können Sie eine der folgenden Möglichkeiten nutzen, um die benötigten Informationen zu erhalten:

- **Verwenden Sie die "S3-Einrichtungsassistent"**. Der S3-Einrichtungsassistent unterstützt Sie beim schnellen Konfigurieren der erforderlichen Werte in StorageGRID und gibt eine oder zwei Dateien aus, die Sie bei der Konfiguration der S3-Anwendung verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und stellt sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.



Wenn Sie eine S3-Applikation konfigurieren, wird die Verwendung des S3-Setup-Assistenten von empfohlen, es sei denn, Sie verfügen über besondere Anforderungen oder Ihre Implementierung erfordert eine umfangreiche Anpassung.

- **Verwenden Sie die "FabricPool Setup-Assistent"**. Ähnlich wie der S3-Einrichtungsassistent unterstützt Sie der FabricPool-Einrichtungsassistent bei der schnellen Konfiguration der erforderlichen Werte und gibt eine Datei aus, die Sie bei der Konfiguration eines FabricPool-Cloud-Tiers in ONTAP verwenden können.



Wenn Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier nutzen möchten, empfiehlt sich die Verwendung des FabricPool Setup-Assistenten, es sei denn, Sie haben besondere Anforderungen oder Ihre Implementierung erfordert erhebliche Anpassungen.

- **Elemente manuell konfigurieren**. Wenn Sie eine Verbindung zu einer Swift-Anwendung herstellen (oder eine Verbindung zu einer S3-Anwendung herstellen und den S3-Einrichtungsassistenten nicht verwenden möchten), können Sie die erforderlichen Werte abrufen, indem Sie die Konfiguration manuell durchführen. Führen Sie hierzu folgende Schritte aus:
 - a. Konfigurieren Sie die HA-Gruppe (High Availability, Hochverfügbarkeit), die Sie für die S3- oder Swift-Applikation verwenden möchten. Siehe "[Konfigurieren Sie Hochverfügbarkeitsgruppen](#)".

- b. Erstellen Sie den Load Balancer-Endpunkt, den die S3- oder Swift-Applikation verwenden wird. Siehe ["Konfigurieren von Load Balancer-Endpunkten"](#).
- c. Erstellen Sie das Mandantenkonto, das die S3- oder Swift-Applikation verwenden wird. Siehe ["Erstellen Sie ein Mandantenkonto"](#).
- d. Melden Sie sich für einen S3-Mandanten beim Mandantenkonto an und generieren Sie für jeden Benutzer, der auf die Applikation zugreift, eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel. Siehe ["Erstellen Sie Ihre eigenen Zugriffsschlüssel"](#).
- e. Erstellen Sie einen oder mehrere S3-Buckets oder Swift-Container im Mandantenkonto. Informationen zu S3 finden Sie unter ["S3-Bucket erstellen"](#). Verwenden Sie für Swift die ["Container-Anforderung SETZEN"](#).
- f. Um Anweisungen zur Platzierung von Objekten, die zu dem neuen Mandanten oder Bucket/Container gehören, hinzuzufügen, erstellen Sie eine neue ILM-Regel und aktivieren Sie zur Verwendung dieser Regel eine neue ILM-Richtlinie. Siehe ["ILM-Regel erstellen"](#) Und ["ILM-Richtlinie erstellen"](#).

Verwenden Sie den S3-Einrichtungsassistenten

Überlegungen und Anforderungen im S3-Setup-Assistenten

Sie können mit dem S3-Einrichtungsassistenten StorageGRID als Objekt-Storage-System für eine S3-Applikation konfigurieren.

Wann der S3-Einrichtungsassistent verwendet werden soll

Der S3-Einrichtungsassistent führt Sie durch jeden Schritt bei der Konfiguration von StorageGRID für die Verwendung mit einer S3-Applikation. Im Rahmen der Ausführung des Assistenten laden Sie Dateien herunter, mit denen Sie Werte in die S3-Anwendung eingeben können. Mit dem Assistenten konfigurieren Sie Ihr System schneller und stellen sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.

Wenn Sie über die Berechtigung für den Root-Zugriff verfügen, können Sie den S3-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID-Grid-Manager verwenden. Sie können aber auch jederzeit auf den Assistenten zugreifen und ihn abschließen. Je nach Ihren Anforderungen können Sie auch einige oder alle erforderlichen Elemente manuell konfigurieren und dann mithilfe des Assistenten die Werte zusammenstellen, die eine S3-Anwendung benötigt.

Bevor Sie den Assistenten verwenden

Vergewissern Sie sich vor der Verwendung des Assistenten, dass Sie diese Voraussetzungen erfüllt haben.

Beziehen Sie IP-Adressen, und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit) konfigurieren, wissen Sie, mit welchen Nodes die S3-Applikation eine Verbindung herstellen und welches StorageGRID-Netzwerk verwendet wird. Sie wissen auch, welche Werte für das Subnetz CIDR, die Gateway-IP-Adresse und die virtuelle IP (VIP)-Adresse eingegeben werden sollen.

Wenn Sie planen, einen virtuellen LAN zur Trennung des Datenverkehrs von der S3-Anwendung zu verwenden, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Siehe ["Konfigurieren Sie die VLAN-Schnittstellen"](#).

Konfigurieren Sie Identity Federation und SSO

Wenn Sie planen, Identity Federation oder Single Sign-On (SSO) für Ihr StorageGRID-System zu verwenden,

haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff für das Mandantenkonto haben soll, das die S3-Anwendung verwenden wird. Siehe "[Verwenden Sie den Identitätsverbund](#)" Und "[Konfigurieren Sie Single Sign-On](#)".

Abrufen und Konfigurieren von Domännennamen

Sie wissen, welcher vollständig qualifizierte Domänenname (FQDN) für StorageGRID verwendet werden soll. DNS-Einträge (Domain Name Server) weisen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen.

Wenn Sie Anforderungen im virtuellen Hosted-Stil von S3 verwenden möchten, sollten Sie dies beachten "[Domännennamen des S3-Endpunkts wurden konfiguriert](#)". Die Verwendung von Anforderungen im virtuellen Hosted-Stil wird empfohlen.

Anforderungen für Load Balancer und Sicherheitszertifikate prüfen

Wenn Sie den StorageGRID Load Balancer einsetzen möchten, haben Sie die allgemeinen Überlegungen zum Lastausgleich besprochen. Sie verfügen über die hochgeladenen Zertifikate oder die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn Sie einen externen (Drittanbieter-)Load Balancer-Endpunkt verwenden möchten, verfügen Sie über den vollständig qualifizierten Domännennamen (FQDN), den Port und das Zertifikat für diesen Load Balancer.

Konfigurieren Sie alle Verbindungen des Grid-Verbunds

Wenn Sie es dem S3-Mandanten erlauben möchten, Kontodaten zu klonen und Bucket-Objekte mithilfe einer Grid-Federation-Verbindung in ein anderes Grid zu replizieren, bestätigen Sie Folgendes, bevor Sie den Assistenten starten:

- Das ist schon "[Grid Federation-Verbindung konfiguriert](#)".
- Der Status der Verbindung lautet **connected**.
- Sie haben Root-Zugriffsberechtigung.

Rufen Sie den S3-Setup-Assistenten auf und vervollständigen Sie sie

Sie können den S3-Einrichtungsassistenten verwenden, um StorageGRID für die Verwendung mit einer S3-Applikation zu konfigurieren. Der Einrichtungsassistent bietet die Werte, die die Anwendung benötigt, um auf einen StorageGRID-Bucket zuzugreifen und Objekte zu speichern.

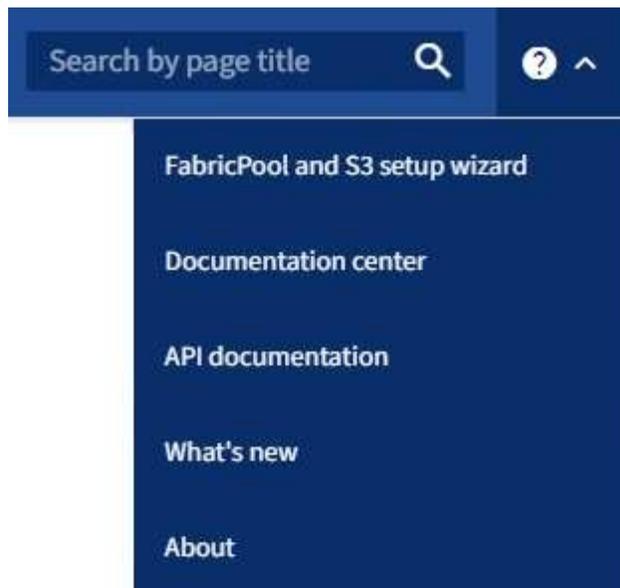
Bevor Sie beginnen

- Sie haben die "[Root-Zugriffsberechtigung](#)".
- Sie haben die geprüft "[Überlegungen und Anforderungen](#)" Zur Verwendung des Assistenten.

Greifen Sie auf den Assistenten zu

Schritte

1. Melden Sie sich mit einem bei Grid Manager an "[Unterstützter Webbrowser](#)".
2. Wenn das Banner **FabricPool and S3 Setup Wizard** auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie in der Kopfzeile des Grid-Managers das Hilfesymbol aus und wählen Sie **FabricPool und S3-Setup-Assistent** aus.



3. Wählen Sie im Abschnitt S3-Anwendung der Seite FabricPool und S3-Setup-Assistent **Jetzt konfigurieren** aus.

Schritt 1 von 6: Konfigurieren Sie die HA-Gruppe

Eine HA-Gruppe ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um die S3 Datenverbindungen verfügbar zu halten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den S3-Betrieb managen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Management von Hochverfügbarkeitsgruppen](#)".

Schritte

1. Wenn Sie einen externen Load Balancer verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **diesen Schritt überspringen** und gehen Sie zu [Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt](#).
2. Um den StorageGRID Load Balancer zu verwenden, können Sie eine neue HA-Gruppe erstellen oder eine vorhandene HA-Gruppe verwenden.

Erstellen Sie eine HA-Gruppe

- a. Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.
- b. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

Feld	Beschreibung
Name DER HA-Gruppe	Ein eindeutiger Anzeigename für diese HA-Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

- c. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

- d. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

Ziehen Sie Zeilen, um die Werte in der Spalte **Priority order** zu ändern.

Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Fehler behoben sind, werden die VIP-Adressen auf die Schnittstelle mit der höchsten Priorität zurückverschoben.

- e. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation — eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: 192.16.0.0/22.
Gateway-IP-Adresse (optional)	Wenn sich die S3-IP-Adressen für den Zugriff auf StorageGRID nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die lokale StorageGRID-VIP-Gateway-IP-Adresse ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

f. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**, um zum S3-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Verwenden Sie die vorhandene HA-Gruppe

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus **Select an HA Group** aus.

b. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt

StorageGRID verwendet einen Load Balancer für das Management des Workloads aus Client-Applikationen. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Sie können den StorageGRID Load Balancer-Dienst verwenden, der auf allen Gateway- und Admin-Nodes vorhanden ist, oder eine Verbindung zu einem externen Load Balancer (Drittanbieter) herstellen. Die Verwendung des StorageGRID Load Balancer wird empfohlen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Überlegungen zum Lastausgleich](#)".

Um den StorageGRID Load Balancer Service zu verwenden, wählen Sie die Registerkarte **StorageGRID Load Balancer** aus und erstellen oder wählen Sie dann den gewünschten Load Balancer-Endpunkt aus. Um einen externen Load Balancer zu verwenden, wählen Sie die Registerkarte **External Load Balancer** und geben Sie Details zum System an, das Sie bereits konfiguriert haben.

Endpunkt erstellen

Schritte

1. Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie **Endpunkt erstellen**.
2. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.
Port	<p>Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind.</p> <p>Hinweis: von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe "Referenz für Netzwerk-Ports".</p>
Client-Typ	Muss S3 sein.
Netzwerkprotokoll	<p>Wählen Sie HTTPS.</p> <p>Hinweis: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.</p>

3. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt zugegriffen wird—Verwendung einer beliebigen IP-Adresse oder Verwendung bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	<p>Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen.</p> <p>Verwenden Sie die Global-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.</p>
Virtuelle IPs von HA-Gruppen	<p>Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen.</p> <p>Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.</p>

Option	Beschreibung
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

4. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

5. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Siehe " Konfigurieren von Load Balancer-Endpunkten " Für Details, was eingegeben werden soll.
StorageGRID S3 und Swift-Zertifikat verwenden	Verwenden Sie diese Option nur, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Siehe " Konfigurieren von S3- und Swift-API-Zertifikaten " Entsprechende Details.

6. Wählen Sie **Finish**, um zum S3-Setup-Assistenten zurückzukehren.

7. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Verwenden Sie den vorhandenen Endpunkt des Load Balancer

Schritte

1. Um einen vorhandenen Endpunkt zu verwenden, wählen Sie seinen Namen aus dem **Select a Load Balancer Endpunkt** aus.
2. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Externen Load Balancer verwenden

Schritte

1. Um einen externen Load Balancer zu verwenden, füllen Sie die folgenden Felder aus.

Feld	Beschreibung
FQDN	Der vollständig qualifizierte Domänenname (FQDN) des externen Load Balancer.
Port	Die Portnummer, die die S3-Anwendung für die Verbindung mit dem externen Load Balancer verwendet.
Zertifikat	Kopieren Sie das Serverzertifikat für den externen Load Balancer und fügen Sie es in dieses Feld ein.

2. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Schritt 3 von 6: Erstellen Sie einen Mandanten und Bucket

Ein Mandant ist eine Einheit, die S3-Applikationen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und bestimmte Funktionen. Sie müssen den Mandanten erstellen, bevor Sie den Bucket erstellen können, den die S3-Applikation zum Speichern ihrer Objekte verwendet.

Ein Bucket ist ein Container, mit dem die Objekte und Objektmetadaten eines Mandanten gespeichert werden können. Obwohl einige Mandanten möglicherweise über viele Buckets verfügen, hilft Ihnen der Assistent dabei, auf schnelle und einfache Weise einen Mandanten und einen Bucket zu erstellen. Sie können den Tenant Manager später verwenden, um zusätzliche Buckets hinzuzufügen, die Sie benötigen.

Sie können einen neuen Mandanten für diese S3-Anwendung erstellen. Optional können Sie auch einen Bucket für den neuen Mandanten erstellen. Schließlich können Sie zulassen, dass der Assistent die S3-Zugriffsschlüssel für den Root-Benutzer des Mandanten erstellt.

Weitere Informationen zu dieser Aufgabe finden Sie unter ["Erstellen eines Mandantenkontos"](#) und ["S3-Bucket erstellen"](#).

Schritte

1. Wählen Sie **Create Tenant**.
2. Geben Sie für die Schritte zum Eingeben von Details die folgenden Informationen ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten.
Client-Typ	Der Typ des Clientprotokolls, das von diesem Mandanten verwendet wird. Für den S3-Setup-Assistenten ist S3 ausgewählt und das Feld deaktiviert.
Storage-Kontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent, einen numerischen Wert für das Kontingent und die Einheiten verfügt.

3. Wählen Sie **Weiter**.

4. Wählen Sie optional alle Berechtigungen aus, die dieser Tenant haben soll.



Einige dieser Berechtigungen haben zusätzliche Anforderungen. Für Details wählen Sie das Hilfesymbol für jede Berechtigung aus.

Berechtigung	Wenn ausgewählt...
Unterstützung von Plattform-Services	Der Mandant kann S3-Platformservices wie CloudMirror verwenden. Siehe "Management von Plattform-Services für S3-Mandantenkonten" .
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für verbundene Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie dies haben "SSO konfiguriert" Für Ihr StorageGRID-System.
S3 Select zulassen	Der Mandant kann S3 SelectObjectContent API-Anforderungen ausgeben, um Objektdaten zu filtern und abzurufen. Siehe "Management von S3 Select für Mandantenkonten" . Wichtig: SelectObjectContent Requests können die Load Balancer Performance für alle S3 Clients und alle Tenants verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Berechtigung	Wenn ausgewählt...
Netzverbundverbindung verwenden	<p>Der Mandant kann eine Grid Federation-Verbindung verwenden.</p> <p>Auswahl dieser Option:</p> <ul style="list-style-type: none"> • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer aus diesem Raster (das <i>source Grid</i>) in das andere Raster der ausgewählten Verbindung (das <i>Destination Grid</i>) geklont werden. • Ermöglicht diesem Mandanten, die Grid-übergreifende Replizierung zwischen entsprechenden Buckets in jedem Grid zu konfigurieren. <p>Siehe "Verwalten Sie die zulässigen Mandanten für den Grid-Verbund".</p> <p>Hinweis: Sie können nur Grid Federation connection verwenden auswählen, wenn Sie einen neuen S3-Mandanten erstellen; Sie können diese Berechtigung nicht für einen vorhandenen Mandanten auswählen.</p>

5. Wenn Sie **Grid Federation connection** verwenden ausgewählt haben, wählen Sie eine der verfügbaren Grid Federation-Verbindungen aus.
6. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System verwendet "[Identitätsföderation](#)", "[Single Sign On \(SSO\)](#)" oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	<ol style="list-style-type: none"> a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

7. Wenn Sie möchten, dass der Assistent die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer erstellt, wählen Sie **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen**.



Wählen Sie diese Option aus, wenn der einzige Benutzer für den Mandanten der Root-Benutzer ist. Wenn andere Benutzer diesen Mandanten verwenden, konfigurieren Sie mit Tenant Manager Schlüssel und Berechtigungen.

8. Wählen Sie **Weiter**.
9. Erstellen Sie für den Schritt „Bucket erstellen“ optional einen Bucket für die Objekte des Mandanten. Andernfalls wählen Sie **Create Tenant without bucket**, um zum zu gelangen [Datenschritt herunterladen](#).



Wenn S3 Object Lock für das Raster aktiviert ist, ist für den in diesem Schritt erstellten Bucket die S3 Object Lock nicht aktiviert. Wenn Sie einen S3 Object Lock Bucket für diese S3-Anwendung verwenden müssen, wählen Sie **Create Tenant without Bucket** aus. Verwenden Sie anschließend Tenant Manager für "[Erstellen Sie den Bucket](#)" Stattdessen.

- a. Geben Sie den Namen des Buckets ein, den die S3-Applikation verwendet. Beispiel: s3-bucket.



Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

- b. Wählen Sie die **Region** für diesen Bucket aus.

Verwenden Sie die Standardregion (US-East-1), es sei denn, Sie möchten ILM zukünftig verwenden, um Objekte basierend auf der Region des Buckets zu filtern.

- c. Wählen Sie **enable object Versioning** aus, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten.
- d. Wählen Sie **Create Tenant and bucket** und gehen Sie zum Download Data Step.

Schritt 4 von 6: Daten herunterladen

Im Schritt zum Herunterladen von Daten können Sie eine oder zwei Dateien herunterladen, um die Details zu dem zu speichern, was Sie gerade konfiguriert haben.

Schritte

1. Wenn Sie **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen** ausgewählt haben, führen Sie einen oder beide der folgenden Schritte aus:
 - Wählen Sie **Download Access keys**, um einen herunterzuladen .csv Datei mit dem Kontonamen des Mandanten, der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel.
 - Wählen Sie das Symbol Kopieren () Um die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.
2. Wählen Sie **Konfigurationswerte herunterladen**, um einen herunterzuladen .txt Datei mit den Einstellungen für den Load Balancer-Endpunkt, den Mandanten, den Bucket und den Root-Benutzer.
3. Speichern Sie diese Informationen an einem sicheren Ort.



Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert haben. Die Tasten sind nach dem Schließen dieser Seite nicht mehr verfügbar. Speichern Sie diese Informationen an einem sicheren Ort, da sie zum Abrufen von Daten von Ihrem StorageGRID-System verwendet werden können.

4. Wenn Sie dazu aufgefordert werden, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Schlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter**, um zur ILM-Regel und zum Richtlinien schritt zu gelangen.

Schritt 5 von 6: Prüfen Sie die ILM-Regel und die ILM-Richtlinie für S3

Informationen Lifecycle Management-Regeln (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System. Mit der bei StorageGRID enthaltenen ILM-Richtlinie werden zwei replizierte Kopien aller Objekte erstellt. Diese Richtlinie ist gültig, bis Sie eine neue vorgeschlagene Richtlinie erstellen und aktivieren.

Schritte

1. Überprüfen Sie die Informationen auf der Seite.
2. Wenn Sie bestimmte Anweisungen für die Objekte hinzufügen möchten, die zum neuen Mandanten oder Bucket gehören, erstellen Sie eine neue Regel und eine neue Richtlinie. Siehe "[ILM-Regel erstellen](#)" Und "[ILM-Richtlinie erstellen: Übersicht](#)".
3. Wählen Sie * Ich habe diese Schritte überprüft und verstehe, was ich tun muss*.
4. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie die nächsten Schritte verstehen.
5. Wählen Sie **Weiter**, um zu **Zusammenfassung** zu gelangen.

Schritt 6 von 6: Zusammenfassung überprüfen

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Notieren Sie sich in den nächsten Schritten die Details, die die zusätzliche Konfiguration beschreiben, die möglicherweise erforderlich ist, bevor Sie eine Verbindung zum S3-Client herstellen. Wenn Sie beispielsweise **als root anmelden** auswählen, gelangen Sie zum Tenant Manager, wo Sie Mandantenbenutzer hinzufügen, zusätzliche Buckets erstellen und Bucket-Einstellungen aktualisieren können.
3. Wählen Sie **Fertig**.
4. Konfigurieren Sie die Anwendung mit der Datei, die Sie von StorageGRID heruntergeladen haben, oder mit den manuell erhaltenen Werten.

Managen von HA-Gruppen

Verwaltung von Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen): Übersicht

Die Netzwerkschnittstellen mehrerer Admin- und Gateway-Nodes können in einer HA-Gruppe (High Availability, Hochverfügbarkeit) gruppieren. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload verwalten.

Was ist eine HA-Gruppe?

Darüber hinaus können HA-Gruppen (High Availability, Hochverfügbarkeit) für hochverfügbare Datenverbindungen für S3 und Swift Clients verwendet oder hochverfügbare Verbindungen mit dem Grid Manager und dem Mandanten Manager hergestellt werden.

Jede HA-Gruppe bietet Zugriff auf die Shared Services auf den ausgewählten Nodes.

- HA-Gruppen, die Gateway-Nodes, Admin-Nodes oder beide umfassen, bieten hochverfügbare Datenverbindungen für S3- und Swift-Clients.
- HA-Gruppen, die nur Admin-Nodes enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und dem Mandanten-Manager.
- Eine HA-Gruppe, die nur SG100- oder SG1000-Appliances und VMware-basierte Software-Nodes enthält, kann für hochverfügbare Verbindungen bereitstellen "[S3-Mandanten, die S3 Select nutzen](#)". HA-Gruppen werden empfohlen, wenn S3 Select verwendet wird, jedoch nicht erforderlich.

Wie erstellen Sie eine HA-Gruppe?

1. Sie wählen eine Netzwerkschnittstelle für einen oder mehrere Admin-Nodes oder Gateway-Knoten aus.

Sie können eine Grid Network (eth0)-Schnittstelle, eine eth2-Schnittstelle (Client Network), eine VLAN-Schnittstelle oder eine Access-Interface verwenden, die Sie dem Node hinzugefügt haben.



Sie können einer HA-Gruppe keine Schnittstelle hinzufügen, wenn ihr eine DHCP-zugewiesene IP-Adresse zugewiesen ist.

2. Sie geben an, dass die primäre Schnittstelle sein soll. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.
3. Sie bestimmen die Prioritätsreihenfolge für alle Backup-Schnittstellen.
4. Sie weisen der Gruppe eine bis 10 virtuelle IP-Adressen (VIP) zu. Client-Anwendungen können eine dieser VIP-Adressen verwenden, um eine Verbindung zu StorageGRID herzustellen.

Anweisungen hierzu finden Sie unter ["Konfigurieren Sie Hochverfügbarkeitsgruppen"](#).

Was ist die aktive Schnittstelle?

Im normalen Betrieb werden alle VIP-Adressen für die HA-Gruppe der primären Schnittstelle hinzugefügt, die die erste Schnittstelle in der Prioritätsreihenfolge ist. Solange die primäre Schnittstelle verfügbar bleibt, wird sie verwendet, wenn sich Clients mit einer beliebigen VIP-Adresse für die Gruppe verbinden. Das heißt, während des normalen Betriebs ist die primäre Schnittstelle die Schnittstelle „Active“ für die Gruppe.

Ebenso fungieren alle Schnittstellen mit niedriger Priorität für die HA-Gruppe im normalen Betrieb als „Backup“-Schnittstellen. Diese Backup-Schnittstellen werden nur dann verwendet, wenn die primäre (derzeit aktive) Schnittstelle nicht mehr verfügbar ist.

Anzeigen des aktuellen HA-Gruppen-Status eines Node

Um zu ermitteln, ob ein Node einer HA-Gruppe zugewiesen ist und seinen aktuellen Status ermittelt, wählen Sie **NODES > Node** aus.

Wenn die Registerkarte **Übersicht** einen Eintrag für **HA-Gruppen** enthält, wird der Knoten den aufgeführten HA-Gruppen zugewiesen. Der Wert nach dem Gruppennamen ist der aktuelle Status des Node in der HA-Gruppe:

- **Aktiv:** Die HA-Gruppe wird derzeit auf diesem Knoten gehostet.
- **Backup:** Die HA-Gruppe benutzt derzeit nicht diesen Knoten; dies ist ein Backup Interface.
- **Angehalten:** Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, da der Dienst hohe Verfügbarkeit (keepalived) manuell angehalten wurde.
- **Fault:** Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, weil einer oder mehrere der folgenden:
 - Der Lastverteilungsservice (nginx-gw) wird auf dem Knoten nicht ausgeführt.
 - Die eth0- oder VIP-Schnittstelle des Node ist nicht aktiv.
 - Der Node ist ausgefallen.

In diesem Beispiel wurde der primäre Admin-Node zwei HA-Gruppen hinzugefügt. Dieser Knoten ist derzeit die aktive Schnittstelle für die Gruppe Admin-Clients und eine Sicherungsschnittstelle für die Gruppe FabricPool-Clients.

DC1-ADM1 (Primary Admin Node) [🔗](#)

Overview Hardware Network Storage Load balancer Tasks

Node information [?](#)

Name: DC1-ADM1

Type: Primary Admin Node

ID: ce00d9c8-8a79-4742-bdef-c9c658db5315

Connection state: ✔ Connected

Software version: 11.6.0 (build 20211207.1804.614bc17)

HA groups: Admin clients (Active)
FabricPool clients (Backup)

IP addresses: 172.16.1.225 - eth0 (Grid Network)
10.224.1.225 - eth1 (Admin Network)
47.47.0.2, 47.47.1.225 - eth2 (Client Network)

[Show additional IP addresses](#) ▼

Was geschieht, wenn die aktive Schnittstelle ausfällt?

Die Schnittstelle, die derzeit die VIP-Adressen hostet, ist die aktive Schnittstelle. Wenn die HA-Gruppe mehrere Schnittstellen umfasst und die aktive Schnittstelle ausfällt, verschieben sich die VIP-Adressen auf die erste verfügbare Backup-Schnittstelle in der Prioritätsreihenfolge. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten verfügbaren Backup-Schnittstelle usw.

Ein Failover kann aus einem der folgenden Gründe ausgelöst werden:

- Der Node, auf dem die Schnittstelle konfiguriert ist, schaltet sich aus.
- Der Node, auf dem die Schnittstelle konfiguriert ist, verliert mindestens 2 Minuten lang die Verbindung zu allen anderen Nodes.
- Die aktive Schnittstelle ausfällt.
- Der Lastverteiler-Dienst wird angehalten.
- Der High Availability Service stoppt.



Der Failover wird möglicherweise nicht durch Netzwerkausfälle außerhalb des Node ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird Failover nicht von den Diensten für den Grid Manager oder den Tenant Manager ausgelöst.

Der Failover-Prozess dauert in der Regel nur wenige Sekunden und ist schnell genug, dass Client-Applikationen nur geringe Auswirkungen haben und sich auf normale Wiederholungsmuster verlassen können, um den Betrieb fortzusetzen.

Wenn ein Fehler behoben ist und eine Schnittstelle mit höherer Priorität wieder verfügbar wird, werden die VIP-Adressen automatisch auf die verfügbare Schnittstelle mit der höchsten Priorität verschoben.

Wie werden HA-Gruppen verwendet?

Es können HA-Gruppen (High Availability, Hochverfügbarkeit) verwendet werden, um hochverfügbare Verbindungen zu StorageGRID für Objektdaten und zur Verwendung durch den Administrator zur Verfügung zu stellen.

- Eine HA-Gruppe kann hochverfügbare administrative Verbindungen mit dem Grid Manager oder dem Mandanten Manager bereitstellen.
- Eine HA-Gruppe kann hochverfügbare Datenverbindungen für S3 und Swift Clients bieten.
- Eine HA-Gruppe, die nur eine Schnittstelle enthält, ermöglicht es Ihnen, viele VIP-Adressen bereitzustellen und explizit IPv6-Adressen festzulegen.

Eine HA-Gruppe kann nur Hochverfügbarkeit bieten, wenn alle Nodes in der Gruppe dieselben Services bereitstellen. Wenn Sie eine HA-Gruppe erstellen, fügen Sie Schnittstellen von den Typen von Nodes hinzu, die die erforderlichen Services bereitstellen.

- **Admin Nodes:** Schließen Sie den Load Balancer Service ein und ermöglichen Sie den Zugriff auf den Grid Manager oder den Tenant Manager.
- **Gateway Nodes:** Fügen Sie den Load Balancer Service ein.

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
Zugriff auf Grid Manager	<ul style="list-style-type: none">• Primärer Admin-Node (Primär)• Nicht primäre Admin-Nodes <p>Hinweis: der primäre Admin-Knoten muss die primäre Schnittstelle sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.</p>
Zugriff nur auf Tenant Manager	<ul style="list-style-type: none">• Primäre oder nicht primäre Admin-Nodes
S3- oder Swift-Client-Zugriff – Load Balancer Service	<ul style="list-style-type: none">• Admin-Nodes• Gateway-Nodes
S3-Client-Zugriff für "S3 Select"	<ul style="list-style-type: none">• SG100- oder SG1000-Appliances• VMware-basierte Software-Nodes <p>Hinweis: HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, aber nicht erforderlich.</p>

Einschränkungen bei der Verwendung von HA-Gruppen mit Grid Manager oder Tenant Manager

Wenn ein Grid Manager oder der Tenant Manager-Dienst ausfällt, wird das Failover von HA-Gruppen nicht ausgelöst.

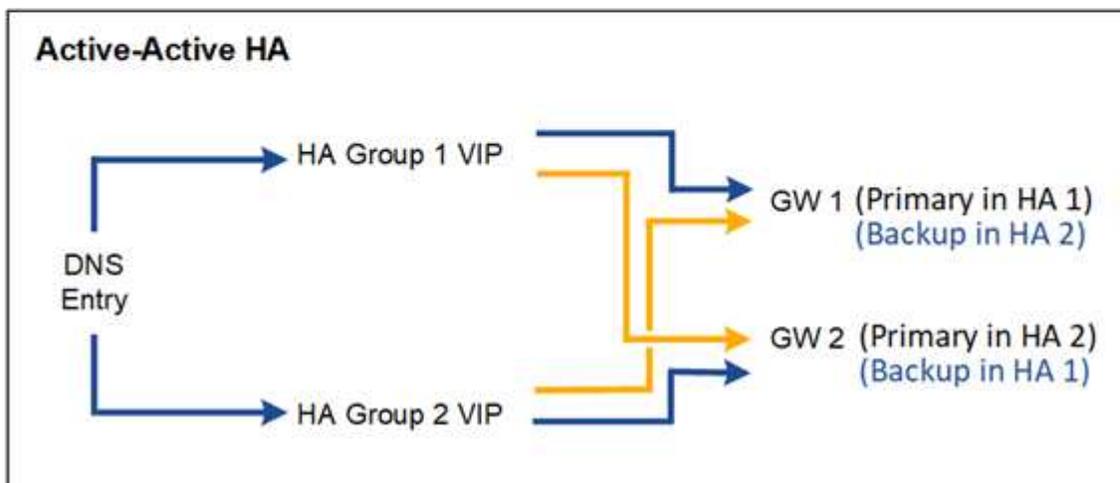
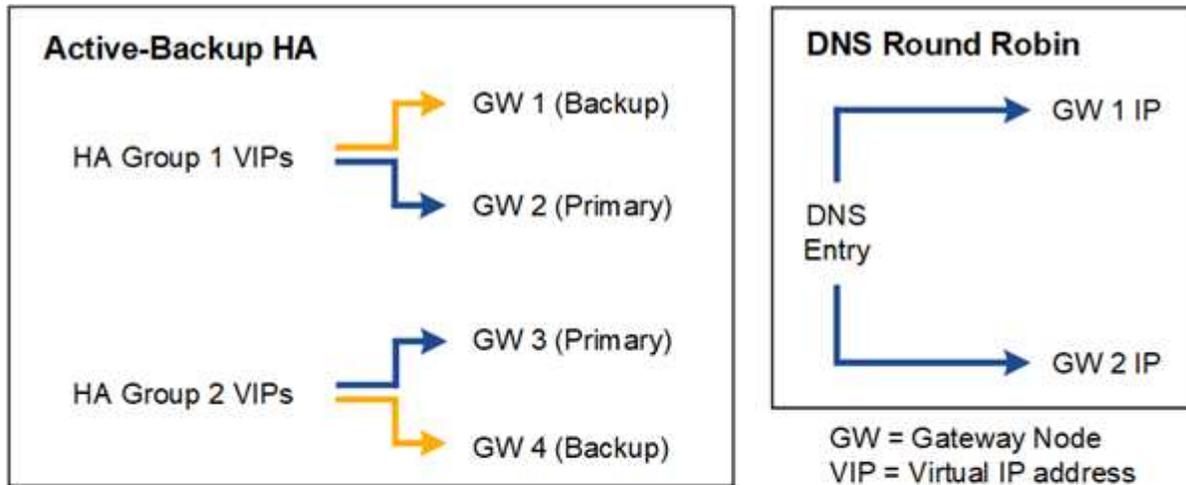
Wenn Sie sich bei einem Failover beim Grid Manager oder beim Tenant Manager angemeldet haben, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

Einige Wartungsverfahren können nicht durchgeführt werden, wenn der primäre Admin-Node nicht verfügbar ist. Während des Failovers können Sie Ihr StorageGRID-System mit dem Grid-Manager überwachen.

Konfigurationsoptionen für HA-Gruppen

Die folgenden Diagramme bieten Beispiele für verschiedene Möglichkeiten zum Konfigurieren von HA-Gruppen. Jede Option hat vor- und Nachteile.

In den Diagrammen zeigt blau die primäre Schnittstelle in der HA-Gruppe an und gelb gibt die Backup-Schnittstelle in der HA-Gruppe an.



Die Tabelle enthält eine Zusammenfassung der Vorteile der einzelnen HA-Konfigurationen, die in der Abbildung dargestellt sind.

Konfiguration	Vorteile	Nachteile
Aktiv/Backup HA	<ul style="list-style-type: none"> Management über StorageGRID ohne externe Abhängigkeiten Schnelles Failover. 	<ul style="list-style-type: none"> In einer HA-Gruppe ist nur ein Node aktiv. Mindestens ein Node pro HA-Gruppe bleibt im Ruhezustand.

Konfiguration	Vorteile	Nachteile
DNS Round Robin	<ul style="list-style-type: none"> • Erhöhter Aggregatdurchsatz: • Keine leerlaufenden Hosts 	<ul style="list-style-type: none"> • Langsamer Failover, der vom Client-Verhalten abhängen kann. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.
Aktiv/aktiv-HA	<ul style="list-style-type: none"> • Der Datenverkehr wird über mehrere HA-Gruppen verteilt. • Hoher Aggregatdurchsatz, der mit der Anzahl der HA-Gruppen skaliert werden kann • Schnelles Failover. 	<ul style="list-style-type: none"> • Komplexer zu konfigurieren. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.

Konfigurieren Sie Hochverfügbarkeitsgruppen

Sie können Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) konfigurieren, um hochverfügbaren Zugriff auf die Services in Admin-Nodes oder Gateway-Nodes bereitzustellen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung.
- Wenn Sie eine VLAN-Schnittstelle in einer HA-Gruppe verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe ["Konfigurieren Sie die VLAN-Schnittstellen"](#).
- Wenn Sie eine Zugriffsoberfläche für einen Node in einer HA-Gruppe verwenden möchten, haben Sie die Schnittstelle erstellt:
 - **Red hat Enterprise Linux oder CentOS (vor der Installation des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **Ubuntu oder Debian (vor der Installation des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **Linux (nach der Installation des Knotens):** ["Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)
 - **VMware (nach der Installation des Knotens):** ["VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)

Erstellen Sie eine Hochverfügbarkeitsgruppe

Wenn Sie eine Hochverfügbarkeitsgruppe erstellen, wählen Sie eine oder mehrere Schnittstellen aus und organisieren sie in Prioritätsreihenfolge. Anschließend weisen Sie der Gruppe eine oder mehrere VIP-Adressen zu.

Eine Schnittstelle muss lauten, damit ein Gateway-Node oder ein Admin-Node in einer HA-Gruppe enthalten sein kann. Eine HA-Gruppe kann nur eine Schnittstelle für jeden angegebenen Node verwenden. Jedoch können andere Schnittstellen für denselben Node in anderen HA-Gruppen verwendet werden.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **CONFIGURATION > Network > High Availability groups**.
2. Wählen Sie **Erstellen**.

Geben Sie Details für die HA-Gruppe ein

Schritte

1. Geben Sie einen eindeutigen Namen für die HA-Gruppe ein.
2. Geben Sie optional eine Beschreibung für die HA-Gruppe ein.
3. Wählen Sie **Weiter**.

Fügen Sie der HA-Gruppe Schnittstellen hinzu

Schritte

1. Wählen Sie eine oder mehrere Schnittstellen aus, die dieser HA-Gruppe hinzugefügt werden sollen.

Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Search... Total interface count: 4

Node	Interface	Site	IPv4 subnet	Node type
<input type="checkbox"/> DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
<input type="checkbox"/> DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected

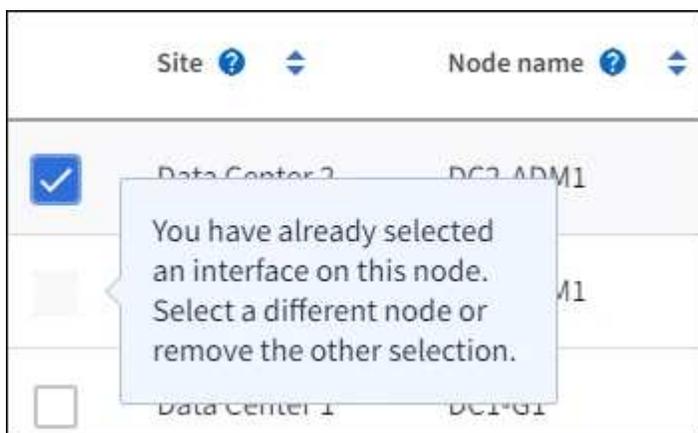


Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

Richtlinien für die Auswahl von Schnittstellen

- Sie müssen mindestens eine Schnittstelle auswählen.
- Sie können nur eine Schnittstelle für einen Node auswählen.
- Wenn die HA-Gruppe den HA-Schutz von Admin Node-Services bietet, zu denen der Grid Manager und der MandantenManager gehören, wählen Sie nur Schnittstellen zu Admin-Nodes aus.

- Wenn die HA-Gruppe einen HA-Schutz für den Client-Datenverkehr von S3 oder Swift bietet, wählen Sie Schnittstellen an Admin-Nodes, Gateway Nodes oder beiden.
- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen, wird ein Informationshinweis angezeigt. Sie werden daran erinnert, dass bei einem Failover Dienste, die vom zuvor aktiven Knoten bereitgestellt werden, möglicherweise auf dem neu aktiven Knoten nicht verfügbar sind. Ein Backup-Gateway-Node kann beispielsweise keinen HA-Schutz für Admin-Node-Services bereitstellen. Ebenso kann ein Backup-Admin-Node nicht alle Wartungsverfahren durchführen, die der primäre Admin-Node bereitstellen kann.
- Wenn Sie keine Schnittstelle auswählen können, ist das Kontrollkästchen deaktiviert. Der QuickInfo enthält weitere Informationen.



- Eine Schnittstelle kann nicht ausgewählt werden, wenn ihr Subnetzwerk oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Sie können keine konfigurierte Schnittstelle auswählen, wenn diese keine statische IP-Adresse hat.

2. Wählen Sie **Weiter**.

Legen Sie die **Prioritätsreihenfolge** fest

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst, können Sie feststellen, welche primäre Schnittstelle und welche Backup-Schnittstellen (Failover) sind. Wenn die primäre Schnittstelle fehlschlägt, werden die VIP-Adressen zur Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität usw. verschoben.

Schritte

1. Ziehen Sie Zeilen in die Spalte **Priority order**, um die primäre Schnittstelle und alle Backup-Schnittstellen zu bestimmen.

Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order 	Node	Interface 	Node type 
1 (Primary interface)	 DC1-ADM1-104-96 	eth2	Primary Admin Node
2	 DC2-ADM1-104-103 	eth2	Admin Node



Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

2. Wählen Sie **Weiter**.

Geben Sie die IP-Adressen ein

Schritte

1. Geben Sie im Feld **Subnetz CIDR** das VIP-Subnetz in CIDR-Notation an - eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32).

Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: 192.16.0.0/22.



Wenn Sie ein 32-Bit-Präfix verwenden, dient die VIP-Netzwerkadresse auch als Gateway-Adresse und VIP-Adresse.

Enter details for the HA group

Subnet CIDR 

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) 

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address 

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

- Wenn auf diese VIP-Adressen von S3-, Swift-, Administrations- oder Mandantenclients aus einem anderen Subnetz zugegriffen wird, geben Sie die **Gateway IP-Adresse** ein. Die Gateway-Adresse muss sich im VIP-Subnetz befinden.

Client- und Admin-Benutzer verwenden dieses Gateway, um auf die virtuellen IP-Adressen zuzugreifen.

- Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden, und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein.

Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

- Wählen Sie **HA-Gruppe erstellen** und wählen Sie **Fertig**.

Die HA-Gruppe wird erstellt. Sie können jetzt die konfigurierten virtuellen IP-Adressen verwenden.



Warten Sie bis zu 15 Minuten, bis Änderungen an einer HA-Gruppe auf alle Nodes angewendet werden.

Nächste Schritte

Wenn Sie diese HA-Gruppe zum Lastausgleich verwenden möchten, erstellen Sie einen Endpunkt zum Load Balancer, um den Port und das Netzwerkprotokoll zu ermitteln und die erforderlichen Zertifikate anzuschließen. Siehe "[Konfigurieren von Load Balancer-Endpunkten](#)".

Bearbeiten Sie eine Hochverfügbarkeitsgruppe

Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) bearbeiten, um ihren Namen und ihre Beschreibung zu ändern, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern

oder virtuelle IP-Adressen hinzuzufügen oder zu aktualisieren.

Beispielsweise müssen Sie möglicherweise eine HA-Gruppe bearbeiten, wenn Sie den Node, der einer ausgewählten Schnittstelle zugeordnet ist, entfernen möchten, wenn Sie ihn an einem Standort ausmustern oder einem Node entfernen möchten.

Schritte

1. Wählen Sie **CONFIGURATION > Network > High Availability groups**.

Auf der Seite „Hochverfügbarkeitsgruppen“ werden alle vorhandenen HA-Gruppen angezeigt.

2. Aktivieren Sie das Kontrollkästchen für die HA-Gruppe, die Sie bearbeiten möchten.
3. Führen Sie einen der folgenden Schritte aus, je nachdem, was Sie aktualisieren möchten:
 - Wählen Sie **Aktionen > virtuelle IP-Adresse bearbeiten**, um VIP-Adressen hinzuzufügen oder zu entfernen.
 - Wählen Sie **Aktionen > HA-Gruppe bearbeiten** aus, um den Namen oder die Beschreibung der Gruppe zu aktualisieren, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern oder VIP-Adressen hinzuzufügen oder zu entfernen.
4. Wenn Sie **virtuelle IP-Adresse bearbeiten** ausgewählt haben:
 - a. Aktualisieren Sie die virtuellen IP-Adressen für die HA-Gruppe.
 - b. Wählen Sie **Speichern**.
 - c. Wählen Sie **Fertig**.
5. Wenn Sie **HA-Gruppe bearbeiten** ausgewählt haben:
 - a. Optional können Sie den Namen oder die Beschreibung der Gruppe aktualisieren.
 - b. Aktivieren oder deaktivieren Sie optional die Kontrollkästchen, um Schnittstellen hinzuzufügen oder zu entfernen.



Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden

- c. Optional können Sie Zeilen ziehen, um die Prioritätsreihenfolge der primären Schnittstelle und aller Backup-Schnittstellen für diese HA-Gruppe zu ändern.
- d. Optional können Sie die virtuellen IP-Adressen aktualisieren.
- e. Wählen Sie **Speichern** und dann **Fertig stellen**.



Warten Sie bis zu 15 Minuten, bis Änderungen an einer HA-Gruppe auf alle Nodes angewendet werden.

Entfernen Sie eine Hochverfügbarkeitsgruppe

Sie können eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) gleichzeitig entfernen.



Sie können eine HA-Gruppe nicht entfernen, wenn sie an einen Load Balancer-Endpunkt gebunden ist. Zum Löschen einer HA-Gruppe müssen Sie sie von allen Endpunkten der Load Balancer entfernen, die sie verwenden.

Um Client-Unterbrechungen zu vermeiden, aktualisieren Sie die betroffenen S3- oder Swift-Client-Applikationen, bevor Sie eine HA-Gruppe entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über eine andere IP-Adresse herzustellen, z. B. die virtuelle IP-Adresse einer anderen HA-Gruppe oder die IP-Adresse, die während der Installation für eine Schnittstelle konfiguriert wurde.

Schritte

1. Wählen Sie **CONFIGURATION > Network > High Availability groups**.
2. Überprüfen Sie die Spalte **Load Balancer Endpunkte** für jede HA-Gruppe, die Sie entfernen möchten. Wenn Load Balancer-Endpunkte aufgeführt sind:
 - a. Gehen Sie zu **CONFIGURATION > Network > Load Balancer Endpunkte**.
 - b. Aktivieren Sie das Kontrollkästchen für den Endpunkt.
 - c. Wählen Sie **Aktionen > Endpunktbindungsmodus bearbeiten**.
 - d. Aktualisieren Sie den Bindungsmodus, um die HA-Gruppe zu entfernen.
 - e. Wählen Sie **Änderungen speichern**.
3. Wenn keine Load Balancer-Endpunkte aufgeführt sind, aktivieren Sie das Kontrollkästchen für jede HA-Gruppe, die Sie entfernen möchten.
4. Wählen Sie **actions > Remove HA Group**.
5. Überprüfen Sie die Nachricht und wählen Sie **HA-Gruppe löschen**, um Ihre Auswahl zu bestätigen.

Alle von Ihnen ausgewählten HA-Gruppen werden entfernt. Ein grünes Banner wird auf der Seite „Hochverfügbarkeitsgruppen“ angezeigt.

Managen Sie den Lastausgleich

Überlegungen zum Lastausgleich

Mit Lastausgleich können Workloads bei der Aufnahme und dem Abruf von S3 und Swift Clients genutzt werden.

Was ist Load Balancing?

Wenn eine Client-Applikation Daten eines StorageGRID Systems speichert oder abrufen, verwendet StorageGRID einen Load Balancer, um den Aufnahme- und Abruf-Workload zu managen. Load Balancing maximiert die Geschwindigkeit und die Verbindungskapazität, indem der Workload auf mehrere Storage Nodes verteilt wird.

Der StorageGRID Load Balancer-Service wird auf allen Admin-Nodes und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Sie beendet die TLS-Beendigung von Client-Anforderungen, prüft die Anforderungen und stellt neue sichere Verbindungen zu den Storage-Nodes her.

Der Load Balancer-Service auf jedem Node wird unabhängig ausgeführt, wenn der Client-Datenverkehr an die Storage Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter.



Obwohl der StorageGRID Load Balancer-Service der empfohlene Load-Balancing-Mechanismus ist, können Sie stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp Ansprechpartner oder unter ["TR-4626: StorageGRID Anbieter- und Global Load Balancer"](#).

Wie viele Nodes für Lastausgleich benötige ich?

Als allgemeine Best Practice sollte jeder Standort in Ihrem StorageGRID-System zwei oder mehr Nodes mit dem Load Balancer Service umfassen. Ein Standort kann beispielsweise zwei Gateway-Nodes oder einen Admin-Node und einen Gateway-Node umfassen. Vergewissern Sie sich, dass für jeden Load-Balancing-Node eine entsprechende Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur vorhanden ist, unabhängig davon, ob Sie SG100- oder SG1000-Servicegeräte, Bare Metal-Nodes oder VM-basierte Nodes verwenden.

Was ist ein Endpunkt eines Load Balancers?

Ein Load Balancer-Endpunkt definiert den Port und das Netzwerkprotokoll (HTTPS oder HTTP), über das eingehende und ausgehende Client-Anwendungsanforderungen auf die Knoten zugreifen, die den Load Balancer-Dienst enthalten. Der Endpunkt definiert außerdem den Client-Typ (S3 oder Swift), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten.

Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie entweder **CONFIGURATION > Network > Load Balancer-Endpunkte** oder schließen Sie den FabricPool- und S3-Setup-Assistenten ab. Weitere Informationen:

- ["Konfigurieren von Load Balancer-Endpunkten"](#)
- ["Verwenden Sie den S3-Einrichtungsassistenten"](#)
- ["Verwenden Sie den FabricPool-Einrichtungsassistenten"](#)

Überlegungen zum Port

Der Port für einen Load Balancer-Endpunkt ist für den ersten erstellten Endpunkt standardmäßig auf 10433 gesetzt. Sie können jedoch einen beliebigen nicht verwendeten externen Port zwischen 1 und 65535 angeben. Wenn Sie Port 80 oder 443 verwenden, verwendet der Endpunkt nur den Load Balancer-Dienst auf Gateway-Nodes. Diese Ports sind für Admin-Nodes reserviert. Wenn Sie denselben Port für mehr als einen Endpunkt verwenden, müssen Sie für jeden Endpunkt einen anderen Bindungsmodus angeben.

Von anderen Netzdiensten verwendete Ports sind nicht zulässig. Siehe ["Referenz für Netzwerk-Ports"](#).

Überlegungen zum Netzwerkprotokoll

In den meisten Fällen sollte für die Verbindungen zwischen Client-Anwendungen und StorageGRID die TLS-Verschlüsselung (Transport Layer Security) verwendet werden. Eine Verbindung mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen, insbesondere in Produktionsumgebungen. Wenn Sie das Netzwerkprotokoll für den StorageGRID Load Balancer-Endpunkt auswählen, sollten Sie **HTTPS** auswählen.

Überlegungen für Load Balancer-Endpunktzertifikate

Wenn Sie **HTTPS** als Netzwerkprotokoll für den Load Balancer-Endpunkt auswählen, müssen Sie ein Sicherheitszertifikat angeben. Beim Erstellen des Load Balancer-Endpunkts können Sie eine der folgenden drei Optionen verwenden:

- **Laden Sie ein signiertes Zertifikat hoch (empfohlen).** Dieses Zertifikat kann entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert werden. Die Verwendung eines öffentlich vertrauenswürdigen CA-Serverzertifikats zum Sichern der Verbindung ist die beste Methode. Im Gegensatz zu generierten Zertifikaten können von einer CA signierte Zertifikate unterbrechungsfrei gedreht werden, was dazu beitragen kann, Ablaufprobleme zu vermeiden.

Sie müssen die folgenden Dateien abrufen, bevor Sie den Load Balancer-Endpunkt erstellen:

- Die Zertifikatdatei des benutzerdefinierten Servers.
- Die Datei mit dem privaten Schlüssel des benutzerdefinierten Serverzertifikats.
- Optional ein CA-Bündel der Zertifikate jeder zwischengeschalteten Zertifizierungsstelle.
- **Generieren Sie ein selbst signiertes Zertifikat.**
- **Verwenden Sie das globale StorageGRID S3 und Swift Zertifikat.** Sie müssen eine benutzerdefinierte Version dieses Zertifikats hochladen oder generieren, bevor Sie es für den Load Balancer-Endpoint auswählen können. Siehe "[Konfigurieren von S3- und Swift-API-Zertifikaten](#)".

Welche Werte brauche ich?

Zum Erstellen des Zertifikats müssen Sie alle Domännennamen und IP-Adressen kennen, die von S3- oder Swift-Client-Anwendungen für den Zugriff auf den Endpoint verwendet werden.

Der Eintrag **Subject DN** (Distinguished Name) für das Zertifikat muss den vollständig qualifizierten Domännennamen enthalten, den die Client-Anwendung für StorageGRID verwendet. Beispiel:

```
Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Bei Bedarf kann das Zertifikat Platzhalter verwenden, um die vollständig qualifizierten Domännennamen aller Admin-Nodes und Gateway-Nodes darzustellen, auf denen der Load Balancer-Dienst ausgeführt wird. Beispiel: *.storagegrid.example.com Verwendet den Platzhalter * für die Darstellung adm1.storagegrid.example.com Und gn1.storagegrid.example.com.

Wenn Sie S3 Virtual Hosted-Style-Anfragen verwenden möchten, muss das Zertifikat für jeden Eintrag auch einen **Alternative Name**-Eintrag enthalten "[Der Domänenname des S3-Endpunkts](#)" Sie haben konfiguriert, einschließlich aller Platzhalternamen. Beispiel:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Wenn Sie Platzhalter für Domännennamen verwenden, lesen Sie die "[Härtungsrichtlinien für Serverzertifikate](#)".

Außerdem müssen Sie für jeden Namen im Sicherheitszertifikat einen DNS-Eintrag definieren.

Wie verwalte ich auslaufende Zertifikate?



Wenn das Zertifikat, mit dem die Verbindung zwischen der S3-Anwendung und StorageGRID gesichert wird, abläuft, kann die Applikation möglicherweise vorübergehend den Zugriff auf StorageGRID verlieren.

Befolgen Sie die folgenden Best Practices, um Probleme mit dem Ablauf von Zertifikaten zu vermeiden:

- Überwachen Sie sorgfältig alle Warnungen, die darauf hinweisen, dass sich das Ablaufdatum des Zertifikats nähert, z. B. das Endpunktzertifikat **Ablauf des Load Balancer** und **Ablauf des globalen Serverzertifikats für S3- und Swift-API**-Warnungen.
- Halten Sie die Versionen des Zertifikats für die StorageGRID- und S3-Anwendung immer synchron. Wenn

Sie das für einen Load Balancer-Endpunkt verwendete Zertifikat ersetzen oder erneuern, müssen Sie das von der S3-Anwendung verwendete entsprechende Zertifikat ersetzen oder erneuern.

- Ein öffentlich signiertes CA-Zertifikat verwenden. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie bald abgelaufene Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat generiert haben und dieses Zertifikat kurz vor dem Ablauf steht, müssen Sie das Zertifikat sowohl in StorageGRID als auch in der S3-Anwendung manuell ersetzen, bevor das vorhandene Zertifikat abläuft.

Überlegungen zum Bindungsmodus

Im Bindungsmodus können Sie festlegen, welche IP-Adressen für den Zugriff auf einen Load Balancer-Endpunkt verwendet werden können. Wenn ein Endpunkt einen Bindungsmodus verwendet, können Clientanwendungen nur auf den Endpunkt zugreifen, wenn sie eine zulässige IP-Adresse oder den entsprechenden vollständig qualifizierten Domännennamen (FQDN) verwenden. Client-Anwendungen, die eine andere IP-Adresse oder FQDN verwenden, können nicht auf den Endpunkt zugreifen.

Sie können einen der folgenden Bindungsmodi festlegen:

- **Global** (Standard): Client-Anwendungen können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie diese Einstellung, es sei denn, Sie müssen den Zugriff auf einen Endpunkt einschränken.
- **Virtuelle IPs von HA-Gruppen**. Client-Anwendungen müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden.
- **Knotentyp**. Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden.

Überlegungen für den Mandantenzugriff

Der Mandantenzugriff ist eine optionale Sicherheitsfunktion, mit der Sie steuern können, welche StorageGRID-Mandantenkonten einen Load-Balancer-Endpunkt für den Zugriff auf ihre Buckets verwenden können. Sie können allen Mandanten den Zugriff auf einen Endpunkt erlauben (Standard), oder Sie können eine Liste der zulässigen oder blockierten Mandanten für jeden Endpunkt festlegen.

Sie können diese Funktion nutzen, um eine bessere Sicherheitsisolierung zwischen Mandanten und ihren Endpunkten zu ermöglichen. Mit dieser Funktion können Sie beispielsweise sicherstellen, dass die streng geheimen oder streng klassifizierten Materialien eines Mandanten für andere Mieter nicht zugänglich sind.



Für die Zugriffssteuerung wird der Mandant aus den Zugriffsschlüsseln ermittelt, die in der Client-Anfrage verwendet werden. Wenn im Rahmen der Anfrage keine Zugriffsschlüssel angegeben werden (z. B. mit anonymem Zugriff), wird der Bucket-Eigentümer zur Ermittlung des Mandanten verwendet.

Beispiel für Mandantenzugriff

Um zu verstehen, wie diese Sicherheitsfunktion funktioniert, betrachten Sie das folgende Beispiel:

1. Sie haben zwei Lastausgleichsendpunkte wie folgt erstellt:

- **Öffentlicher** Endpunkt: Nutzt Port 10443 und erlaubt den Zugriff auf alle Mandanten.
- **Top secret** Endpunkt: Verwendet Port 10444 und erlaubt nur den Zugriff auf den **Top secret** Mieter. Alle anderen Mandanten werden für den Zugriff auf diesen Endpunkt gesperrt.

2. Der `top-secret.pdf` Befindet sich in einem Eimer im Besitz des **Top Secret** Mieters.

Um auf den zuzugreifen `top-secret.pdf` Ein Benutzer im **Top Secret**-Mieter kann eine GET-Anfrage an ausstellen `https://w.x.y.z:10444/top-secret.pdf`. Da dieser Mandant den Endpunkt 10444 verwenden darf, kann der Benutzer auf das Objekt zugreifen. Wenn ein Benutzer eines anderen Mandanten jedoch dieselbe Anforderung an dieselbe URL ausgibt, erhält er eine Meldung über „Zugriff verweigert“. Der Zugriff wird verweigert, selbst wenn die Anmeldeinformationen und die Signatur gültig sind.

CPU-Verfügbarkeit

Der Load Balancer Service läuft auf jedem Admin-Node und Gateway-Node unabhängig, wenn der S3- oder Swift-Datenverkehr zu den Storage-Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter. Die Informationen zur CPU-Auslastung des Knotens werden alle paar Minuten aktualisiert. Die Gewichtung kann jedoch häufiger aktualisiert werden. Allen Storage-Nodes wird ein Mindestwert für das Basisgewicht zugewiesen, selbst wenn ein Node eine Auslastung von 100 % meldet oder seine Auslastung nicht meldet.

In manchen Fällen sind die Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich der Load Balancer Service befindet.

Konfigurieren von Load Balancer-Endpunkten

Load Balancer-Endpunkte bestimmen die Ports und Netzwerkprotokolle S3 und Swift-Clients können beim Herstellen einer Verbindung zum StorageGRID Load Balancer auf Gateway und Admin-Nodes verwendet werden.



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben die geprüft "[Überlegungen zum Lastausgleich](#)".
- Wenn Sie zuvor einen Port neu zugeordnet haben, den Sie für den Load Balancer-Endpunkt verwenden möchten, haben Sie diesen "[Port-Remap wurde entfernt](#)".
- Sie haben alle Hochverfügbarkeitsgruppen (High Availability groups, die Sie verwenden möchten, erstellt. HA-Gruppen werden empfohlen, jedoch nicht erforderlich. Siehe "[Management von Hochverfügbarkeitsgruppen](#)".
- Wenn der Endpunkt des Load Balancer verwendet wird "[S3 Mandanten für S3 Select](#)", Es darf die IP-Adressen oder FQDNs von Bare-Metal-Knoten nicht verwenden. Für die bei S3 Select verwendeten Load Balancer-Endpunkte sind nur SG100- oder SG1000-Appliances und VMware-basierte Software-Nodes zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)".

- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), haben Sie die Informationen für das Serverzertifikat.



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

- Zum Hochladen eines Zertifikats benötigen Sie das Serverzertifikat, den privaten Zertifikatschlüssel und optional ein CA-Bundle.
- Zum Generieren eines Zertifikats benötigen Sie alle Domain-Namen und IP-Adressen, die S3- oder Swift-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen auch das Thema (Distinguished Name) kennen.
- Wenn Sie das StorageGRID S3- und Swift-API-Zertifikat verwenden möchten (das auch für direkte Verbindungen zu Speicherknoten verwendet werden kann), haben Sie das Standardzertifikat bereits durch ein benutzerdefiniertes Zertifikat ersetzt, das von einer externen Zertifizierungsstelle signiert ist. Siehe "[Konfigurieren von S3- und Swift-API-Zertifikaten](#)".

Erstellen Sie einen Endpunkt für den Load Balancer

Jeder Load Balancer-Endpunkt gibt einen Port, einen Client-Typ (S3 oder Swift) und ein Netzwerkprotokoll (HTTP oder HTTPS) an.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **CONFIGURATION > Network > Load Balancer Endpunkte**.
2. Wählen Sie **Erstellen**.

Geben Sie Details zu Endpunkten ein

Schritte

1. Geben Sie Details für den Endpunkt ein.

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt. Sie können jedoch einen beliebigen nicht verwendeten externen Port zwischen 1 und 65535 eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert. Diese Ports sind für Admin-Nodes reserviert.
Client-Typ	Der Typ der Client-Anwendung, die diesen Endpunkt verwenden wird, entweder S3 oder Swift .

Feld	Beschreibung
Netzwerkprotokoll	<p>Das Netzwerkprotokoll, das Clients bei der Verbindung mit diesem Endpunkt verwenden werden.</p> <ul style="list-style-type: none"> • Wählen Sie HTTPS für sichere, TLS verschlüsselte Kommunikation (empfohlen). Sie müssen ein Sicherheitszertifikat anhängen, bevor Sie den Endpunkt speichern können. • Wählen Sie HTTP für eine weniger sichere, unverschlüsselte Kommunikation. Verwenden Sie HTTP nur für ein Grid, das nicht produktionsbereit ist.

2. Wählen Sie **Weiter**.

Wählen Sie einen Bindungsmodus aus

Schritte

1. Wählen Sie einen Bindungsmodus für den Endpunkt aus, um zu steuern, wie auf den Endpunkt zugegriffen wird—Verwenden einer beliebigen IP-Adresse oder Verwenden bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	<p>Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen.</p> <p>Verwenden Sie die Global-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.</p>
Virtuelle IPs von HA-Gruppen	<p>Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen.</p> <p>Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.</p>
Node-Schnittstellen	<p>Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.</p>
Node-Typ	<p>Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.</p>



Wenn mehr als ein Endpunkt denselben Port verwendet, verwendet StorageGRID diese Prioritätsreihenfolge, um zu entscheiden, welcher Endpunkt verwendet werden soll:
Virtuelle IPs von HA-Gruppen > Knotenschnittstellen > Knotentyp > global.

2. Wenn Sie **virtuelle IPs von HA-Gruppen** ausgewählt haben, wählen Sie eine oder mehrere HA-Gruppen aus.
3. Wenn Sie **Node-Schnittstellen** ausgewählt haben, wählen Sie für jeden Admin-Node oder Gateway-Node eine oder mehrere Node-Schnittstellen aus, die mit diesem Endpunkt verknüpft werden sollen.
4. Wenn Sie **Node type** ausgewählt haben, wählen Sie entweder Admin-Nodes aus, die sowohl den primären Admin-Node als auch alle nicht-primären Admin-Nodes enthalten, oder Gateway-Nodes.

Kontrolle des Mandantenzugriffs

Schritte

1. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben. Nachdem Sie Mandantenkonten hinzugefügt haben, können Sie den Load Balancer-Endpunkt bearbeiten, um bestimmte Konten zuzulassen oder zu blockieren.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen**, um den neuen Load Balancer-Endpunkt hinzuzufügen. Fahren Sie dann mit fort [Nachdem Sie fertig sind](#). Andernfalls wählen Sie **Weiter**, um das Zertifikat anzuhängen.

Zertifikat anhängen

Schritte

1. Wenn Sie einen **HTTPS**-Endpunkt erstellen, wählen Sie den Typ des Sicherheitszertifikats aus, das Sie an den Endpunkt anhängen möchten.

Das Zertifikat sichert die Verbindungen zwischen S3- und Swift-Clients und dem Load Balancer-Service auf Admin-Node oder Gateway-Nodes.

- **Zertifikat hochladen.** Wählen Sie diese Option aus, wenn Sie über benutzerdefinierte Zertifikate zum Hochladen verfügen.
- **Zertifikat generieren.** Wählen Sie diese Option aus, wenn Sie über die Werte verfügen, die zum Generieren eines benutzerdefinierten Zertifikats erforderlich sind.

- **Verwenden Sie StorageGRID S3 und Swift Zertifikat.** Wählen Sie diese Option aus, wenn Sie das globale S3- und Swift-API-Zertifikat verwenden möchten, das auch für direkte Verbindungen zu Storage-Nodes verwendet werden kann.

Sie können diese Option nur auswählen, wenn Sie das von der Grid-CA signierte Standard-API-Zertifikat S3 und Swift durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert wurde. Siehe "[Konfigurieren von S3- und Swift-API-Zertifikaten](#)".

2. Wenn Sie das StorageGRID S3- und Swift-Zertifikat nicht verwenden, laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

- a. Wählen Sie **Zertifikat hochladen**.
- b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
 - **Server-Zertifikat:** Die benutzerdefinierte Server-Zertifikatdatei in PEM-Kodierung.
 - **Zertifikat privater Schlüssel:** Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (.key).



Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket:** Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
- c. Erweitern Sie **Zertifikatdetails**, um die Metadaten für jedes hochgeladene Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.
 - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung .pem.

Beispiel: storagegrid_certificate.pem

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere Stelle zu kopieren.
- d. Wählen Sie **Erstellen**. + der Endpunkt des Load Balancer wird erstellt. Das individuelle Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3 und Swift Clients und dem Endpunkt verwendet.

Zertifikat wird generiert

- a. Wählen Sie **Zertifikat erstellen**.
- b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.

Feld	Beschreibung
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domännennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. Hinweis: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten für das generierte Zertifikat anzuzeigen.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

e. Wählen Sie **Erstellen**.

Der Endpunkt des Load Balancer wird erstellt. Das individuelle Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3 und Swift Clients und diesem Endpunkt verwendet.

Nachdem Sie fertig sind

Schritte

1. Wenn Sie einen DNS verwenden, stellen Sie sicher, dass der DNS einen Datensatz enthält, mit dem der vollständig qualifizierte StorageGRID-Domännennamen (FQDN) jeder IP-Adresse zugeordnet wird, die Clients zum Verbindungsaufbau verwenden.

Die IP-Adresse, die Sie im DNS-Datensatz eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Load-Balancing-Nodes verwenden:

- Wenn Sie eine HA-Gruppe konfiguriert haben, stellen Clients eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, stellen Clients mithilfe der IP-Adresse eines Gateway-Node oder Admin-Node eine Verbindung zum StorageGRID Load Balancer-Service her.

Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

2. S3- und Swift-Clients erhalten die für die Verbindung mit dem Endpunkt erforderlichen Informationen:

- Port-Nummer
- Vollständig qualifizierter Domain-Name oder IP-Adresse
- Alle erforderlichen Zertifikatsdetails

Load Balancer-Endpunkte anzeigen und bearbeiten

Sie können Details zu vorhandenen Load Balancer-Endpunkten anzeigen, einschließlich der Zertifikatmetadaten für einen gesicherten Endpunkt. Sie können auch den Namen oder den Bindungsmodus eines Endpunkts ändern und alle zugehörigen Zertifikate aktualisieren.

Sie können den Servicetyp (S3 oder Swift), den Port oder das Protokoll (HTTP oder HTTPS) nicht ändern.

- Um grundlegende Informationen für alle Load Balancer-Endpunkte anzuzeigen, lesen Sie die Tabelle auf der Seite Load Balancer Endpunkte durch.

<input type="checkbox"/>	Name ? ↕	Port ? ↕	Network protocol ? ↕	Binding mode ? ↕	Certificate expiration ? ↕
<input type="checkbox"/>	S3 load balancer endpoint	10443	HTTPS	Global	Jun 12th, 2024

- Um alle Details zu einem bestimmten Endpunkt einschließlich Zertifikatmetadaten anzuzeigen, wählen Sie in der Tabelle den Namen des Endpunkts aus.

S3 load balancer endpoint

Port: 10443
Client type: S3
Network protocol: HTTPS
Binding mode: Global
Endpoint ID: 3d02c126-9437-478c-8b24-08384401d3cb

[Remove](#)

Binding mode

[Certificate](#)

[Tenant access \(2 allowed\)](#)

You can select a different binding mode or change IP addresses for the current binding mode.

[Edit binding mode](#)

Binding mode: Global



This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **Aktionen** auf der Seite Load Balancer Endpoints oder die Detailseite für einen bestimmten Endpunkt.



Nach dem Bearbeiten eines Endpunkts müssen Sie möglicherweise bis zu 15 Minuten warten, bis Ihre Änderungen auf alle Nodes angewendet werden.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktname bearbeiten	<ol style="list-style-type: none">Aktivieren Sie das Kontrollkästchen für den Endpunkt.Wählen Sie Aktionen > Endpunktname bearbeiten aus.Geben Sie den neuen Namen ein.Wählen Sie Speichern.	<ol style="list-style-type: none">Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen.Wählen Sie das Bearbeitungssymbol .Geben Sie den neuen Namen ein.Wählen Sie Speichern.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktbindungsmodus bearbeiten	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie Aktionen > Endpunktbindungsmodus bearbeiten. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie Bindungsmodus bearbeiten. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie Änderungen speichern.
Endpunktzertifikat bearbeiten	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie Aktionen > Endpunktzertifikat bearbeiten aus. c. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. d. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Zertifikat aus. c. Wählen Sie Zertifikat bearbeiten. d. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. e. Wählen Sie Änderungen speichern.
Bearbeiten Sie den Mandantenzugriff	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie actions > Edit Tenant Access. c. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. d. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Tenant Access. c. Wählen Sie Mandantenzugriff bearbeiten. d. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. e. Wählen Sie Änderungen speichern.

Entfernen Sie Load Balancer-Endpunkte

Sie können einen oder mehrere Endpunkte über das Menü **Aktionen** entfernen oder einen einzelnen Endpunkt von der Detailseite entfernen.



Um Client-Unterbrechungen zu vermeiden, aktualisieren Sie die betroffenen S3- oder Swift-Client-Applikationen, bevor Sie einen Load Balancer-Endpunkt entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über einen Port herzustellen, der einem anderen Load Balancer-Endpunkt zugewiesen ist. Aktualisieren Sie auch die erforderlichen Zertifikatsinformationen.

- So entfernen Sie einen oder mehrere Endpunkte:
 - a. Aktivieren Sie auf der Seite Load Balancer das Kontrollkästchen für jeden Endpunkt, den Sie entfernen möchten.
 - b. Wählen Sie **Aktionen > Entfernen**.
 - c. Wählen Sie **OK**.
- So entfernen Sie einen Endpunkt auf der Detailseite:
 - a. Auf der Seite Load Balancer. Wählen Sie den Endpunktnamen aus.
 - b. Wählen Sie auf der Detailseite * Entfernen.
 - c. Wählen Sie **OK**.

Konfigurieren Sie die Domännennamen des S3-Endpunkts

Um Anforderungen im virtuellen Hosted-Stil von S3 zu unterstützen, müssen Sie die Liste der S3-Endpunkt-Domännennamen, mit denen S3-Clients eine Verbindung herstellen, mit dem Grid Manager konfigurieren.



Die Verwendung einer IP-Adresse für einen Domännennamen des Endpunkts wird nicht unterstützt. Zukünftige Versionen verhindern diese Konfiguration.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".
- Sie haben bestätigt, dass ein Grid-Upgrade nicht ausgeführt wird.



Nehmen Sie keine Änderungen an der Domännennamenkonfiguration vor, wenn ein Grid-Upgrade durchgeführt wird.

Über diese Aufgabe

Um Clients die Verwendung von S3-Endpunkt-Domain-Namen zu ermöglichen, müssen Sie folgende Aktionen durchführen:

- Verwenden Sie den Grid-Manager, um dem StorageGRID System die S3-Endpunkt-Domain-Namen hinzuzufügen.
- Stellen Sie das sicher "[Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet](#)" Ist für alle Domännennamen signiert, die der Client benötigt.

Beispiel: Wenn der Endpunkt lautet `s3.company.com`, Sie müssen sicherstellen, dass das Zertifikat verwendet für HTTPS-Verbindungen enthält die `s3.company.com` endpunkt und Wildcard-alternativer Name (SAN) des Endpunkts: `*.s3.company.com`.

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Datensätze für die IP-Adressen ein, die Clients zum Verbindungsaufbau verwenden, und stellen Sie sicher, dass die Datensätze auf alle erforderlichen S3-Endpunkt-Domännennamen verweisen, einschließlich aller Platzhalternamen.



Clients können sich mit StorageGRID über die IP-Adresse eines Gateway-Node, eines Admin-Nodes oder eines Storage-Nodes oder durch Verbindung mit der virtuellen IP-Adresse einer Hochverfügbarkeitsgruppe verbinden. Sie sollten verstehen, wie Client-Anwendungen eine Verbindung zum Raster herstellen, sodass Sie die richtigen IP-Adressen in die DNS-Einträge aufnehmen können.

Clients, die HTTPS-Verbindungen (empfohlen) zum Raster verwenden, können eines der folgenden Zertifikate verwenden:

- Clients, die eine Verbindung zu einem Load Balancer-Endpunkt herstellen, können für diesen Endpunkt ein benutzerdefiniertes Zertifikat verwenden. Jeder Load Balancer-Endpunkt kann so konfiguriert werden, dass er unterschiedliche S3-Endpunkt-Domännennamen erkennt.
- Clients, die sich mit einem Load-Balancer-Endpunkt oder direkt mit einem Storage-Node verbinden, können das globale S3- und Swift-API-Zertifikat so anpassen, dass alle erforderlichen S3-Endpunkt-Domännennamen enthalten sind.



Wenn Sie keine S3-Endpunkt-Domännennamen hinzufügen und die Liste leer ist, wird die Unterstützung für Anforderungen im virtuellen Hosted-Stil von S3 deaktiviert.

Fügen Sie einen S3-Endpunkt-Domännennamen hinzu

Schritte

1. Wählen Sie **CONFIGURATION > Network > S3-Endpunkt-Domännennamen**.
2. Geben Sie den Domainnamen in das Feld **Domain Name 1** ein. Wählen Sie **Add another Domain Name**, um weitere Domainnamen hinzuzufügen.
3. Wählen Sie **Speichern**.
4. Stellen Sie sicher, dass die von Clients verwendeten Serverzertifikate mit den erforderlichen S3-Endpunkt-Domännennamen übereinstimmen.
 - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der ein eigenes Zertifikat verwendet, "[Aktualisieren Sie das dem Endpunkt zugeordnete Zertifikat](#)".
 - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der das globale S3- und Swift-API-Zertifikat verwendet oder direkt mit Storage-Nodes verbunden ist, "[Aktualisieren Sie das globale S3- und Swift-API-Zertifikat](#)".
5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass die Anforderungen für den Domännennamen des Endpunkts aufgelöst werden können.

Ergebnis

Wenn Clients nun den Endpunkt verwenden `bucket.s3.company.com`, Der DNS-Server löst sich auf den richtigen Endpunkt und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Benennen Sie einen S3-Endpunkt-Domännennamen um

Wenn Sie einen Namen ändern, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.

Schritte

1. Wählen Sie **CONFIGURATION > Network > S3-Endpunkt-Domännennamen**.
2. Wählen Sie das Feld für den Domännennamen aus, das Sie bearbeiten möchten, und nehmen Sie die erforderlichen Änderungen vor.

3. Wählen Sie **Speichern**.
4. Wählen Sie **Ja**, um Ihre Änderung zu bestätigen.

Löschen Sie einen S3-Endpoint-Domännennamen

Wenn Sie einen Namen entfernen, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.

Schritte

1. Wählen Sie **CONFIGURATION > Network > S3-Endpoint-Domännennamen**.
2. Klicken Sie auf das Löschsymboll  Neben dem Domännennamen.
3. Wählen Sie **Ja**, um den Löschvorgang zu bestätigen.

Verwandte Informationen

- ["S3-REST-API VERWENDEN"](#)
- ["Zeigen Sie IP-Adressen an"](#)
- ["Konfigurieren Sie Hochverfügbarkeitsgruppen"](#)

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Zum Speichern oder Abrufen von Objekten verbinden sich S3- und Swift-Client-Anwendungen mit dem Load Balancer-Dienst, der auf allen Admin-Knoten und Gateway-Knoten enthalten ist, oder mit dem Local Distribution Router (LDR)-Dienst, der auf allen Storage-Knoten enthalten ist.

Client-Applikationen können mithilfe der IP-Adresse eines Grid-Node und der Portnummer des Service auf diesem Node eine Verbindung zu StorageGRID herstellen. Optional können Sie Gruppen für Hochverfügbarkeit (High Availability, HA) von Load-Balancing-Nodes erstellen, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn Sie eine Verbindung zu StorageGRID über einen vollständig qualifizierten Domännennamen (FQDN) anstelle einer IP- oder VIP-Adresse herstellen möchten, können Sie DNS-Einträge konfigurieren.

In dieser Tabelle sind die verschiedenen Verbindungsmethoden aufgeführt, mit denen Clients eine Verbindung zu StorageGRID herstellen können, sowie die für den jeweiligen Verbindungstyp verwendeten IP-Adressen und Ports. Wenn Sie bereits Load Balancer-Endpunkte und Hochverfügbarkeitsgruppen (HA-Gruppen) erstellt haben, finden Sie weitere Informationen unter [Wo finden Sie IP-Adressen](#) Um diese Werte im Grid-Manager zu finden.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084 Swift-Standardports: <ul style="list-style-type: none"> • HTTPS: 18083 • HTTP: 18085

Beispiel-URLs

Um eine Client-Applikation mit dem Endpunkt Load Balancer einer HA-Gruppe von Gateway Nodes zu verbinden, verwenden Sie eine wie unten gezeigt strukturierte URL:

`https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 lautet und die Portnummer des Endpunkts des Load Balancer 10443 lautet, könnte eine Applikation die folgende URL verwenden, um eine Verbindung zum StorageGRID herzustellen:

`https://192.0.2.5:10443`

Wo finden Sie IP-Adressen

1. Melden Sie sich mit einem bei Grid Manager an "[Unterstützter Webbrowser](#)".
2. So suchen Sie die IP-Adresse eines Grid-Knotens:
 - a. Wählen Sie **KNOTEN**.
 - b. Wählen Sie den Admin-Node, Gateway-Node oder Storage-Node aus, mit dem Sie eine Verbindung herstellen möchten.
 - c. Wählen Sie die Registerkarte **Übersicht**.
 - d. Notieren Sie im Abschnitt Node-Informationen die IP-Adressen für den Node.
 - e. Wählen Sie **Mehr anzeigen**, um IPv6-Adressen und Schnittstellen-Zuordnungen anzuzeigen.

Sie können Verbindungen von Client-Anwendungen zu einer beliebigen IP-Adresse in der Liste herstellen:

- **Eth0:** Grid Network
- **Eth1:** Admin-Netzwerk (optional)
- **Eth2:** Client-Netzwerk (optional)



Wenn ein Admin-Node oder ein Gateway-Node angezeigt wird und dieser in einer Hochverfügbarkeitsgruppe der aktive Node ist, wird auf eth2 die virtuelle IP-Adresse der HA-Gruppe angezeigt.

3. So finden Sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe:
 - a. Wählen Sie **CONFIGURATION > Network > High Availability groups**.
 - b. Notieren Sie in der Tabelle die virtuelle IP-Adresse der HA-Gruppe.
4. So finden Sie die Portnummer eines Load Balancer-Endpunkts:
 - a. Wählen Sie **CONFIGURATION > Network > Load Balancer Endpunkte**.
 - b. Notieren Sie sich die Portnummer für den zu verwendenden Endpunkt.



Wenn die Portnummer 80 oder 443 ist, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. Alle anderen Ports werden sowohl an Gateway-Knoten als auch an Admin-Nodes konfiguriert.

- c. Wählen Sie den Namen des Endpunkts aus der Tabelle aus.
- d. Bestätigen Sie, dass der **Client-Typ** (S3 oder Swift) mit der Client-Anwendung übereinstimmt, die den Endpunkt verwendet.

Netzwerke und Verbindungen verwalten

Netzwerkeinstellungen konfigurieren: Übersicht

Sie können verschiedene Netzwerkeinstellungen vom Grid Manager konfigurieren, um den Betrieb Ihres StorageGRID Systems zu optimieren.

Konfigurieren Sie die VLAN-Schnittstellen

Das können Sie "[Erstellung von Virtual LAN-Schnittstellen \(VLAN\)](#)" Isolieren und partitionieren Sie den Datenverkehr für Sicherheit, Flexibilität und Performance. Jede VLAN-Schnittstelle ist einer oder mehreren übergeordneten Schnittstellen auf Admin-Nodes und Gateway-Nodes zugeordnet. Die VLAN-Schnittstellen können in HA-Gruppen und in Load Balancer Endpunkten eingesetzt werden, um den Client- oder Admin-Datenverkehr nach Applikation oder Mandanten zu trennen.

Richtlinien für die Verkehrsklassifizierung

Verwenden Sie können "[Richtlinien zur Verkehrsklassifizierung](#)" Zur Identifizierung und Verarbeitung verschiedener Arten von Netzwerkverkehr, einschließlich des Datenverkehrs in Bezug auf bestimmte Buckets, Mandanten, Client-Subnetze oder Lastausgleichsendpunkte. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Richtlinien für StorageGRID-Netzwerke

Mit dem Grid Manager können Sie StorageGRID-Netzwerke und -Verbindungen konfigurieren und verwalten.

Siehe "[Konfiguration von S3- und Swift-Client-Verbindungen](#)" Informationen zum Verbinden von S3 oder Swift Clients

Standard-StorageGRID-Netzwerke

Standardmäßig unterstützt StorageGRID drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass er Ihren Sicherheits- und Zugriffsanforderungen entspricht.

Weitere Informationen zur Netzwerktopologie finden Sie unter "[Netzwerkrichtlinien](#)".

Grid-Netzwerk

Erforderlich. Das Grid-Netzwerk wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das System bietet Konnektivität zwischen allen Nodes im Grid und allen Standorten und Subnetzen.

Admin-Netzwerk

Optional Das Admin-Netzwerk wird in der Regel für die Systemadministration und -Wartung verwendet. Sie kann auch für den Zugriff auf das Client-Protokoll verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Standorten routingfähig sein.

Client-Netzwerk

Optional Das Client-Netzwerk ist ein offenes Netzwerk, das normalerweise für den Zugriff auf S3- und Swift-Client-Applikationen verwendet wird, sodass das Grid-Netzwerk isoliert und gesichert werden kann. Das Client-Netzwerk kann mit jedem Subnetz kommunizieren, das über das lokale Gateway erreichbar ist.

Richtlinien

- Jeder StorageGRID Grid Node benötigt für jedes ihm zugewiesene Netzwerk eine dedizierte Netzwerkschnittstelle, eine IP-Adresse, eine Subnetzmaske und ein Gateway.
- Ein Grid-Knoten kann nicht mehr als eine Schnittstelle in einem Netzwerk haben.
- Es wird ein einzelnes Gateway pro Netzwerk und pro Grid-Node unterstützt, das sich im gleichen Subnetz wie der Node befindet. Sie können bei Bedarf komplexere Routing-Lösungen im Gateway implementieren.
- Auf jedem Node ist jedes Netzwerk einer bestimmten Netzwerkschnittstelle zugeordnet.

Netzwerk	Schnittstellename
Raster	Eth0
Admin (optional)	Eth1
Client (optional)	Eth2

- Wenn der Node mit einer StorageGRID Appliance verbunden ist, werden für jedes Netzwerk bestimmte Ports verwendet. Weitere Informationen finden Sie in den Installationsanweisungen für Ihr Gerät.
- Die Standardroute wird automatisch pro Knoten generiert. Wenn eth2 aktiviert ist, verwendet 0.0.0.0/0 das Client-Netzwerk auf eth2. Wenn eth2 nicht aktiviert ist, verwendet 0.0.0.0/0 das Grid-Netzwerk auf eth0.
- Das Client-Netzwerk ist erst betriebsbereit, wenn der Grid-Node dem Grid beigetreten ist
- Das Admin-Netzwerk kann während der Bereitstellung des Grid-Knotens konfiguriert werden, um den Zugriff auf die Installations-Benutzeroberfläche zu ermöglichen, bevor das Grid vollständig installiert ist.

Optionale Schnittstellen

Optional können Sie einem Node zusätzliche Schnittstellen hinzufügen. Beispielsweise möchten Sie einem Admin- oder Gateway-Node eine Trunk-Schnittstelle hinzufügen, sodass Sie verwenden können ["VLAN-Schnittstellen"](#) Zur Trennung des Datenverkehrs von unterschiedlichen Applikationen oder Mandanten. Oder Sie möchten möglicherweise eine Zugriffsschnittstelle hinzufügen, die in A verwendet werden soll ["Hochverfügbarkeitsgruppe \(High Availability Group, HA-Gruppe\)"](#).

Informationen zum Hinzufügen von Trunk- oder Access-Schnittstellen finden Sie unter:

- **VMware (nach der Installation des Knotens):** ["VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)
 - **RHEL oder CentOS (vor dem Installieren des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **Ubuntu oder Debian (vor der Installation des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens):** ["Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)

Zeigen Sie IP-Adressen an

Sie können die IP-Adresse für jeden Grid-Node im StorageGRID System anzeigen. Sie können sich dann mithilfe dieser IP-Adresse am Grid Node an der Befehlszeile anmelden und verschiedene Wartungsverfahren durchführen.

Bevor Sie beginnen

Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).

Über diese Aufgabe

Informationen zum Ändern von IP-Adressen finden Sie unter ["Konfigurieren Sie IP-Adressen"](#).

Schritte

1. Wählen Sie **NODES > Grid Node > Übersicht** aus.
2. Wählen Sie **Mehr anzeigen** rechts neben dem Titel der IP-Adressen.

Die IP-Adressen für diesen Grid-Node werden in einer Tabelle aufgeführt.

Overview Hardware Network Storage Objects ILM Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021
 Type: Storage Node
 ID: f0890e03-4c72-401f-ae92-245511a38e51
 Connection state: Connected
 Storage used: Object data 7% [?](#)
 Object metadata 5% [?](#)
 Software version: 11.6.0 (build 20210915.1941.afce2d9)
 IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses ^](#)

Interface ⌵	IP address ⌵
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts [^](#)

Alert name ⌵	Severity ? ⌵	Time triggered ⌵	Current values
ILM placement unachievable 🔗	Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Unterstützte Chiffren für ausgehende TLS-Verbindungen

Das StorageGRID System unterstützt eine begrenzte Anzahl von Verschlüsselungssuiten für TLS-Verbindungen (Transport Layer Security) zu den externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3 für Verbindungen zu externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

Die zur Verwendung mit externen Systemen unterstützten TLS-Chiffren wurden ausgewählt, um die Kompatibilität mit verschiedenen externen Systemen sicherzustellen. Die Liste ist größer als die Liste der Chiffren, die zur Verwendung mit S3- oder Swift-Client-Applikationen unterstützt werden. Um Chiffren zu konfigurieren, gehen Sie zu **CONFIGURATION > Security > Security settings** und wählen **TLS und SSH**

Policies aus.



TLS-Konfigurationsoptionen wie Protokollversionen, Chiffren, Schlüsselaustauschalgorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Wenden Sie sich an Ihren NetApp Ansprechpartner, wenn Sie spezifische Anfragen zu diesen Einstellungen haben.

Konfigurieren Sie die VLAN-Schnittstellen

Sie können virtuelle LAN-Schnittstellen (VLAN) auf Admin-Nodes und Gateway-Nodes erstellen und diese in HA-Gruppen und Load Balancer-Endpunkten verwenden, um den Datenverkehr für Sicherheit, Flexibilität und Performance zu isolieren und zu partitionieren.

Überlegungen zu VLAN-Schnittstellen

- Sie erstellen eine VLAN-Schnittstelle, indem Sie eine VLAN-ID eingeben und eine übergeordnete Schnittstelle auf einem oder mehreren Nodes auswählen.
- Eine übergeordnete Schnittstelle muss als Trunk-Schnittstelle am Switch konfiguriert sein.
- Eine übergeordnete Schnittstelle kann das Grid-Netzwerk (eth0), das Client-Netzwerk (eth2) oder eine zusätzliche Trunk-Schnittstelle für die VM oder Bare-Metal-Host (z. B. ens256) sein.
- Sie können für jede VLAN-Schnittstelle nur eine übergeordnete Schnittstelle für einen bestimmten Node auswählen. Beispielsweise können Sie nicht sowohl die Grid-Netzwerkschnittstelle als auch die Client-Netzwerkschnittstelle auf demselben Gateway-Node wie die übergeordnete Schnittstelle für dasselbe VLAN verwenden.
- Wenn die VLAN-Schnittstelle für den Admin-Node-Datenverkehr dient, der Datenverkehr zum Grid-Manager und dem Mandanten-Manager enthält, wählen Sie nur Schnittstellen auf Admin-Nodes aus.
- Wenn die VLAN-Schnittstelle für S3- oder Swift-Client-Datenverkehr dient, wählen Sie Schnittstellen entweder auf Admin-Nodes oder Gateway-Nodes aus.
- Wenn Sie Leitungsbündelschnittstellen hinzufügen müssen, lesen Sie die folgenden Informationen:
 - **VMware (nach der Installation des Knotens):** ["VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)
 - **RHEL oder CentOS (vor dem Installieren des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **Ubuntu oder Debian (vor der Installation des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens):** ["Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)

Erstellen einer VLAN-Schnittstelle

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung.
- Im Netzwerk wurde eine Trunk-Schnittstelle konfiguriert und mit dem VM- oder Linux-Node verbunden. Sie kennen den Namen der Trunk-Schnittstelle.
- Sie kennen die ID des zu konfigurierende VLANs.

Über diese Aufgabe

Ihr Netzwerkadministrator hat möglicherweise eine oder mehrere Trunk-Schnittstellen und ein oder mehrere

VLANs konfiguriert, um den Client- oder Admin-Datenverkehr verschiedener Applikationen oder Mandanten zu trennen. Jedes VLAN wird durch eine numerische ID oder ein Tag identifiziert. Beispielsweise könnte Ihr Netzwerk VLAN 100 für FabricPool-Datenverkehr und VLAN 200 für eine Archivierungsanwendung verwenden.

Sie können den Grid-Manager verwenden, um VLAN-Schnittstellen zu erstellen, die Clients den Zugriff auf StorageGRID in einem bestimmten VLAN ermöglichen. Wenn Sie VLAN-Schnittstellen erstellen, geben Sie die VLAN-ID an und wählen Sie übergeordnete Schnittstellen (Trunk) auf einem oder mehreren Nodes aus.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **KONFIGURATION > Netzwerk > VLAN-Schnittstellen**.
2. Wählen Sie **Erstellen**.

Geben Sie Details zu den VLAN-Schnittstellen ein

Schritte

1. Geben Sie die ID des VLANs in Ihrem Netzwerk an. Sie können einen beliebigen Wert zwischen 1 und 4094 eingeben.

VLAN-IDs müssen nicht eindeutig sein. Beispielsweise können Sie die VLAN-ID 200 für den Admin-Datenverkehr an einem Standort und dieselbe VLAN-ID für den Client-Datenverkehr an einem anderen Standort verwenden. Sie können separate VLAN-Schnittstellen mit verschiedenen Gruppen von übergeordneten Schnittstellen an jedem Standort erstellen. Zwei VLAN-Schnittstellen mit derselben ID können jedoch nicht dieselbe Schnittstelle auf einem Node gemeinsam nutzen. Wenn Sie eine ID angeben, die bereits verwendet wurde, wird eine Meldung angezeigt.

2. Geben Sie optional eine kurze Beschreibung für die VLAN-Schnittstelle ein.
3. Wählen Sie **Weiter**.

Wählen Sie übergeordnete Schnittstellen

In der Tabelle sind die verfügbaren Schnittstellen für alle Admin-Nodes und Gateway-Nodes an jedem Standort im Raster aufgeführt. Schnittstellen des Admin-Netzwerks (eth1) können nicht als übergeordnete Schnittstellen verwendet werden und werden nicht angezeigt.

Schritte

1. Wählen Sie eine oder mehrere übergeordnete Schnittstellen aus, an die dieses VLAN angeschlossen werden soll.

Sie möchten beispielsweise ein VLAN an die Schnittstelle „Client Network“ (eth2) für einen Gateway-Node und einen Admin-Node anschließen.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
<input type="checkbox"/>	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
<input checked="" type="checkbox"/>	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
<input type="checkbox"/>	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
<input checked="" type="checkbox"/>	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
<input type="checkbox"/>	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

[Previous](#)
[Continue](#)

2. Wählen Sie **Weiter**.

Bestätigen Sie die Einstellungen

Schritte

1. Überprüfen Sie die Konfiguration und nehmen Sie alle Änderungen vor.
 - Wenn Sie die VLAN-ID oder Beschreibung ändern möchten, wählen Sie oben auf der Seite **VLAN-Details eingeben** aus.
 - Wenn Sie eine übergeordnete Schnittstelle ändern möchten, wählen Sie oben auf der Seite die Option **übergeordnete Schnittstellen auswählen** aus, oder wählen Sie **Zurück**.
 - Wenn Sie eine übergeordnete Schnittstelle entfernen müssen, wählen Sie den Papierkorb aus .
2. Wählen Sie **Speichern**.
3. Warten Sie bis zu 5 Minuten, bis die neue Schnittstelle auf der Seite Hochverfügbarkeitsgruppen als Auswahl angezeigt wird und in der Tabelle **Netzwerkschnittstellen** für den Knoten (**NODES > Parent Interface Node > Network**) aufgelistet wird.

Bearbeiten Sie eine VLAN-Schnittstelle

Wenn Sie eine VLAN-Schnittstelle bearbeiten, können Sie die folgenden Arten von Änderungen vornehmen:

- Ändern Sie die VLAN-ID oder -Beschreibung.
- Übergeordnete Schnittstellen hinzufügen oder entfernen.

Sie möchten beispielsweise eine übergeordnete Schnittstelle von einer VLAN-Schnittstelle entfernen, wenn Sie den zugeordneten Node außer Betrieb setzen möchten.

Beachten Sie Folgendes:

- Sie können keine VLAN-ID ändern, wenn die VLAN-Schnittstelle in einer HA-Gruppe verwendet wird.
- Sie können eine übergeordnete Schnittstelle nicht entfernen, wenn diese übergeordnete Schnittstelle in einer HA-Gruppe verwendet wird.

Nehmen Sie beispielsweise an, dass VLAN 200 an den übergeordneten Schnittstellen auf den Nodes A und B. angeschlossen ist. Wenn eine HA-Gruppe die VLAN 200-Schnittstelle für Node A und die eth2-Schnittstelle für Node B verwendet, können Sie die nicht verwendete übergeordnete Schnittstelle für Node B entfernen, Sie können jedoch die verwendete übergeordnete Schnittstelle für Node A nicht entfernen.

Schritte

1. Wählen Sie **KONFIGURATION > Netzwerk > VLAN-Schnittstellen**.
2. Aktivieren Sie das Kontrollkästchen für die VLAN-Schnittstelle, die Sie bearbeiten möchten. Wählen Sie dann **Aktionen > Bearbeiten** aus.
3. Optional können Sie die VLAN-ID oder die Beschreibung aktualisieren. Wählen Sie anschließend **Weiter**.

Sie können keine VLAN-ID aktualisieren, wenn das VLAN in einer HA-Gruppe verwendet wird.
4. Aktivieren oder deaktivieren Sie optional die Kontrollkästchen, um übergeordnete Schnittstellen hinzuzufügen oder nicht verwendete Schnittstellen zu entfernen. Wählen Sie anschließend **Weiter**.
5. Überprüfen Sie die Konfiguration und nehmen Sie alle Änderungen vor.
6. Wählen Sie **Speichern**.

Entfernen Sie eine VLAN-Schnittstelle

Sie können eine oder mehrere VLAN-Schnittstellen entfernen.

Sie können eine VLAN-Schnittstelle nicht entfernen, wenn sie derzeit in einer HA-Gruppe verwendet wird. Sie müssen die VLAN-Schnittstelle aus der HA-Gruppe entfernen, bevor Sie sie entfernen können.

Um Unterbrechungen des Client-Traffic zu vermeiden, sollten Sie einen der folgenden Schritte in Betracht ziehen:

- Fügen Sie einer neuen VLAN-Schnittstelle zur HA-Gruppe hinzu, bevor Sie diese VLAN-Schnittstelle entfernen.
- Erstellen Sie eine neue HA-Gruppe, die diese VLAN-Schnittstelle nicht verwendet.
- Wenn die VLAN-Schnittstelle, die Sie entfernen möchten, derzeit die aktive Schnittstelle ist, bearbeiten Sie die HA-Gruppe. Verschieben Sie die VLAN-Schnittstelle, die Sie entfernen möchten, auf die Unterseite der Prioritätenliste. Warten Sie, bis die Kommunikation auf der neuen primären Schnittstelle eingerichtet ist, und entfernen Sie dann die alte Schnittstelle aus der HA-Gruppe. Schließlich, löschen Sie die VLAN-Schnittstelle auf diesem Knoten.

Schritte

1. Wählen Sie **KONFIGURATION > Netzwerk > VLAN-Schnittstellen**.
2. Aktivieren Sie das Kontrollkästchen für jede VLAN-Schnittstelle, die Sie entfernen möchten. Wählen Sie dann **Aktionen > Löschen** aus.
3. Wählen Sie **Ja**, um Ihre Auswahl zu bestätigen.

Alle ausgewählten VLAN-Schnittstellen werden entfernt. Auf der Seite VLAN-Schnittstellen wird ein grünes Erfolgsbanner angezeigt.

Verwalten von Richtlinien zur Verkehrsklassifizierung

Managen von Richtlinien zur Verkehrsklassifizierung: Übersicht

Zur Verbesserung Ihrer QoS-Angebote (Quality of Service) können Sie Richtlinien zur Traffic-Klassifizierung erstellen, um verschiedene Arten von Netzwerkverkehr zu identifizieren und zu überwachen. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Richtlinien zur Traffic-Klassifizierung werden auf Endpunkte im StorageGRID Load Balancer Service für Gateway-Knoten und Admin-Nodes angewendet. Zum Erstellen von Richtlinien für die Verkehrsklassifizierung müssen Sie bereits Load Balancer Endpunkte erstellt haben.

Übereinstimmungsregeln

Jede Traffic-Klassifizierungsrichtlinie enthält mindestens eine übereinstimmende Regel, um den Netzwerkverkehr zu identifizieren, der mit einer oder mehreren der folgenden Einheiten in Verbindung steht:

- Buckets
- Subnetz
- Mandant
- Load Balancer-Endpunkte

StorageGRID überwacht den Datenverkehr, der mit allen Regeln innerhalb der Richtlinie im Einklang mit den Zielen der Regel steht. Jeder Traffic, der einer Richtlinie entspricht, wird von dieser Richtlinie übernommen. Umgekehrt können Sie Regeln festlegen, die mit dem gesamten Verkehr übereinstimmen, außer einer angegebenen Einheit.

Traffic-Beschränkung

Optional können Sie einer Richtlinie die folgenden Begrenzungstypen hinzufügen:

- Aggregatbandbreite
- Bandbreite pro Anforderung
- Gleichzeitige Anfragen
- Anforderungsrate

Grenzwerte werden pro Load Balancer erzwungen. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, sind die maximalen Raten ein Vielfaches der von Ihnen angegebenen Ratenlimits.



Sie können Richtlinien erstellen, um die aggregierte Bandbreite zu begrenzen oder die Bandbreite nach Bedarf zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben.

Bei Bandbreitenbeschränkungen oder -Anforderungen werden die Anforderungen mit der von Ihnen festgelegten Rate in- oder Out-Streaming übertragen. StorageGRID kann nur eine Geschwindigkeit erzwingen. Daher ist die jeweils spezifischste Richtlinienabgleiche nach Matcher-Typ erzwungen. Die von der Anforderung verbrauchte Bandbreite wird nicht mit anderen weniger spezifischen übereinstimmenden Richtlinien verglichen, die Richtlinien zur Gesamtbandbreite enthalten. Bei allen anderen Grenzwerttypen werden

Clientanforderungen um 250 Millisekunden verzögert und bei Anfragen, die die übereinstimmende Richtlinienbegrenzung überschreiten, eine langsame Antwort von 503 erhalten.

Im Grid Manager können Sie Traffic-Diagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzen durchsetzen.

Richtlinien für die Verkehrsklassifizierung mit SLAs

Sie können Richtlinien für die Traffic-Klassifizierung in Verbindung mit Kapazitätsgrenzen und Datensicherung verwenden, um Service Level Agreements (SLAs) durchzusetzen, die Besonderheiten bei Kapazität, Datensicherung und Performance bieten.

Das folgende Beispiel zeigt drei SLA-Tiers. Sie können Traffic-Klassifizierungsrichtlinien erstellen, um die Performance-Ziele jeder SLA-Ebene zu erreichen.

Service Level-Ebene	Kapazität	Datensicherung	Maximal zulässige Leistung	Kosten
Gold	1 PB Speicherplatz zulässig	3 ILM-Regel für Kopien	25 K Anfragen/Sek. 5 GB/s (40 Gbit/s) Bandbreite	Kosten pro Monat
Silber	250 TB Speicherplatz zulässig	ILM-Regel für 2 Kopien	10 K Anfragen/Sek. 1.25 GB/s (10 Gbit/s) Bandbreite	Kosten pro Monat
Bronze	100 TB Speicherplatz zulässig	ILM-Regel für 2 Kopien	5 K Anfragen/Sek. 1 GB/s (8 Gbit/s) Bandbreite	Kosten pro Monat

Richtlinien für die Verkehrsklassifizierung erstellen

Sie können Richtlinien zur Verkehrsklassifizierung erstellen, wenn Sie den Netzwerk-Traffic nach Bucket, Bucket-Regex, CIDR, Load-Balancer-Endpunkt oder Mandant überwachen und optional begrenzen möchten. Optional können Sie Obergrenzen für eine Richtlinie basierend auf der Bandbreite, der Anzahl gleichzeitiger Anfragen oder der Anfragerate festlegen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben alle Load Balancer-Endpunkte erstellt, die übereinstimmen sollen.
- Sie haben alle Mandanten erstellt, denen Sie entsprechen möchten.

Schritte

1. Wählen Sie **CONFIGURATION > Network > traffic classification**.
2. Wählen Sie **Erstellen**.

3. Geben Sie einen Namen und eine Beschreibung (optional) für die Richtlinie ein und wählen Sie **Weiter**.

Beschreiben Sie beispielsweise, auf welche Weise diese Richtlinie zur Klassifizierung von Verkehrsdaten zutrifft und welche Begrenzung sie hat.

4. Wählen Sie **Regel hinzufügen** und geben Sie die folgenden Details an, um eine oder mehrere übereinstimmende Regeln für die Richtlinie zu erstellen. Jede Richtlinie, die Sie erstellen, sollte mindestens eine übereinstimmende Regel haben. Wählen Sie **Weiter**.

Feld	Beschreibung
Typ	<p>Wählen Sie die Verkehrstypen aus, für die die entsprechende Regel gilt. Traffic-Typen sind Bucket, Bucket-Regex, CIDR, Load Balancer-Endpunkt und Mandant.</p>
Match-Wert	<p>Geben Sie den Wert ein, der dem ausgewählten Typ entspricht.</p> <ul style="list-style-type: none">• Bucket: Geben Sie einen oder mehrere Bucket-Namen ein.• Bucket-regex: Geben Sie einen oder mehrere reguläre Ausdrücke ein, die für einen Satz von Bucket-Namen verwendet werden. <p>Der reguläre Ausdruck ist nicht verankert. Verwenden Sie den Anker \wedge, um am Anfang des Bucket-Namens zu übereinstimmen, und verwenden Sie den Anker ϵ, um am Ende des Namens zu übereinstimmen. Die Übereinstimmung mit regulären Ausdrücken unterstützt eine Teilmenge der PCRE-Syntax (Perl Compatible Regular Expression).</p> <ul style="list-style-type: none">• CIDR: Geben Sie ein oder mehrere IPv4-Subnetze in CIDR-Notation ein, die mit dem gewünschten Subnetz übereinstimmen.• Load-Balancer-Endpunkt: Wählen Sie einen Endpunktnamen aus. Dies sind die Lastausgleichsendpunkte, die Sie auf dem definiert haben "Konfigurieren von Load Balancer-Endpunkten".• Tenant: Tenant Matching verwendet die Zugriffsschlüssel-ID. Wenn die Anforderung keine Zugriffsschlüssel-ID enthält (z. B. anonymer Zugriff), wird die Eigentümerschaft des abgerufenen Buckets verwendet, um den Mandanten zu bestimmen.
Umgekehrtes Match	<p>Wenn Sie den gesamten Netzwerkverkehr <i>except</i> mit dem gerade definierten Typ und Match-Wert abstimmen möchten, aktivieren Sie das Kontrollkästchen inverse Übereinstimmung. Andernfalls lassen Sie das Kontrollkästchen deaktiviert.</p> <p>Wenn Sie beispielsweise möchten, dass diese Richtlinie auf alle Endpunkte mit Ausnahme eines Lastausgleichs angewendet wird, geben Sie den auszuschließenden Lastausgleichsendpunkt an, und wählen Sie inverse Übereinstimmung aus.</p> <p>Bei einer Richtlinie, die mehrere Matriken enthält, bei denen mindestens eine inverse Matrix ist, sollten Sie darauf achten, keine Richtlinie zu erstellen, die allen Anforderungen entspricht.</p>

5. Wählen Sie optional **Limit hinzufügen** und wählen Sie die folgenden Details aus, um eine oder mehrere

Grenzwerte hinzuzufügen, um den Netzwerkverkehr zu steuern, der von einer Regel abgeglichen wird.



StorageGRID sammelt Kennzahlen, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends besser verstehen können.

Feld	Beschreibung
Typ	<p>Die Art der Begrenzung, die auf den Netzwerkverkehr angewendet werden soll, der der Regel entspricht. Beispielsweise können Sie die Bandbreite oder die Anforderungsrate begrenzen.</p> <p>Hinweis: Sie können Richtlinien erstellen, um die Gesamtbandbreite zu begrenzen oder die Bandbreite pro Anfrage zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Wenn die aggregierte Bandbreite verwendet wird, ist die Bandbreite pro Anforderung nicht verfügbar. Umgekehrt ist die aggregierte Bandbreite nicht verfügbar, wenn die Bandbreite pro Anforderung verwendet wird. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben.</p> <p>Bei Bandbreitenbeschränkungen wendet StorageGRID die Richtlinie an, die der jeweils festgelegten Grenzwertart am besten entspricht. Wenn Sie beispielsweise eine Richtlinie haben, die Datenverkehr in nur eine Richtung begrenzt, ist der Datenverkehr in die entgegengesetzte Richtung unbegrenzt, selbst wenn der Datenverkehr mit zusätzlichen Richtlinien mit Bandbreitenbeschränkungen übereinstimmt. StorageGRID implementiert die „besten“ Matches für Bandbreitenlimits in der folgenden Reihenfolge:</p> <ul style="list-style-type: none">• Exakte IP-Adresse (/32-Maske)• Exakter Bucket-Name• Eimer-Regex• Mandant• Endpunkt• Nicht exakte CIDR-Übereinstimmungen (nicht /32)• Umgekehrte Übereinstimmungen
Gilt für	Gibt an, ob diese Begrenzung auf Client-Leseanforderungen (GET oder HEAD) oder Schreibanforderungen (PUT, POST oder DELETE) zutrifft.
Wert	<p>Der Wert, auf den der Netzwerkverkehr begrenzt wird, abhängig von der ausgewählten Einheit. Geben Sie beispielsweise 10 ein, und wählen Sie MiB/s aus, um zu verhindern, dass der Netzwerkverkehr, der dieser Regel entspricht, 10 MiB/s überschreitet</p> <p>Hinweis: Je nach Einstellung der Einheiten sind die verfügbaren Einheiten entweder binär (z. B. gib) oder dezimal (z. B. GB). Um die Einstellung Einheiten zu ändern, wählen Sie oben rechts im Grid-Manager das Dropdown-Menü Benutzer aus, und wählen Sie dann Benutzereinstellungen aus.</p>

Feld	Beschreibung
Einheit	Die Einheit, die den eingegebenen Wert beschreibt.

Wenn Sie beispielsweise eine Bandbreitenbegrenzung von 40 GB/s für eine SLA-Ebene erstellen möchten, erstellen Sie zwei aggregierte Bandbreitenlimits: GET/HEAD bei 40 GB/s und PUT/POST/DELETE bei 40 GB/s.

- Wählen Sie **Weiter**.
- Lesen und prüfen Sie die Richtlinie zur Verkehrsklassifizierung. Verwenden Sie die Schaltfläche * Zurück*, um zurückzugehen und Änderungen vorzunehmen. Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie **Speichern und fortfahren**.

Der S3- und Swift-Client-Traffic wird nun gemäß der Traffic-Klassifizierungsrichtlinie behandelt.

Nachdem Sie fertig sind

["Zeigen Sie Metriken zum Netzwerkverkehr an"](#) Um zu überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Richtlinie zur Verkehrsklassifizierung bearbeiten

Sie können eine Traffic-Klassifizierungsrichtlinie bearbeiten, um ihren Namen oder ihre Beschreibung zu ändern oder um Regeln oder Grenzen für die Richtlinie zu erstellen, zu bearbeiten oder zu löschen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung.

Schritte

- Wählen Sie **CONFIGURATION > Network > traffic classification**.

Die Seite für die Verkehrsklassifizierungsrichtlinien wird angezeigt, und die vorhandenen Richtlinien werden in einer Tabelle aufgeführt.

- Bearbeiten Sie die Richtlinie über das Menü Aktionen oder die Detailseite. Siehe ["Erstellen von Richtlinien zur Verkehrsklassifizierung"](#) Für das, was zu betreten ist.

Menü „Aktionen“

- Aktivieren Sie das Kontrollkästchen für die Richtlinie.
- Wählen Sie **Actions > Edit**.

Detailseite

- Wählen Sie den Richtliniennamen aus.
- Klicken Sie neben dem Richtliniennamen auf die Schaltfläche **Bearbeiten**.

- Bearbeiten Sie für den Schritt Richtliniennamen eingeben optional den Richtliniennamen oder die Beschreibung, und wählen Sie **Weiter** aus.

4. Fügen Sie für den Schritt übereinstimmende Regeln hinzufügen optional eine Regel hinzu oder bearbeiten Sie die Werte **Typ** und **Match** der bestehenden Regel und wählen Sie **Weiter**.
5. Für den Schritt Grenzen festlegen können Sie optional ein Limit hinzufügen, bearbeiten oder löschen und dann **Weiter** auswählen.
6. Überprüfen Sie die aktualisierte Richtlinie, und wählen Sie **Speichern und fortfahren**.

Die an der Richtlinie vorgenommenen Änderungen werden gespeichert, und der Netzwerkverkehr wird nun gemäß den Richtlinien zur Klassifizierung von Verkehrsmeldungen verarbeitet. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Löschen einer Traffic-Klassifizierungsrichtlinie

Sie können eine Verkehrsklassifizierungsrichtlinie löschen, wenn Sie sie nicht mehr benötigen. Achten Sie darauf, die richtige Richtlinie zu löschen, da eine Richtlinie beim Löschen nicht abgerufen werden kann.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **CONFIGURATION > Network > traffic classification**.

Die Seite für die Verkehrsklassifizierungsrichtlinien wird mit den vorhandenen Richtlinien in einer Tabelle angezeigt.

2. Löschen Sie die Richtlinie über das Menü Aktionen oder die Detailseite.

Menü „Aktionen“

- a. Aktivieren Sie das Kontrollkästchen für die Richtlinie.
- b. Wählen Sie **Aktionen > Entfernen**.

Seite mit den Details der Richtlinie

- a. Wählen Sie den Richtliniennamen aus.
- b. Klicken Sie neben dem Richtliniennamen auf die Schaltfläche **Entfernen**.

3. Wählen Sie **Ja**, um zu bestätigen, dass Sie die Richtlinie löschen möchten.

Die Richtlinie wird gelöscht.

Zeigen Sie Metriken zum Netzwerkverkehr an

Sie können den Netzwerkverkehr überwachen, indem Sie die Diagramme anzeigen, die auf der Seite für die Verkehrsklassifizierungsrichtlinien verfügbar sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Root-Zugriffsberechtigung oder die Berechtigung für die Mandantenkonten.

Über diese Aufgabe

Für alle vorhandenen Richtlinien zur Verkehrsklassifizierung können Sie Metriken für den Load Balancer-Dienst anzeigen, um zu ermitteln, ob die Richtlinie den Datenverkehr im Netzwerk erfolgreich einschränkt. Anhand der Daten in den Diagrammen können Sie feststellen, ob Sie die Richtlinie anpassen müssen.

Auch wenn für eine Richtlinie zur Klassifizierung von Datenverkehr keine Grenzen gesetzt wurden, werden Kennzahlen erfasst und die Diagramme bieten nützliche Informationen zum Verständnis von Verkehrstrends.

Schritte

1. Wählen Sie **CONFIGURATION > Network > traffic classification**.

Die Seite für die Verkehrsklassifizierungsrichtlinien wird angezeigt, und die vorhandenen Richtlinien werden in der Tabelle aufgeführt.

2. Wählen Sie den Richtliniennamen für die Verkehrsklassifizierung aus, für den Sie Metriken anzeigen möchten.
3. Wählen Sie die Registerkarte **Metriken**.

Die Richtliniendiagramme für die Verkehrsklassifizierung werden angezeigt. Die Diagramme zeigen Metriken nur für den Datenverkehr an, der mit der ausgewählten Richtlinie übereinstimmt.

Die folgenden Diagramme sind auf der Seite enthalten.

- Anforderungsrate: Dieses Diagramm zeigt die Bandbreite an, die dieser Richtlinie entspricht, die von allen Load Balancern verarbeitet wird. Die empfangenen Daten umfassen Anforderungskopfzeilen für alle Anfragen und die Körperdatengröße für Antworten mit Körperdaten. „Gesendet“ enthält Antwortkopfzeilen für alle Anfragen und die Größe der Antwortkörperdaten für Anforderungen, die Körperdaten in die Antwort einschließen.



Wenn die Anforderungen abgeschlossen sind, zeigt dieses Diagramm nur die Bandbreitennutzung an. Bei langsamen oder großen Objektanforderungen kann die tatsächliche unmittelbare Bandbreite von den in diesem Diagramm gemeldeten Werten abweichen.

- Fehlerreaktionsrate: Dieses Diagramm bietet eine ungefähre Rate, mit der Anfragen, die dieser Richtlinie entsprechen, Fehler (HTTP-Statuscode ≥ 400) an Clients zurückgeben.
 - Durchschnittliche Anforderungsdauer (kein Fehler): Diese Grafik bietet eine durchschnittliche Dauer erfolgreicher Anfragen, die dieser Richtlinie entsprechen.
 - Verwendung der Richtlinienbandbreite: Dieses Diagramm gibt die Bandbreite an, die dieser Richtlinie entspricht, die von allen Lastverteilern verarbeitet wird. Die empfangenen Daten umfassen Anforderungskopfzeilen für alle Anfragen und die Körperdatengröße für Antworten mit Körperdaten. „Gesendet“ enthält Antwortkopfzeilen für alle Anfragen und die Größe der Antwortkörperdaten für Anforderungen, die Körperdaten in die Antwort einschließen.
4. Positionieren Sie den Cursor über einem Liniendiagramm, um ein Popup-Fenster mit Werten für einen bestimmten Teil des Diagramms anzuzeigen.
 5. Wählen Sie **Grafana Dashboard** direkt unter dem Metrics-Titel, um alle Diagramme für eine Richtlinie anzuzeigen. Zusätzlich zu den vier Diagrammen aus der Registerkarte **Metriken** können Sie zwei weitere Diagramme anzeigen:

- Schreib Anforderungsrate nach Objektgröße: Die Rate für PUT/POST/DELETE-Anfragen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Raten pro Sekunde an. Die in der Hover-Ansicht angezeigten Raten werden auf Ganzzahlen gekürzt und können 0 melden, wenn im Bucket Anfragen ohne Null angezeigt werden.
- Leseanforderungsrate nach Objektgröße: Die Rate für GET/HEAD-Anfragen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Raten pro Sekunde an. Die in der Hover-Ansicht angezeigten Raten werden auf Ganzzahlen gekürzt und können 0 melden, wenn im Bucket Anfragen ohne Null angezeigt werden.

6. Alternativ können Sie über das Menü * SUPPORT* auf die Diagramme zugreifen.

- Wählen Sie **SUPPORT > Tools > Metriken**.
- Wählen Sie im Abschnitt **Grafana** die Option **Richtlinie zur Traffic-Klassifizierung** aus.
- Wählen Sie die Richtlinie aus dem Menü oben links auf der Seite aus.
- Positionieren Sie den Cursor über einem Diagramm, um ein Popup-Fenster anzuzeigen, in dem Datum und Uhrzeit der Probe, Objektgrößen, die in der Anzahl zusammengefasst werden, und die Anzahl der Anfragen pro Sekunde in diesem Zeitraum angezeigt werden.

Richtlinien für die Verkehrsklassifizierung werden anhand ihrer ID identifiziert. Richtlinien-IDs werden auf der Seite für die Verkehrsklassifizierungsrichtlinien aufgeführt.

7. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

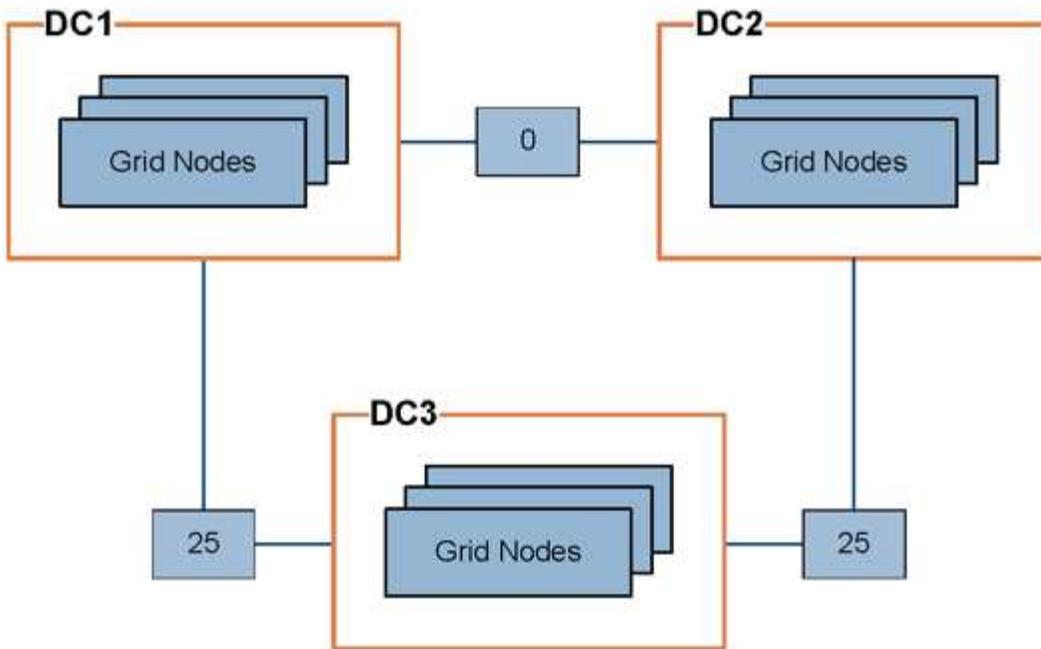
Verwalten Sie Verbindungskosten

Durch die Verbindungskosten können Sie festlegen, welcher Datacenter-Standort einen angeforderten Service bereitstellt, wenn zwei oder mehr Datacenter-Standorte vorhanden sind. Sie können die Verbindungskosten anpassen, um die Latenz zwischen Standorten reflektieren.

Was sind Verbindungskosten?

- Die Link-Kosten werden verwendet, um Prioritäten zu setzen, welche Objektkopie für die Bearbeitung von Objektabrufungen verwendet wird.
- Die Link-Kosten werden von der Grid-Management-API und der Mandanten-Management-API verwendet, um festzustellen, welche internen StorageGRID-Services verwendet werden sollen.
- Verbindungskosten werden vom Load Balancer-Service auf Admin-Nodes und Gateway-Nodes zum direkten Client-Verbindungen verwendet. Siehe "[Überlegungen zum Lastausgleich](#)".

Das Diagramm zeigt ein drei Standortrastrer mit Verbindungskosten, die zwischen Standorten konfiguriert sind:



- Der Load Balancer auf Admin-Nodes und Gateway-Nodes verteilt Client-Verbindungen zu allen Storage-Nodes am selben Datacenter-Standort und zu allen Datacenter-Standorten, für die keine Linkkosten anfallen.

Im Beispiel verteilt ein Gateway-Node am Datacenter-Standort 1 (DC1) Client-Verbindungen gleichmäßig auf Storage-Nodes an DC1 und Storage Nodes an DC2. Ein Gateway-Node bei DC3 sendet Client-Verbindungen nur zu Storage-Nodes an DC3.

- Beim Abrufen eines Objekts, das als mehrere replizierte Kopien vorhanden ist, ruft StorageGRID die Kopie im Datacenter ab, das die niedrigsten Verbindungskosten bietet.

Wenn in dem Beispiel eine Client-Anwendung bei DC2 ein Objekt abrufen, das sowohl bei DC1 als auch bei DC3 gespeichert ist, wird das Objekt von DC1 abgerufen, da die Verbindungskosten von DC1 zu DC2 0 sind, was niedriger ist als die Verbindungskosten von DC3 zu DC2 (25).

Verbindungskosten sind willkürliche relative Zahlen ohne spezifische Maßeinheit. So werden beispielsweise die Linkkosten von 50 weniger bevorzugt genutzt als eine Linkkosten von 25. In der Tabelle sind die häufig verwendeten Verbindungskosten aufgeführt.

Verlinken	Verbindungskosten	Hinweise
Zwischen physischen Datacenter-Standorten zu wechseln	25 (Standard)	Über WAN-Verbindung verbundene Datacenter.
Zwischen logischen Datacenter-Standorten am selben physischen Standort	0	Logische Rechenzentren befinden sich in demselben physischen Gebäude oder Campus, das über ein LAN verbunden ist.

Verbindungskosten aktualisieren

Sie können die Verbindungskosten zwischen Datacenter-Standorten aktualisieren, um die Latenz zwischen

Standorten wiederzugeben.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Berechtigung zur Konfiguration der Grid-Topologie-Seite".

Schritte

1. Wählen Sie **SUPPORT > Other > Link Cost**.

The screenshot shows the 'Link Cost' configuration page. At the top, there is a header with a logo and the text 'Link Cost' and 'Updated: 2023-02-15 18:09:28 MST'. Below the header, there is a section titled 'Site Names (1 - 3 of 3)' with a refresh icon. This section contains a table with three rows:

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Below the table, there is a 'Show 50 Records Per Page' dropdown, a 'Refresh' button, and navigation links 'Previous', '1', and 'Next'. Below this is a section titled 'Link Costs' with a table:

Link Source	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	

At the bottom right of the 'Link Costs' section, there is an 'Apply Changes' button with a right-pointing arrow.

2. Wählen Sie eine Website unter **Link Source** aus, und geben Sie unter **Link Destination** einen Kostenwert zwischen 0 und 100 ein.

Sie können die Verbindungskosten nicht ändern, wenn die Quelle mit dem Ziel identisch ist.

Um Änderungen abzubrechen, wählen Sie „ Zurücksetzen.

3. Wählen Sie **Änderungen Anwenden**.

Verwenden Sie AutoSupport

Verwenden Sie AutoSupport: Übersicht

Die AutoSupport-Funktion ermöglicht es Ihrem StorageGRID System, Gesundheits- und Statusmeldungen an den technischen Support zu senden.

Durch den Einsatz von AutoSupport werden die Problembestimmung und -Behebung erheblich beschleunigt. Der technische Support überwacht auch den Storage-Bedarf Ihres Systems und hilft Ihnen dabei zu ermitteln, ob Sie neue Nodes oder Standorte hinzufügen müssen. Optional können Sie AutoSupport Meldungen so konfigurieren, dass sie an ein zusätzliches Ziel gesendet werden.

Sie sollten StorageGRID AutoSupport nur auf dem primären Admin-Knoten konfigurieren. Sie müssen jedoch konfigurieren [Hardware-AutoSupport](#) Auf jedem Gerät.

Informationen, die in AutoSupport Meldungen enthalten sind

AutoSupport Meldungen enthalten Informationen, z. B. die folgenden:

- StorageGRID Softwareversion
- Betriebssystemversion
- Attributinformationen auf System- und Standortebeine
- Aktuelle Warnmeldungen und Alarme (Altsystem)
- Aktueller Status aller Grid-Aufgaben, einschließlich historischer Daten
- Verwendung der Admin-Node-Datenbank
- Anzahl der verlorenen oder fehlenden Objekte
- Grid-Konfigurationseinstellungen
- NMS-Einheiten
- Aktive ILM-Richtlinie
- Bereitgestellte Grid-Spezifikations-Datei
- Diagnostische Metriken

Sie können die AutoSupport-Funktion und die einzelnen AutoSupport-Optionen bei der Erstinstallation von StorageGRID aktivieren oder später aktivieren. Wenn AutoSupport nicht aktiviert ist, wird im Grid Manager-Dashboard eine Meldung angezeigt. Die Meldung enthält einen Link zur AutoSupport-Konfigurationsseite.

The AutoSupport feature is disabled. You should enable AutoSupport to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.



Wenn Sie die Nachricht schließen, wird sie erst wieder angezeigt, wenn Ihr Browser-Cache gelöscht wird, auch wenn AutoSupport deaktiviert bleibt.

Was ist Digital Advisor?

Digital Advisor ist Cloud-basiert und nutzt prädiktive Analysen und Community-Wissen der installierten Basis von NetApp. Kontinuierliche Risikobewertungen, prädiktive Warnungen, beschreibende Tipps und automatisierte Aktionen helfen Ihnen, Probleme zu vermeiden, bevor sie auftreten. Dies führt zu verbesserter Systemintegrität und höherer Systemverfügbarkeit.

Sie müssen AutoSupport aktivieren, wenn Sie die Digital Advisor Dashboards und Funktionen auf der NetApp Support-Website verwenden möchten.

["Digital Advisor-Dokumentation"](#)

Protokolle zum Senden von AutoSupport Meldungen

Sie können eines von drei Protokollen zum Senden von AutoSupport Meldungen wählen:

- HTTPS

- HTTP
- SMTP

Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, müssen Sie einen SMTP-Mail-Server konfigurieren.

AutoSupport-Optionen

Sie können eine beliebige Kombination der folgenden Optionen verwenden, um AutoSupport Meldungen an den technischen Support zu senden:

- **Wöchentlich:** Senden Sie automatisch einmal pro Woche AutoSupport-Nachrichten. Standardeinstellung: Aktiviert.
- **Event-triggered:** Sendet automatisch AutoSupport jede Stunde oder wenn wichtige Systemereignisse auftreten. Standardeinstellung: Aktiviert.
- **Auf Anfrage:** Technischen Support erlauben, um zu verlangen, dass Ihr StorageGRID-System AutoSupport-Nachrichten automatisch sendet, was nützlich ist, wenn sie aktiv an einem Problem arbeiten (erfordert HTTPS AutoSupport Übertragungsprotokoll). Standardeinstellung: Deaktiviert.
- **Vom Benutzer ausgelöst:** Senden Sie AutoSupport-Nachrichten jederzeit manuell.

AutoSupport für Appliances

AutoSupport für Appliances meldet StorageGRID-Hardwareprobleme, während StorageGRID AutoSupport StorageGRID-Softwareprobleme meldet (mit Ausnahme von SGF6112, bei denen StorageGRID AutoSupport sowohl Hardware- als auch Softwareprobleme meldet). Sie müssen AutoSupport auf jeder Appliance konfigurieren, mit Ausnahme der SGF6112, für die keine zusätzliche Konfiguration erforderlich ist. AutoSupport wird für Services und Storage Appliances unterschiedlich implementiert.

Sie müssen AutoSupport in SANtricity für jede Storage Appliance aktivieren. Sie können SANtricity AutoSupport während der ersten Appliance-Einrichtung oder nach der Installation einer Appliance konfigurieren:

- Für SG6000 und SG5700 Appliances, "[Konfigurieren Sie AutoSupport in SANtricity System Manager](#)"

AutoSupport Meldungen von E-Series Appliances können in StorageGRID AutoSupport enthalten sein, wenn Sie die AutoSupport-Bereitstellung als Proxy in konfigurieren "[SANtricity System Manager](#)".

StorageGRID AutoSupport meldet keine Hardwareprobleme, z. B. DIMM- oder HIC-Fehler (Host Interface Card). Einige Komponentenfehler können jedoch ausgelöst werden "[Warnmeldungen zu Hardware](#)". Bei StorageGRID Appliances mit einem Baseboard Management Controller (BMC) wie SG100, SG1000, SG6060 oder SGF6024 können Sie E-Mail- und SNMP-Traps konfigurieren, um Hardwareausfälle zu melden:

- "[Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein](#)"
- "[Konfigurieren Sie die SNMP-Einstellungen](#)" Für den SG6000-CN Controller oder die Service Appliances SG100 und SG1000

Verwandte Informationen

["NetApp Support"](#)

Konfigurieren Sie AutoSupport

Sie können die AutoSupport-Funktion und die einzelnen AutoSupport-Optionen bei der

Erstinstallation von StorageGRID aktivieren oder später aktivieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Berechtigung Root-Zugriff oder andere Grid-Konfigurationen.
- Wenn Sie HTTPS zum Senden von AutoSupport-Nachrichten verwenden, haben Sie den ausgehenden Internetzugang auf den primären Admin-Knoten entweder direkt oder bereitgestellt "[Verwenden eines Proxy-Servers](#)" (Eingehende Verbindungen sind nicht erforderlich).
- Wenn HTTP auf der Seite StorageGRID AutoSupport ausgewählt ist, haben Sie einen Proxyserver für die Weiterleitung von AutoSupport-Nachrichten als HTTPS konfiguriert. Die AutoSupport Server von NetApp lehnen über HTTP gesendete Nachrichten ab.

["Erfahren Sie mehr über das Konfigurieren von Administrator-Proxy-Einstellungen"](#).

- Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, haben Sie einen SMTP-Mail-Server konfiguriert. Die gleiche E-Mail-Serverkonfiguration wird für Benachrichtigungen über Alarm E-Mails verwendet (altes System).

Geben Sie das Protokoll für AutoSupport Meldungen an

Sie können eines der folgenden Protokolle zum Senden von AutoSupport Meldungen verwenden:

- **HTTPS:** Dies ist die Standard-Einstellung und wird für Neuinstallationen empfohlen. Dieses Protokoll verwendet Port 443. Wenn Sie möchten [Aktivieren Sie die Funktion „AutoSupport On Demand“](#), Müssen Sie HTTPS verwenden.
- **HTTP:** Wenn Sie HTTP auswählen, müssen Sie einen Proxyserver konfigurieren, um AutoSupport-Nachrichten als HTTPS weiterzuleiten. Die AutoSupport Server von NetApp lehnen über HTTP gesendete Nachrichten ab. Dieses Protokoll verwendet Port 80.
- **SMTP:** Verwenden Sie diese Option, wenn Sie AutoSupport-Nachrichten per E-Mail versenden möchten. Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, müssen Sie auf der Seite Legacy E-Mail-Einrichtung einen SMTP-Mail-Server konfigurieren (**SUPPORT > Alarme (alt) > Legacy E-Mail-Setup**).



SMTP war das einzige Protokoll, das vor der StorageGRID 11.2-Version für AutoSupport-Meldungen verfügbar war. Wenn Sie zunächst eine frühere Version von StorageGRID installiert haben, ist SMTP möglicherweise das ausgewählte Protokoll.

Das von Ihnen festgelegte Protokoll wird für das Senden aller Typen von AutoSupport Meldungen verwendet.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.

Die Seite AutoSupport wird angezeigt, und die Registerkarte **Einstellungen** ist ausgewählt.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings **Results**

Protocol Details

Protocol HTTPS HTTP SMTP

NetApp Support Certificate Validation

AutoSupport Details

Enable Weekly AutoSupport

Enable Event-Triggered AutoSupport

Enable AutoSupport on Demand

Software Updates

Check for software updates

Additional AutoSupport Destination

Enable Additional AutoSupport Destination

Save Send User-Triggered AutoSupport

2. Wählen Sie das Protokoll aus, das Sie zum Senden von AutoSupport Meldungen verwenden möchten.
3. Wenn Sie **HTTPS** ausgewählt haben, wählen Sie aus, ob die Verbindung zum NetApp Support Server mit einem TLS-Zertifikat gesichert werden soll.
 - **NetApp Supportzertifikat verwenden** (Standard): Die Zertifikatvalidierung stellt sicher, dass die Übertragung von AutoSupport Meldungen sicher ist. Das NetApp Supportzertifikat ist bereits mit der StorageGRID Software installiert.
 - **Zertifikat nicht überprüfen**: Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, keine Zertifikatvalidierung zu verwenden, z.B. wenn es ein vorübergehendes Problem mit einem Zertifikat gibt.
4. Wählen Sie **Speichern**.

Alle wöchentlichen, vom Benutzer ausgelösten und von Ereignissen ausgelösten Meldungen werden über das ausgewählte Protokoll gesendet.

Deaktivieren Sie wöchentliche AutoSupport-Meldungen

Standardmäßig wird das StorageGRID System so konfiguriert, dass einmal pro Woche eine AutoSupport Meldung an den NetApp Support gesendet wird.

Um zu bestimmen, wann die wöchentliche AutoSupport-Nachricht gesendet wird, gehen Sie auf die Registerkarte **AutoSupport > Results**. Sehen Sie im Abschnitt **Wöchentliche AutoSupport** den Wert für **Nächste geplante Zeit** an.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Weekly AutoSupport

Next Scheduled Time ⓘ 2021-09-14 21:10:00 MDT

Most Recent Result ⓘ Idle (NetApp Support)

Last Successful Time ⓘ N/A (NetApp Support)

Sie können das automatische Senden von wöchentlichen AutoSupport Meldungen jederzeit deaktivieren.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **Weekly AutoSupport** aktivieren.
3. Wählen Sie **Speichern**.

Deaktivieren Sie ereignisgesteuerte AutoSupport Meldungen

Standardmäßig wird das StorageGRID System so konfiguriert, dass es eine AutoSupport Meldung an den NetApp Support sendet, wenn eine wichtige Meldung oder ein anderes bedeutendes Systemereignis auftritt.

Sie können AutoSupport Meldungen, bei denen Ereignisse ausgelöst wurden, jederzeit deaktivieren.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **Event-Triggered AutoSupport** aktivieren.
3. Wählen Sie **Speichern**.

AutoSupport-on-Demand aktivieren

AutoSupport On Demand kann Ihnen bei der Lösung von Problemen helfen, an denen der technische Support aktiv arbeitet.

AutoSupport-on-Demand ist standardmäßig deaktiviert. Wenn Sie diese Funktion aktivieren, kann der technische Support von Ihrem StorageGRID System automatisch AutoSupport Meldungen senden. Der technische Support kann auch das Abfrageintervall für AutoSupport-on-Demand-Abfragen festlegen.

Der technische Support kann AutoSupport On Demand nicht aktivieren oder deaktivieren.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.
2. Wählen Sie **HTTPS** für das Protokoll aus.

3. Aktivieren Sie das Kontrollkästchen **Weekly AutoSupport** aktivieren.
4. Aktivieren Sie das Kontrollkästchen **AutoSupport on Demand aktivieren**.
5. Wählen Sie **Speichern**.

AutoSupport-on-Demand ist aktiviert, und der technische Support kann AutoSupport-on-Demand-Anfragen an StorageGRID senden.

Deaktivieren Sie die Prüfung auf Softwareupdates

Standardmäßig wendet sich StorageGRID an NetApp, um zu ermitteln, ob Software-Updates für Ihr System verfügbar sind. Wenn ein StorageGRID-Hotfix oder eine neue Version verfügbar ist, wird die neue Version auf der Seite StorageGRID-Aktualisierung angezeigt.

Bei Bedarf können Sie optional die Prüfung auf Softwareupdates deaktivieren. Wenn Ihr System beispielsweise keinen WAN-Zugriff hat, sollten Sie die Prüfung deaktivieren, um Download-Fehler zu vermeiden.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **nach Softwareupdates suchen**.
3. Wählen Sie **Speichern**.

Fügen Sie ein weiteres AutoSupport Ziel hinzu

Wenn Sie AutoSupport aktivieren, werden Zustandsmeldungen und Statusmeldungen an den NetApp Support gesendet. Sie können ein zusätzliches Ziel für alle AutoSupport Meldungen angeben.

Informationen zum Überprüfen oder Ändern des Protokolls zum Senden von AutoSupport Meldungen finden Sie in den Anweisungen an [Geben Sie das Protokoll für AutoSupport Meldungen an](#).



Sie können das SMTP-Protokoll nicht zum Senden von AutoSupport Meldungen an ein weiteres Ziel verwenden.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.
2. Wählen Sie **Zusätzliches AutoSupport-Ziel aktivieren**.
3. Geben Sie Folgendes an:

Feld	Beschreibung
Hostname	Der Hostname oder die IP-Adresse des Servers eines zusätzlichen AutoSupport-Zielservers. Hinweis: Sie können nur ein zusätzliches Ziel eingeben.
Port	Der Port, über den eine Verbindung zu einem zusätzlichen AutoSupport-Zielservers hergestellt wird. Der Standardwert ist Port 80 für HTTP oder Port 443 für HTTPS.

Feld	Beschreibung
Zertifizierungsvalidierung	<p>Ob ein TLS-Zertifikat verwendet wird, um die Verbindung zum zusätzlichen Ziel zu sichern.</p> <ul style="list-style-type: none"> • Wählen Sie Zertifikat nicht verifizieren, um Ihre AutoSupport-Nachrichten ohne Zertifikatvalidierung zu senden. <p>Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, die Zertifikatvalidierung nicht zu verwenden, z. B. wenn ein vorübergehendes Problem mit einem Zertifikat vorliegt.</p> <ul style="list-style-type: none"> • Wählen Sie Benutzerdefiniertes CA-Paket verwenden, um die Zertifikatvalidierung zu verwenden.

4. Wenn Sie **benutzerdefiniertes CA-Paket verwenden** ausgewählt haben, führen Sie einen der folgenden Schritte aus:

- Wählen Sie **Durchsuchen**, navigieren Sie zu der Datei mit den Zertifikaten und wählen Sie dann **Öffnen**, um die Datei hochzuladen.
- Verwenden Sie ein Bearbeitungswerkzeug, um alle Inhalte der einzelnen PEM-kodierten CA-Zertifikatdateien in das Feld **CA Bundle** zu kopieren und einzufügen, das in der Zertifikatskette verknüpft ist.

Sie müssen Folgendes einschließen `-----BEGIN CERTIFICATE-----` Und `-----END CERTIFICATE-----` Wählen Sie aus.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination

Hostname

Port

Certificate Validation

CA Bundle

5. Wählen Sie **Speichern**.

Alle zukünftigen wöchentlichen, ereignisgesteuert und vom Benutzer ausgelösten AutoSupport Meldungen werden an das zusätzliche Ziel gesendet.

Senden Sie manuell eine AutoSupport Meldung aus

Um den technischen Support bei der Fehlerbehebung bei Problemen mit Ihrem StorageGRID System zu unterstützen, können Sie manuell eine AutoSupport Meldung auslösen, die gesendet werden soll.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über die Berechtigung Root-Zugriff oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.
2. Wählen Sie auf der Registerkarte **Einstellungen** die Option **vom Benutzer ausgelöste AutoSupport** senden.

StorageGRID versucht, eine AutoSupport Nachricht an den technischen Support zu senden. Wenn der Versuch erfolgreich ist, werden die **aktuellsten Ergebnisse** und **Letzte erfolgreiche Zeit** Werte auf der

Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, werden die **neuesten Ergebnisse**-Werte auf „Fehlgeschlagen“ aktualisiert, und StorageGRID versucht nicht, die AutoSupport-Nachricht erneut zu senden.



Nachdem Sie eine vom Benutzer ausgelöste AutoSupport-Nachricht gesendet haben, aktualisieren Sie die AutoSupport-Seite im Browser nach 1 Minute, um auf die neuesten Ergebnisse zuzugreifen.

Fehlerbehebung für AutoSupport Meldungen

Wenn das Senden einer AutoSupport Meldung fehlschlägt, führt das StorageGRID System abhängig vom Typ der AutoSupport Meldung unterschiedliche Aktionen durch. Sie können den Status von AutoSupport-Meldungen überprüfen, indem Sie **SUPPORT > Werkzeuge > AutoSupport > Ergebnisse** auswählen.

Wenn die AutoSupport-Meldung nicht gesendet wird, wird „failed“ auf der Registerkarte **Results** der Seite **AutoSupport** angezeigt.

Category	Property	Value
Weekly AutoSupport	Next Scheduled Time	2023-02-18 04:37:38 MST
	Most Recent Result	Idle (NetApp Support)
	Last Successful Time	N/A (NetApp Support)
Event-Triggered AutoSupport	Most Recent Result	Failed (NetApp Support)
	Last Successful Time	N/A (NetApp Support)



Wenn Sie einen Proxyserver für die Weiterleitung von AutoSupport-Nachrichten an NetApp konfiguriert haben, sollten Sie dies tun "[Überprüfen Sie, ob die Konfigurationseinstellungen des Proxy-Servers korrekt sind](#)".

Wöchentlicher AutoSupport-Nachrichtenfehler

Wenn eine wöchentliche AutoSupport-Meldung nicht gesendet werden kann, werden im StorageGRID System folgende Aktionen ausgeführt:

1. Aktualisiert das Attribut für das aktuellste Ergebnis, um es erneut zu versuchen.
2. Versucht, die AutoSupport Meldung alle vier Minuten für eine Stunde 15 Mal erneut zu senden.
3. Nach einer Stunde des Sendefehlens aktualisiert das Attribut „Aktuelles Ergebnis“ auf „Fehlgeschlagen“.
4. Versucht, eine AutoSupport-Nachricht zum nächsten geplanten Zeitpunkt erneut zu senden.
5. Behält den regulären AutoSupport-Zeitplan bei, wenn die Meldung fehlschlägt, weil der NMS-Dienst nicht verfügbar ist und wenn eine Meldung vor sieben Tagen gesendet wird.
6. Wenn der NMS-Dienst wieder verfügbar ist, sendet sofort eine AutoSupport-Nachricht, wenn eine Nachricht für sieben Tage oder länger nicht gesendet wurde.

Vom Benutzer ausgelöste oder ereignisgesteuerte AutoSupport-Meldung ist fehlgeschlagen

Wenn eine vom Benutzer ausgelöste oder eine AutoSupport Meldung, die aufgrund eines Ereignisses ausgelöst wird, nicht gesendet wird, ergreift das StorageGRID System folgende Maßnahmen:

1. Zeigt eine Fehlermeldung an, wenn der Fehler bekannt ist. Wenn z. B. ein Benutzer das SMTP-Protokoll auswählt, ohne korrekte E-Mail-Konfigurationseinstellungen vorzunehmen, wird der folgende Fehler angezeigt: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Versucht nicht, die Nachricht erneut zu senden.
3. Protokolliert den Fehler in `nms.log`.

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und Ihr E-Mail-Server ausgeführt wird (**SUPPORT > Alarme (alt) > > Legacy E-Mail-Setup**). Die folgende Fehlermeldung kann auf der AutoSupport-Seite angezeigt werden: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Erfahren Sie, wie Sie ["Konfigurieren Sie die E-Mail-Servereinstellungen"](#).

Korrigieren Sie einen Fehler bei der AutoSupport-Meldung

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und Ihr E-Mail-Server ausgeführt wird. Die folgende Fehlermeldung kann auf der AutoSupport-Seite angezeigt werden: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Senden Sie AutoSupport Nachrichten aus der E-Series über StorageGRID

Sie können AutoSupport Meldungen von E-Series SANtricity System Manager über einen StorageGRID Admin-Node anstelle des Storage Appliance Management-Ports an den technischen Support senden.

Siehe ["E-Series Hardware AutoSupport"](#) Weitere Informationen zur Verwendung von AutoSupport mit E-Series Appliances

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über Administratorrechte oder Root-Zugriffsberechtigungen für die Storage-Appliance.
- Sie haben SANtricity AutoSupport konfiguriert:
 - Für SG6000 und SG5700 Appliances, "[Konfigurieren Sie AutoSupport in SANtricity System Manager](#)"



Sie müssen über SANtricity-Firmware 8.70 oder höher verfügen, um mit dem Grid Manager auf SANtricity System Manager zuzugreifen.

Über diese Aufgabe

E-Series AutoSupport-Meldungen enthalten Details zur Storage Hardware und sind spezifischer als andere AutoSupport-Meldungen, die vom StorageGRID System gesendet werden.

Sie können eine spezielle Proxy-Server-Adresse in SANtricity System Manager konfigurieren, um AutoSupport-Meldungen über einen StorageGRID-Admin-Knoten ohne Verwendung des Management-Ports der Appliance zu übertragen. AutoSupport-Nachrichten, die auf diese Weise übertragen werden, werden vom gesendet "[Administratorknoten des bevorzugten Absenders](#)", Und sie verwenden jede "[Administrator-Proxy-Einstellungen](#)" Die im Grid Manager konfiguriert wurden.

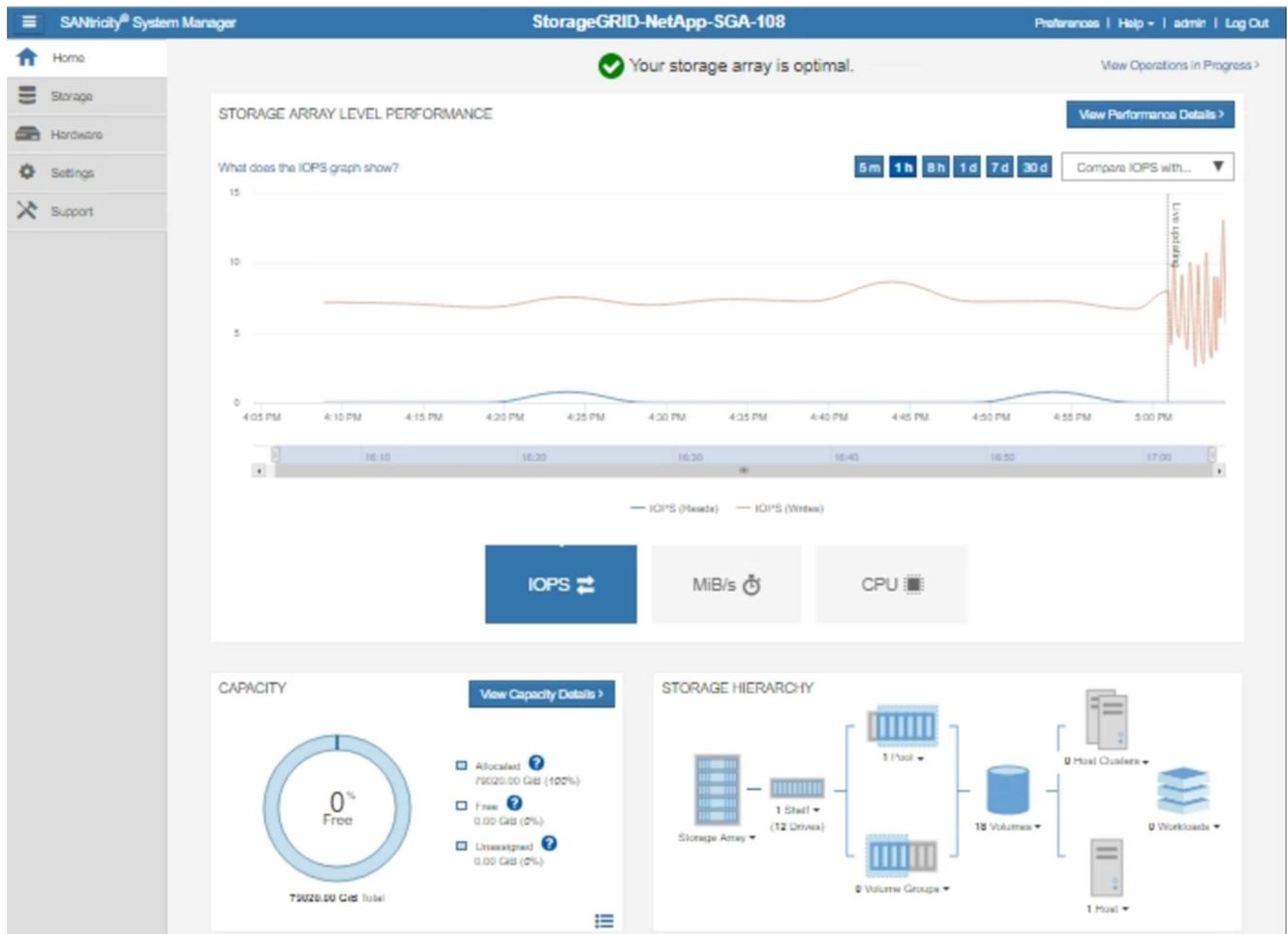


Dieses Verfahren dient nur zur Konfiguration eines StorageGRID-Proxyservers für AutoSupport-Meldungen der E-Serie. Weitere Informationen zur Konfiguration der E-Series AutoSupport finden Sie unter "[NetApp E-Series und SANtricity Dokumentation](#)".

Schritte

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie in der Liste der Knoten links den Speicher-Appliance-Node aus, den Sie konfigurieren möchten.
3. Wählen Sie **SANtricity System Manager**.

Die Startseite von SANtricity System Manager wird angezeigt.



4. Wählen Sie **SUPPORT** > **Support Center** > **AutoSupport**.

Die Seite AutoSupport-Vorgänge wird angezeigt.

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled 

[Enable/Disable AutoSupport Features](#)

AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)

AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)

Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)

The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)

Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)

Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Wählen Sie **AutoSupport-Bereitstellungsmethode konfigurieren**.

Die Seite AutoSupport-Bereitstellungsmethode konfigurieren wird angezeigt.

Configure AutoSupport Delivery Method ✕

Select AutoSupport dispatch delivery method...

HTTPS
 HTTP
 Email

HTTPS delivery settings Show destination address

Connect to support team...

Directly ?
 via Proxy server ?

Host address ?

Port number ?

My proxy server requires authentication
 via Proxy auto-configuration script (PAC) ?

6. Wählen Sie **HTTPS** für die Liefermethode aus.



Das Zertifikat, das HTTPS aktiviert, ist vorinstalliert.

7. Wählen Sie **über Proxy-Server**.

8. Eingabe `tunnel-host` Für die **Host-Adresse**.

`tunnel-host` Hat die besondere Adresse, um einen Admin-Node zum Senden von E-Series AutoSupport Meldungen zu verwenden.

9. Eingabe `10225` Für die * Portnummer*.

`10225` Ist die Portnummer auf dem StorageGRID Proxy-Server, der AutoSupport Meldungen vom E-Series Controller in der Appliance empfängt.

10. Wählen Sie **Testkonfiguration** aus, um die Routing- und Konfigurationseinstellungen Ihres AutoSupport Proxy-Servers zu testen.

Falls richtig, erscheint eine Meldung in einem grünen Banner: „Ihre AutoSupport-Konfiguration wurde verifiziert.“

Wenn der Test fehlschlägt, wird eine Fehlermeldung in einem roten Banner angezeigt. Überprüfen Sie Ihre StorageGRID-DNS-Einstellungen und Netzwerk, stellen Sie sicher, dass die ["Administratorknoten des bevorzugten Absenders"](#) Kann eine Verbindung zur NetApp Support Site herstellen und den Test erneut versuchen.

11. Wählen Sie **Speichern**.

Die Konfiguration wird gespeichert, und es wird eine Bestätigungsmeldung angezeigt: „AutoSupport-Bereitstellungsmethode wurde konfiguriert.“

Managen Sie Storage-Nodes

Storage-Nodes Verwalten: Übersicht

Storage-Nodes stellen Festplattenkapazität und Services zur Verfügung. Das Verwalten von Storage-Nodes umfasst Folgendes:

- Management der Storage-Optionen
- Um zu verstehen, welche Wasserzeichen für das Storage-Volume sind und wie Sie mit Wasserzeichen-Überschreibungen steuern können, wann Storage-Nodes schreibgeschützt sind
- Monitoring und Management des Speicherplatzes, der für Objektmetadaten verwendet wird
- Globale Einstellungen für gespeicherte Objekte konfigurieren
- Konfigurationseinstellungen für Speicherknoten werden angewendet
- Verwalten vollständiger Speicherknoten

Was ist ein Storage-Node?

Storage-Nodes managen und speichern Objektdaten und Metadaten. Jedes StorageGRID System muss mindestens drei Storage-Nodes aufweisen. Wenn Sie über mehrere Standorte verfügen, muss jeder Standort im StorageGRID System auch drei Storage-Nodes aufweisen.

Ein Storage Node umfasst die Services und Prozesse, die zum Speichern, Verschieben, Überprüfen und Abrufen von Objektdaten und Metadaten auf der Festplatte erforderlich sind. Auf der Seite **NODES** können Sie detaillierte Informationen zu den Speicherknoten anzeigen.

Was ist der ADC-Dienst?

Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen miteinander. Der ADC-Service wird auf jedem der ersten drei Storage-Nodes an einem Standort gehostet.

Der ADC-Dienst verwaltet Topologiedaten, einschließlich Standort und Verfügbarkeit von Diensten. Wenn ein Grid-Knoten Informationen von einem anderen Grid-Knoten benötigt oder eine Aktion von einem anderen Grid-Knoten ausgeführt werden muss, kontaktiert er einen ADC-Service, um den besten Grid-Knoten für die Bearbeitung seiner Anforderung zu finden. Darüber hinaus behält der ADC-Dienst eine Kopie der Konfigurationspakete der StorageGRID-Bereitstellung bei, sodass jeder Grid-Knoten aktuelle Konfigurationsinformationen abrufen kann. ADC-Informationen für einen Speicherknoten können Sie auf der

Seite Grid Topology anzeigen (**SUPPORT > Grid Topology**).

Zur Erleichterung von verteilten und isanded-Operationen synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen über Services und Topologie mit den anderen ADC-Diensten im StorageGRID-System.

Im Allgemeinen unterhalten alle Rasterknoten eine Verbindung zu mindestens einem ADC-Dienst. So wird sichergestellt, dass die Grid-Nodes immer auf die neuesten Informationen zugreifen. Wenn Grid-Nodes verbunden sind, speichern sie Zertifikate anderer Grid-Nodes, sodass die Systeme auch dann weiterhin mit bekannten Grid-Nodes funktionieren können, wenn ein ADC-Service nicht verfügbar ist. Neue Grid-Knoten können nur Verbindungen über einen ADC-Dienst herstellen.

Durch die Verbindung jedes Grid-Knotens kann der ADC-Service Topologiedaten erfassen. Die Informationen zu diesem Grid-Node umfassen die CPU-Last, den verfügbaren Festplattenspeicher (wenn der Storage vorhanden ist), unterstützte Services und die Standort-ID des Grid-Node. Andere Dienste fragen den ADC-Service nach Topologiedaten durch Topologieabfragen. Der ADC-Dienst reagiert auf jede Abfrage mit den neuesten Informationen, die vom StorageGRID-System empfangen wurden.

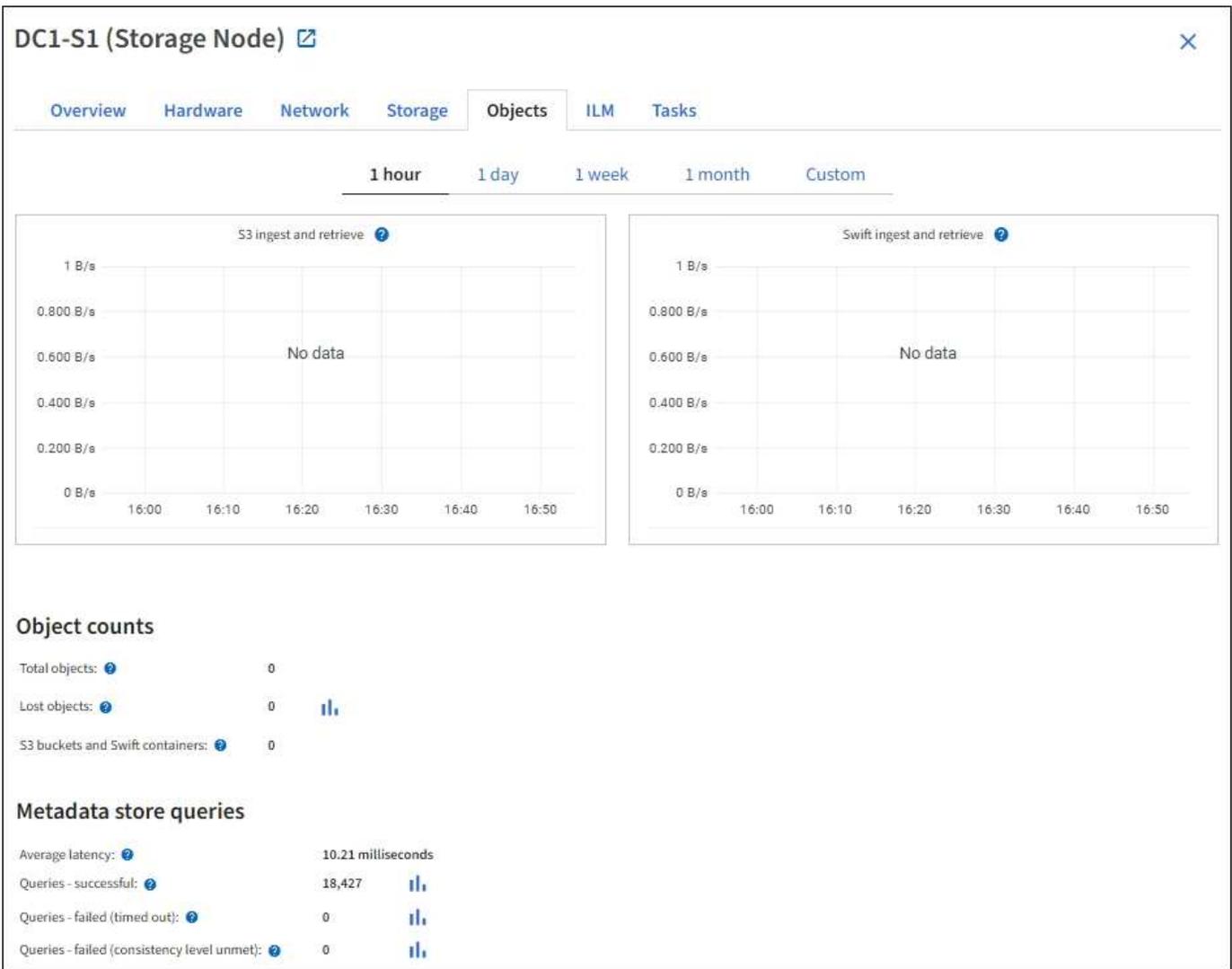
Was ist der DDS-Service?

Der DDS-Service (Distributed Data Store) wird von einem Storage-Node gehostet und führt Hintergrundaufgaben zu den im StorageGRID-System gespeicherten Objektmetadaten durch.

Anzahl der Objekte

Der DDS-Dienst verfolgt die Gesamtzahl der im StorageGRID-System aufgenommenen Objekte sowie die Gesamtzahl der über die unterstützten Schnittstellen (S3 oder Swift) des Systems aufgenommenen Objekte.

Die Anzahl der Objekte insgesamt wird auf der Seite Nodes > Registerkarte Objekte für jeden Storage Node angezeigt.



Abfragen

Sie können die durchschnittliche Zeit für die Ausführung einer Abfrage zum Metadatenpeicher durch den spezifischen DDS-Dienst, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtzahl der fehlgeschlagenen Abfragen für ein Timeout-Problem identifizieren.

Vielleicht möchten Sie nach Abfrageinformationen suchen, um den Zustand des Metadatenpeichers, Cassandra, zu überwachen. Dies hat Auswirkungen auf die Aufnahme- und Abrufleistung des Systems. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenpeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl von verfügbaren Metadatenpeichern zum Zeitpunkt der Durchführung einer Abfrage durch den spezifischen DDS-Service.

Auf der Diagnosesseite erhalten Sie zusätzliche Informationen über den aktuellen Zustand Ihres Rasters. Siehe ["Führen Sie eine Diagnose aus"](#).

Konsistenzgarantien und -Kontrollen

StorageGRID garantiert die Konsistenz zwischen Lese- und Schreibvorgängen bei neu erstellten Objekten.

Jeder GET-Vorgang nach einem erfolgreich abgeschlossenen PUT-Vorgang kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen bleiben irgendwann konsistent.

Was ist der LDR-Service?

Der Service Local Distribution Router (LDR) wird von jedem Speicherknoten gehostet und übernimmt den Content-Transport des StorageGRID-Systems. Der Content-Transport umfasst viele Aufgaben, einschließlich Datenspeicherung, Routing und Bearbeitung von Anfragen. Der LDR-Dienst erledigt die meiste harte Arbeit des StorageGRID-Systems durch die Verarbeitung von Datenübertragungslasten und Datenverkehrsfunktionen.

Der LDR-Service übernimmt folgende Aufgaben:

- Abfragen
- Information Lifecycle Management-Aktivitäten (ILM)
- Löschen von Objekten
- Objekt-Storage
- Objektdatenübertragung von einem anderen LDR-Service (Storage Node)
- Datenspeicher-Management
- Protokollschnittstellen (S3 und Swift)

Der LDR-Service managt auch die Zuordnung von S3- und Swift-Objekten zu den eindeutigen „Content Handles“ (UUIDs), die das StorageGRID System jedem aufgenommene Objekt zuweist.

Abfragen

LDR-Abfragen umfassen Abfragen zum Objektspeicherort während Abruf- und Archivierungsvorgängen. Sie können die durchschnittliche Zeit zum Ausführen einer Abfrage, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtzahl der Abfragen, die aufgrund eines Timeout-Problems fehlgeschlagen sind, identifizieren.

Sie können Abfrageinformationen prüfen, um den Zustand des MetadatenSpeichers zu überwachen und die Aufnahme- und Abrufleistung des Systems zu beeinträchtigen. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der MetadatenSpeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl an verfügbaren MetadatenSpeichern zum Zeitpunkt einer Abfrage durch den spezifischen LDR-Service.

Auf der Diagnosesseite erhalten Sie zusätzliche Informationen über den aktuellen Zustand Ihres Rasters. Siehe ["Führen Sie eine Diagnose aus"](#).

ILM-Aktivität

Mithilfe der ILM-Metriken (Information Lifecycle Management) können Sie die Bewertung von Objekten für die ILM-Implementierung durchführen. Sie können diese Metriken im Dashboard oder unter **NODES > Storage Node > ILM** anzeigen.

Objektspeicher

Der zugrunde liegende Datenspeicher eines LDR-Service wird in eine feste Anzahl an Objektspeichern (auch

Storage-Volumes genannt) unterteilt. Jeder Objektspeicher ist ein separater Bereitstellungspunkt.

Auf der Seite Knoten > Speicher werden die Objektspeicher für einen Speicherknoten angezeigt.

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

Das Objekt speichert in einem Storage-Node werden durch eine Hexadezimalzahl zwischen 0000 und 002F identifiziert, die als Volume-ID bezeichnet wird. Der Speicherplatz ist im ersten Objektspeicher (Volume 0) für Objekt-Metadaten in einer Cassandra-Datenbank reserviert. Für Objektdaten werden alle verbleibenden Speicherplatz auf diesem Volume verwendet. Alle anderen Objektspeichern werden ausschließlich für Objektdaten verwendet, zu denen replizierte Kopien und nach dem Erasure-Coding-Verfahren Fragmente gehören.

Um sicherzustellen, dass selbst der Speicherplatz für replizierte Kopien genutzt wird, werden Objektdaten für ein bestimmtes Objekt auf Basis des verfügbaren Storage in einem Objektspeicher gespeichert. Wenn ein oder mehrere Objektspeichern die Kapazität voll haben, speichern die übrigen Objektspeicher weiterhin Objekte, bis kein Platz mehr auf dem Speicherknoten vorhanden ist.

Metadatensicherung

Objektmetadaten sind Informationen mit oder eine Beschreibung eines Objekts, z. B. Änderungszeit des Objekts oder der Storage-Standort. StorageGRID speichert Objekt-Metadaten in einer Cassandra-Datenbank, die über eine Schnittstelle zum LDR-Service verfügt.

Um Redundanz sicherzustellen und so vor Verlust zu schützen, werden an jedem Standort drei Kopien von Objekt-Metadaten aufbewahrt. Diese Replikation ist nicht konfigurierbar und wird automatisch ausgeführt.

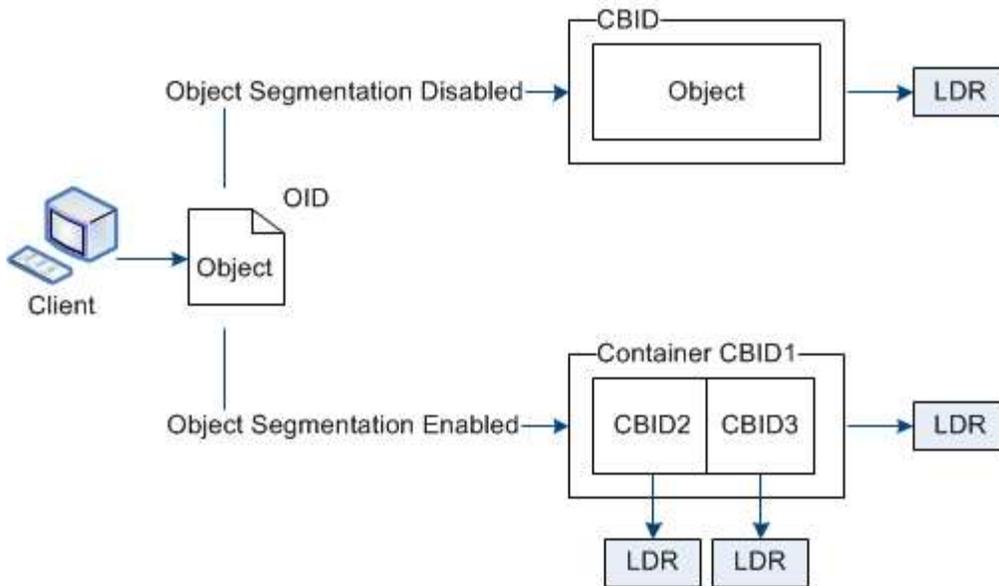
"Management von Objekt-Metadaten-Storage"

Verwenden Sie Speicheroptionen

Was ist Objektsegmentierung?

Bei der Objektsegmentierung wird ein Objekt in eine Sammlung kleinerer Objekte fester Größe aufgeteilt, um die Storage- und Ressourcennutzung für große Objekte zu optimieren. Auch beim S3-Multi-Part-Upload werden segmentierte Objekte erstellt, wobei ein Objekt die einzelnen Teile darstellt.

Wenn ein Objekt in das StorageGRID-System aufgenommen wird, teilt der LDR-Service das Objekt in Segmente auf und erstellt einen Segment-Container, der die Header-Informationen aller Segmente als Inhalt auflistet.



Beim Abruf eines Segment-Containers fasst der LDR-Service das ursprüngliche Objekt aus seinen Segmenten zusammen und gibt das Objekt dem Client zurück.

Der Container und die Segmente werden nicht unbedingt auf demselben Storage Node gespeichert. Container und Segmente können auf jedem Storage-Node innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

Jedes Segment wird vom StorageGRID System unabhängig behandelt und trägt zur Anzahl der Attribute wie verwaltete Objekte und gespeicherte Objekte bei. Wenn ein im StorageGRID System gespeichertes Objekt beispielsweise in zwei Segmente aufgeteilt wird, erhöht sich der Wert von verwalteten Objekten nach Abschluss der Aufnahme um drei Segmente:

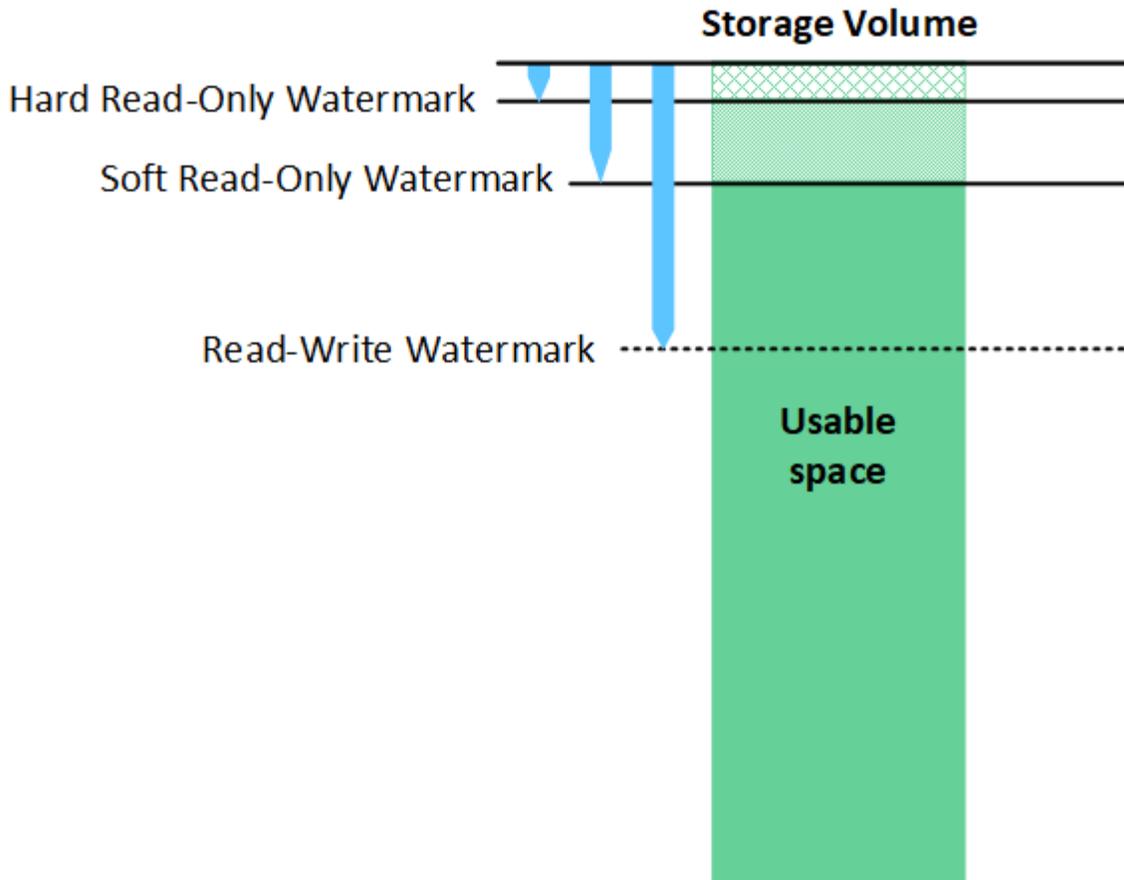
`segment container + segment 1 + segment 2 = three stored objects`

Die Performance beim Umgang mit großen Objekten lässt sich verbessern, indem Folgendes sichergestellt wird:

- Jedes Gateway und jeder Storage-Node verfügt über eine ausreichende Netzwerkbandbreite für den erforderlichen Durchsatz. Konfigurieren Sie beispielsweise separate Grid- und Client-Netzwerke auf 10-Gbit/s-Ethernet-Schnittstellen.
- Für den erforderlichen Durchsatz werden ausreichend Gateway und Storage-Nodes implementiert.
- Jeder Storage-Node verfügt über eine ausreichende Festplatten-I/O-Performance für den erforderlichen Durchsatz.

Was sind Wasserzeichen für Storage-Volumes?

StorageGRID verwendet drei Storage-Volume-Wasserzeichen, um sicherzustellen, dass Storage-Nodes sicher in einen schreibgeschützten Zustand überführt werden, bevor deren Speicherplatz kritisch knapp wird. Damit können Storage-Nodes, die aus einem schreibgeschützten Zustand migriert wurden, erneut Lese- und Schreibvorgänge werden.



Storage Volume-Wasserzeichen gelten nur für den Speicherplatz, der für replizierte und nach Datenkonsistenz (Erasure Coding) verwendet wird. Weitere Informationen über den Speicherplatz, der für Objekt-Metadaten auf Volume 0 reserviert ist, finden Sie unter "[Management von Objekt-Metadaten-Storage](#)".

Was ist das Soft Read-Only Watermark?

Das **Speichervolumen Soft Read-Only Watermark** ist das erste Wasserzeichen, das angibt, dass der für Objektdaten nutzbare Speicherplatz eines Speicherknoten voll wird.

Wenn jedes Volume in einem Storage-Node weniger freien Speicherplatz als das Soft Read-Only-Wasserzeichen dieses Volumes besitzt, wechselt der Storage-Node in den Modus *read-only*. Schreibgeschützter Modus bedeutet, dass der Storage Node für den Rest des StorageGRID Systems schreibgeschützte Dienste anbietet, aber alle ausstehenden Schreibenanforderungen erfüllt.

Angenommen, jedes Volume in einem Speicherknoten hat einen Soft Read-Only-Wasserzeichen von 10 GB. Sobald jedes Volume weniger als 10 GB freien Speicherplatz hat, wechselt der Storage-Node in den Modus „Soft Read“.

Was ist die Hard Read-Only Watermark?

Das **Speichervolumen Hard Read-Only Watermark** ist das nächste Wasserzeichen, um anzuzeigen, dass der nutzbare Speicherplatz eines Knotens für Objektdaten voll wird.

Wenn der freie Speicherplatz auf einem Volume kleiner ist als das harte Read-Only-Wasserzeichen dieses Volumes, schlägt das Schreiben auf das Volume fehl. Schreibvorgänge auf anderen Volumes können jedoch fortgesetzt werden, bis der freie Speicherplatz auf diesen Volumes kleiner als ihre Hard Read-Only-

Wasserzeichen ist.

Angenommen, jedes Volume in einem Speicherknoten hat einen Hard Read-Only-Wasserzeichen von 5 GB. Sobald jedes Volume weniger als 5 GB freien Speicherplatz hat, akzeptiert der Speicherknoten keine Schreibanforderungen mehr.

Der Hard Read-Only-Wasserzeichen ist immer kleiner als der Soft Read-Only-Wasserzeichen.

Was ist der Read-Write-Wasserzeichen?

Das **Storage Volume Read-Write Watermark** gilt nur für Storage-Nodes, die in den schreibgeschützten Modus gewechselt sind. Er bestimmt, wann der Node wieder Lese-/Schreibzugriff werden kann. Wenn der freie Speicherplatz auf einem Speichervolumen in einem Speicherknoten größer ist als das Read-Write-Wasserzeichen dieses Volumens, wechselt der Knoten automatisch zurück in den Lese-Schreib-Zustand.

Angenommen, der Storage-Node ist in den schreibgeschützten Modus migriert. Nehmen Sie auch an, dass jedes Volume ein Read-Write-Wasserzeichen von 30 GB hat. Sobald der freie Speicherplatz eines beliebigen Volumens auf 30 GB ansteigt, wird der Node erneut zum Lesen/Schreiben.

Der Read-Write-Wasserzeichen ist immer größer als der Soft Read-Only-Wasserzeichen und der Hard Read-Only-Wasserzeichen.

Anzeigen von Wasserzeichen für Speichervolumen

Sie können die aktuellen Einstellungen für Wasserzeichen und die systemoptimierten Werte anzeigen. Wenn keine optimierten Wasserzeichen verwendet werden, können Sie festlegen, ob Sie die Einstellungen anpassen können oder sollten.

Bevor Sie beginnen

- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

Aktuelle Wasserzeichen-Einstellungen anzeigen

Im Grid Manager können Sie die aktuellen Einstellungen für Speicherwasserzeichen anzeigen.

Schritte

1. Wählen Sie **KONFIGURATION > System > Speicheroptionen**.
2. Sehen Sie sich im Abschnitt Speicherwasserzeichen die Einstellungen für die drei Überschreibungen der Speichervolumen an.

Storage Options

- Overview
- Configuration

Storage Options Overview

Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

- Wenn die Wasserzeichen **0** überschreiben, sind alle drei Wasserzeichen für jedes Speichervolumen auf jedem Speicherknoten optimiert, basierend auf der Größe des Speicherknoten und der relativen Kapazität des Volumes.

Dies ist die Standardeinstellung und die empfohlene Einstellung. Sie sollten diese Werte nicht aktualisieren. Nach Bedarf können Sie optional [Anzeigen optimierter Speicherabdrücke](#).

- Wenn es sich bei den Wasserzeichen um nicht-0-Werte handelt, werden benutzerdefinierte (nicht optimierte) Wasserzeichen verwendet. Es wird nicht empfohlen, benutzerdefinierte Wasserzeichen zu verwenden. Befolgen Sie die Anweisungen für "[Fehlerbehebung Warnungen bei niedriger Schreibschutzmarke überschreiben](#)" Um zu bestimmen, ob Sie die Einstellungen anpassen können oder sollen.

Anzeigen optimierter Speicherabdrücke

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das **Speichervolumen Soft Read-Only Watermark** berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

1. Wählen Sie **SUPPORT > Tools > Metriken**.
2. Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
3. Um das empfohlene Mindestwasserzeichen für weichen, schreibgeschützten Wert anzuzeigen, geben Sie die folgende Prometheus-Metrik ein, und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der mindestens optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das **Speichervolumen-Soft-Read-Only-Wasserzeichen**, wird für den

Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

4. Um das empfohlene maximale Softread-only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der maximal optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt.

Management von Objekt-Metadaten-Storage

Die Kapazität der Objektmetadaten eines StorageGRID Systems steuert die maximale Anzahl an Objekten, die auf diesem System gespeichert werden können. Um sicherzustellen, dass Ihr StorageGRID System über ausreichend Platz zum Speichern neuer Objekte verfügt, müssen Sie wissen, wo und wie StorageGRID Objekt-Metadaten speichert.

Was sind Objekt-Metadaten?

Objektmetadaten sind alle Informationen, die ein Objekt beschreiben. StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im Grid zu verfolgen und den Lebenszyklus eines jeden Objekts mit der Zeit zu managen.

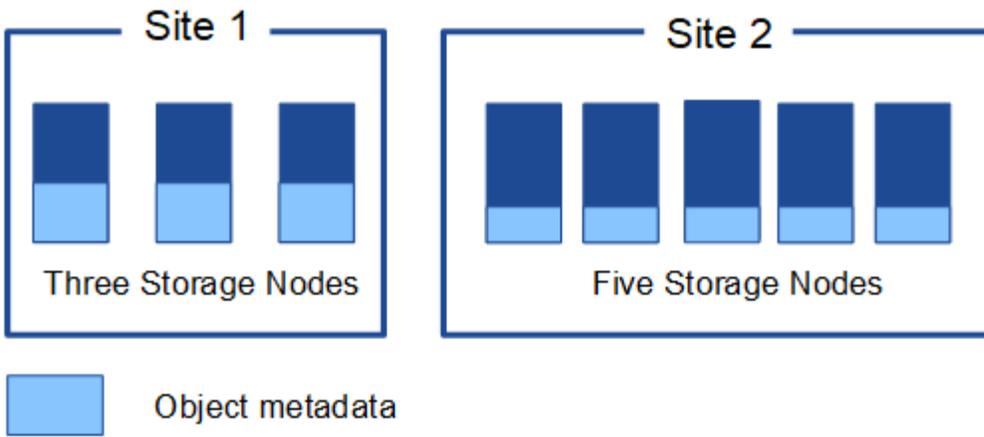
Für ein Objekt in StorageGRID enthalten die Objektmetadaten die folgenden Informationstypen:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), dem Objektnamen, dem Namen des S3-Buckets oder Swift-Containers, dem Mandanten-Kontonamen oder -ID, der logischen Größe des Objekts, dem Datum und der Uhrzeit der ersten Erstellung des Objekts und Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, Segment-IDs und Datengrößen.

Wie werden Objekt-Metadaten gespeichert?

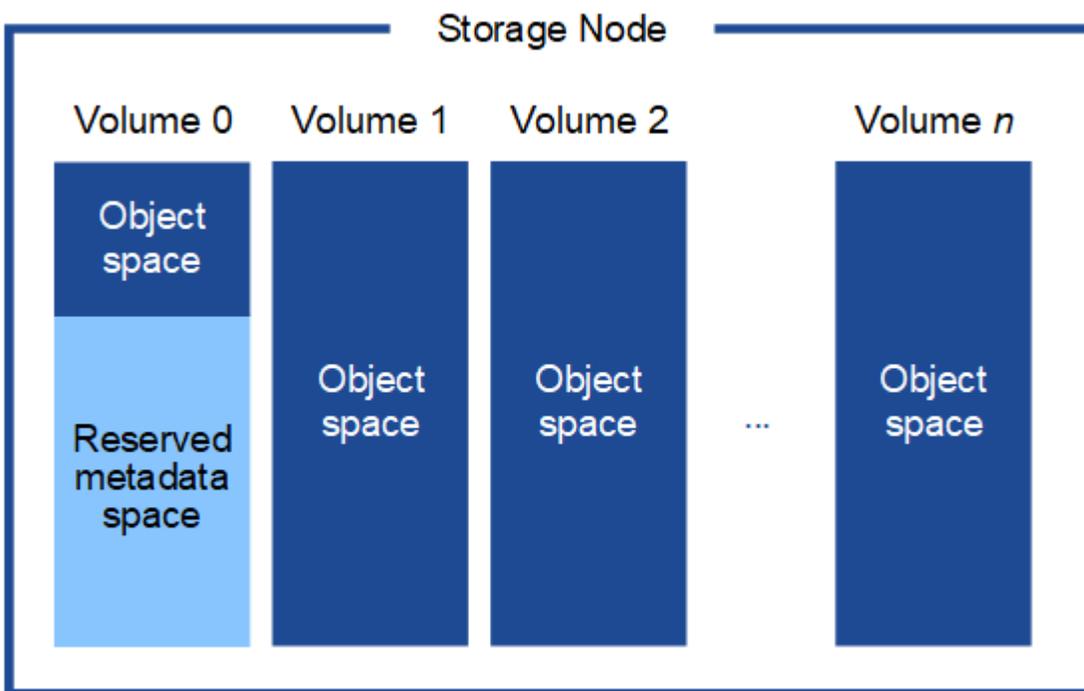
StorageGRID speichert Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert werden. Um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen, speichert StorageGRID drei Kopien der Metadaten für alle Objekte im System an jedem Standort.

Diese Abbildung zeigt die Speicherknoten an zwei Standorten. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten. Die Metadaten jedes Standorts werden unter alle Storage-Nodes an diesem Standort unterteilt.



Wo werden Objekt-Metadaten gespeichert?

Diese Abbildung zeigt die Storage Volumes für einen einzelnen Storage-Node.



Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objekt-Metadaten auf dem Storage Volume 0 jedes Storage-Nodes. Sie verwendet den reservierten Speicherplatz zum Speichern von Objektmetadaten und zum Ausführen wichtiger Datenbankvorgänge. Alle übrigen Speicherplatz auf dem Storage Volume 0 und allen anderen Storage Volumes im Storage Node werden ausschließlich für Objektdaten (replizierte Kopien und nach Datenkonsistenz) verwendet.

Der Speicherplatz, der für Objektmetadaten auf einem bestimmten Storage Node reserviert ist, hängt von mehreren Faktoren ab, die im Folgenden beschrieben werden.

Einstellung für reservierten Speicherplatz für Metadaten

Die Einstellung *Metadaten Reserved Space* stellt die Menge an Speicherplatz dar, die für Metadaten auf Volume 0 jedes Storage-Node reserviert wird. Wie in der Tabelle gezeigt, basiert der Standardwert dieser Einstellung auf:

- Die Softwareversion, die Sie bei der Erstinstallation von StorageGRID verwendet haben.
- Die RAM-Menge auf jedem Storage-Node.

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Größe auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz für Metadaten
11.5 bis 11.7	128 GB oder mehr auf jedem Storage-Node im Grid	8 TB (8,000 GB)
	Weniger als 128 GB auf jedem Storage-Node im Grid	3 TB (3,000 GB)
11.1 bis 11.4	128 GB oder mehr auf jedem Speicherknoten an einem beliebigen Standort	4 TB (4,000 GB)
	Weniger als 128 GB auf jedem Speicherknoten an jedem Standort	3 TB (3,000 GB)
11.0 oder früher	Beliebiger Betrag	2 TB (2,000 GB)

Einstellung für reservierten Speicherplatz für Metadaten anzeigen

Befolgen Sie diese Schritte, um die Einstellung für reservierten Speicherplatz für Metadaten für Ihr StorageGRID-System anzuzeigen.

Schritte

1. Wählen Sie **KONFIGURATION > System > Speicheroptionen**.
2. Suchen Sie in der Tabelle Speicherwasserzeichen **Metadatenreservierter Speicherplatz**.



Storage Options Overview

Updated: 2021-12-10 13:53:01 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	8,000 GB

Im Screenshot beträgt der Wert **Metadaten reservierter Speicherplatz** 8,000 GB (8 TB). Dies ist die Standardeinstellung für eine neue StorageGRID 11.6 oder höher-Installation, bei der jeder Speicherknoten mindestens 128 GB RAM hat.

Tatsächlich reservierter Speicherplatz für Metadaten

Im Gegensatz zur Einstellung „systemweiter reservierter Speicherplatz für Metadaten“ wird für jeden Storage-Node der tatsächlich reservierte Speicherplatz für Objektmetadaten ermittelt. Für jeden bestimmten Storage-Node hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe des Volumes 0 für den Node und der systemweiten Einstellung **Metadaten reservierter Speicherplatz** ab.

Größe von Volume 0 für den Node	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht in der Produktion)	10% des Volumens 0
500 GB oder mehr	Die kleineren Werte: <ul style="list-style-type: none">• Lautstärke 0• Einstellung für reservierten Speicherplatz für Metadaten

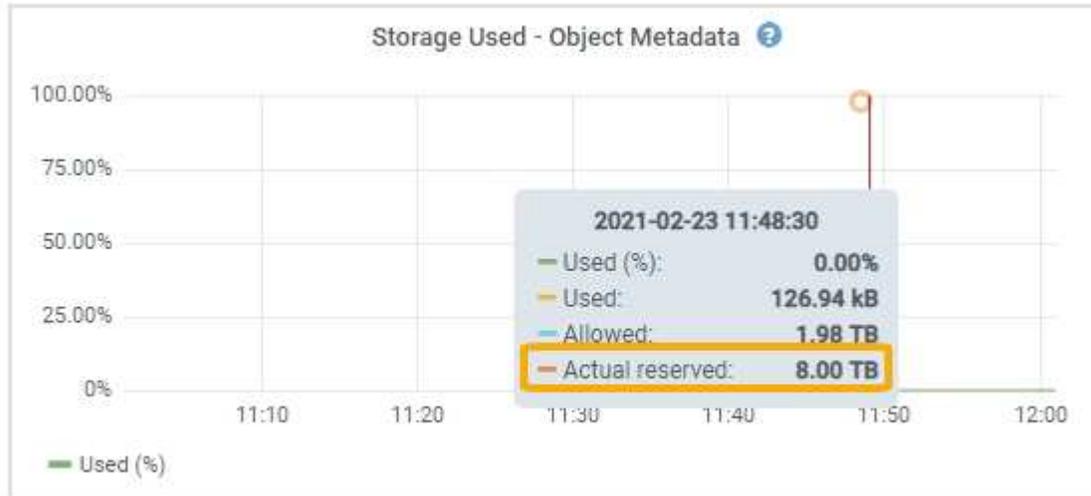
Zeigen Sie den tatsächlich reservierten Speicherplatz für Metadaten an

Führen Sie die folgenden Schritte aus, um den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Storage-Node anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **NODES > Storage Node** aus.
2. Wählen Sie die Registerkarte **Storage** aus.

3. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objekt Metadaten und suchen Sie den Wert **tatsächlich reserviert**.



Im Screenshot beträgt der **tatsächliche reservierte** Wert 8 TB. Dieser Screenshot ist für einen großen Speicherknoten in einer neuen StorageGRID 11.6 Installation. Da die Einstellung für den systemweiten reservierten Speicherplatz für Metadaten kleiner als das Volume 0 für diesen Storage-Node ist, entspricht der tatsächlich reservierte Speicherplatz für diesen Node der Einstellung für den reservierten Speicherplatz.

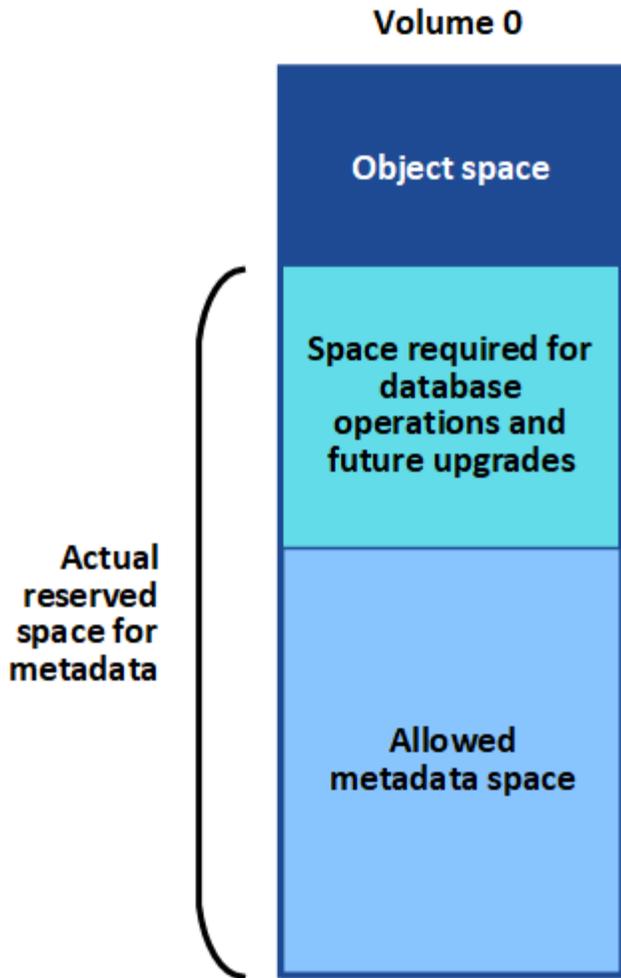
Beispiel für den tatsächlich reservierten Metadaten Speicherplatz

Angenommen, Sie installieren ein neues StorageGRID-System mit Version 11.7. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für eine neue StorageGRID 11.6-Installation oder höher, wenn jeder Speicherknoten mehr als 128 GB RAM hat.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)

Zulässiger Metadaten Speicherplatz

Der tatsächlich reservierte Speicherplatz jedes Storage-Node für Metadaten wird in den Speicherplatz für Objekt-Metadaten (den „*zulässigen Metadaten Speicherplatz*“) und den Platzbedarf für wichtige Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Updates unterteilt. Der zulässige Metadaten Speicherplatz bestimmt die gesamte Objektkapazität.



Die folgende Tabelle zeigt, wie StorageGRID den **zulässigen Metadaten Speicherplatz** für verschiedene Storage-Nodes berechnet, basierend auf der Speichermenge für den Node und dem tatsächlich reservierten Speicherplatz für Metadaten.

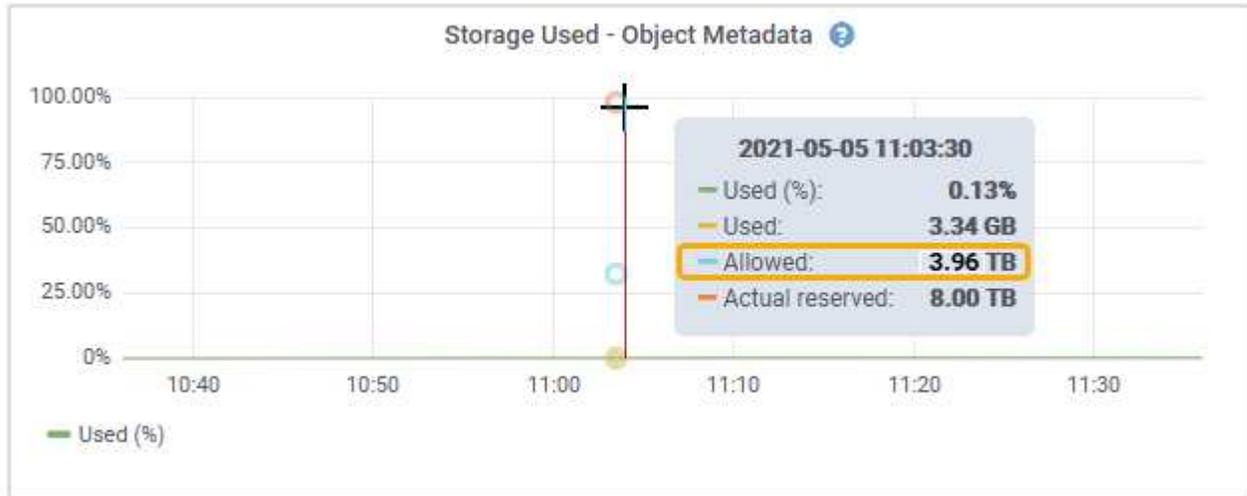
		Speichermenge auf Speicherknoten	
	< 128 GB	>= 128 GB	Tatsächlich reservierter Platz für Metadaten
<= 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.98 TB	4 TB

Zeigen Sie den zulässigen Metadatenbereich an

Führen Sie die folgenden Schritte aus, um den zulässigen Metadaten Speicher für einen Storage-Node anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie den Speicherknoten aus.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objekt Metadaten und suchen Sie den Wert **erlaubt**.



Im Screenshot beträgt der **zulässige**-Wert 3.96 TB, was der maximale Wert für einen Storage Node ist, dessen tatsächlicher reservierter Speicherplatz für Metadaten mehr als 4 TB beträgt.

Der **zulässige**-Wert entspricht dieser Prometheus-Metrik:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Beispiel für zulässigen Metadaten Speicherplatz

Angenommen, Sie installieren ein StorageGRID System mit Version 11.6. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für StorageGRID 11.6 oder höher, wenn jeder Speicher-Node mehr als 128 GB RAM hat.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)
- Der zulässige Speicherplatz für Metadaten auf SN1 beträgt 3 TB, basierend auf der im angegebenen Berechnung [Tabelle für zulässigem Speicherplatz für Metadaten](#): (Tatsächlich reservierter Platz für Metadaten – 1 TB) × 60%, bis zu einem Maximum von 3.96 TB.

Storage-Nodes unterschiedlicher Größen beeinflussen die Objektkapazität

Wie oben beschrieben, verteilt StorageGRID Objektmetadaten gleichmäßig über Storage-Nodes an jedem Standort. Wenn ein Standort Storage-Nodes unterschiedlicher Größen enthält, bestimmt der kleinste Node am Standort die Metadaten-Kapazität des Standorts.

Beispiel:

- Sie haben ein Raster mit drei Storage Nodes unterschiedlicher Größe an einem einzigen Standort.
- Die Einstellung **Metadaten reservierter Platz** beträgt 4 TB.
- Die Storage-Nodes haben die folgenden Werte für den tatsächlich reservierten Metadaten Speicherplatz und den zulässigen Metadaten Speicherplatz.

Storage-Node	Größe von Volumen 0	Tatsächlich reservierter Metadaten Speicherplatz	Zulässiger Metadaten Speicherplatz
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

Da Objektmetadaten gleichmäßig auf die Storage-Nodes an einem Standort verteilt werden, kann jeder Node in diesem Beispiel nur 1.32 TB Metadaten enthalten. Die zusätzlichen 0.66 TB an erlaubten Metadaten für SN2 und SN3 können nicht verwendet werden.



Da StorageGRID alle Objektmetadaten für ein StorageGRID System an jedem Standort speichert, wird die Gesamtkapazität der Metadaten eines StorageGRID Systems durch die Objektmetadaten des kleinsten Standorts bestimmt.

Und da die Objektmetadaten die maximale Objektanzahl steuern, wenn einem Node die Metadatenkapazität ausgeht, ist das Grid effektiv voll.

Verwandte Informationen

- Informationen zum Überwachen der Objektmetadatenkapazität für jeden Storage-Node finden Sie in den Anweisungen für ["Monitoring von StorageGRID"](#).
- Um die Objekt-Metadaten-Kapazität Ihres Systems zu erhöhen, ["Erweitern Sie Ihr Raster"](#) Durch Hinzufügen neuer Storage-Nodes.

Gespeicherte Objekte komprimieren

Sie können die Objektkomprimierung aktivieren, um die Größe der in StorageGRID gespeicherten Objekte zu reduzieren und so weniger Storage zu belegen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Standardmäßig ist die Objektkomprimierung deaktiviert. Wenn Sie die Komprimierung aktivieren, versucht StorageGRID beim Speichern jedes Objekts mithilfe einer verlustfreien Komprimierung zu komprimieren.



Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

Bevor Sie die Objektkomprimierung aktivieren, beachten Sie Folgendes:

- Sie sollten nicht **komprimieren gespeicherte Objekte** auswählen, es sei denn, Sie wissen, dass die gespeicherten Daten komprimierbar sind.
- Applikationen, die Objekte in StorageGRID speichern, komprimieren möglicherweise Objekte, bevor sie gespeichert werden. Wenn eine Client-Anwendung ein Objekt bereits komprimiert hat, bevor es in StorageGRID gespeichert wird, verringert die Auswahl dieser Option die Größe eines Objekts nicht weiter.
- Wählen Sie nicht **gespeicherte Objekte komprimieren** wenn Sie NetApp FabricPool mit StorageGRID verwenden.
- Wenn **compress Stored Objects** ausgewählt ist, sollten S3- und Swift-Client-Anwendungen die Ausführung VON GET Object-Operationen vermeiden, die einen Bereich von Bytes angeben, der zurückgegeben werden soll. Diese Vorgänge „range Read“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. VORGÄNGE ZUM ABRUFEN von Objekten, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.



Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Schritte

1. Wählen Sie **CONFIGURATION > System > Objektkomprimierung**.
2. Aktivieren Sie das Kontrollkästchen **gespeicherte Objekte komprimieren**.
3. Wählen Sie **Speichern**.

Konfigurationseinstellungen für Storage-Nodes

Jeder Speicher-Node verwendet mehrere Konfigurationseinstellungen und Zähler. Möglicherweise müssen Sie die aktuellen Einstellungen anzeigen oder Zähler zurücksetzen, um Alarme zu löschen (Legacy-System).



Mit Ausnahme der in der Dokumentation ausdrücklich enthaltenen Anweisungen sollten Sie sich mit dem technischen Support in Verbindung setzen, bevor Sie die Konfigurationseinstellungen für den Storage-Node ändern. Nach Bedarf können Sie Ereigniszähler zurücksetzen, um ältere Alarme zu löschen.

Führen Sie die folgenden Schritte aus, um auf die Konfigurationseinstellungen und -Zähler eines Storage Node zuzugreifen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **site > Storage Node** aus.
3. Erweitern Sie den Speicherknoten, und wählen Sie den Dienst oder die Komponente aus.
4. Wählen Sie die Registerkarte **Konfiguration**.

In den folgenden Tabellen sind die Konfigurationseinstellungen für Storage Node zusammengefasst.

LDR

Attributname	Codieren	Beschreibung
HTTP-Status	HSTE	Der aktuelle Status von HTTP für S3, Swift und anderen internen StorageGRID-Datenverkehr: <ul style="list-style-type: none">• Offline: Es sind keine Vorgänge zulässig. Jede Client-Anwendung, die versucht, eine HTTP-Sitzung für den LDR-Dienst zu öffnen, erhält eine Fehlermeldung. Aktive Sitzungen werden ordnungsgemäß geschlossen.• Online: Der Vorgang wird normal fortgesetzt
Automatisches Starten von HTTP	HTAS	<ul style="list-style-type: none">• Wenn diese Option ausgewählt ist, hängt der Zustand des Systems beim Neustart vom Status der Komponente LDR > Storage ab. Wenn die Komponente LDR > Storage beim Neustart schreibgeschützt ist, ist auch die HTTP-Schnittstelle schreibgeschützt. Wenn die Komponente LDR > Speicherung Online ist, ist HTTP auch Online. Andernfalls bleibt die HTTP-Schnittstelle im Status Offline.• Wenn diese Option nicht aktiviert ist, bleibt die HTTP-Schnittstelle offline, bis sie explizit aktiviert ist.

LDR > Datenspeicher

Attributname	Codieren	Beschreibung
Anzahl Verlorener Objekte Zurücksetzen	RCOR	Setzen Sie den Zähler für die Anzahl der verlorenen Objekte dieses Dienstes zurück.

LDR > Storage

Attributname	Codieren	Beschreibung
Storage-Zustand - Gewünscht	SSDS	<p>Eine vom Benutzer konfigurierbare Einstellung für den gewünschten Status der Speicherkomponente. Der LDR-Dienst liest diesen Wert und versucht, den durch dieses Attribut angegebenen Status zu entsprechen. Der Wert wird bei Neustarts dauerhaft verwendet.</p> <p>Mit dieser Einstellung können Sie beispielsweise dazu zwingen, dass Speicher schreibgeschützt wird, selbst wenn genügend Speicherplatz vorhanden ist. Dies kann bei der Fehlerbehebung hilfreich sein.</p> <p>Das Attribut kann einen der folgenden Werte annehmen:</p> <ul style="list-style-type: none"> • Offline: Wenn der gewünschte Status Offline ist, schaltet der LDR-Dienst die LDR > Storage-Komponente offline. • Schreibgeschützt: Wenn der gewünschte Status schreibgeschützt ist, verschiebt der LDR-Service den Speicherstatus auf schreibgeschützt und hört auf, neue Inhalte zu akzeptieren. Beachten Sie, dass Inhalte möglicherweise noch für kurze Zeit im Speicherknoten gespeichert werden, bis offene Sitzungen geschlossen sind. • Online: Den Wert bei Online während des normalen Systembetriebs belassen. Der Speicherstatus – der aktuelle Status der Speicherkomponente wird durch den Service dynamisch festgelegt, basierend auf dem Zustand des LDR-Service, z. B. der Menge des verfügbaren Objektspeicherspeichers. Wenn der Speicherplatz knapp ist, ist die Komponente schreibgeschützt.
Zeitüberschreitung Bei Der Integritätsprüfung	SHCT	<p>Die Zeitgrenze in Sekunden, innerhalb derer ein Integritätstest abgeschlossen werden muss, damit ein Speichervolumen als ordnungsgemäß angesehen wird. Ändern Sie diesen Wert nur, wenn Sie dazu vom Support aufgefordert werden.</p>

LDR > Verifizierung

Attributname	Codieren	Beschreibung
Fehlende Objekte Zurücksetzen Anzahl	VCMI	<p>Setzt die Anzahl der erkannten fehlenden Objekte zurück (OMIS). Nur nach Abschluss der Objektprüfung verwenden. Fehlende replizierte Objektdaten werden vom StorageGRID System automatisch wiederhergestellt.</p>

Attributname	Codieren	Beschreibung
Verifizierungsrate	VPRI	Legen Sie die Geschwindigkeit fest, mit der die Hintergrundüberprüfung durchgeführt wird. Weitere Informationen zur Konfiguration der Hintergrundüberprüfung finden Sie unter.
Anzahl Der Beschädigten Objekte Zurücksetzen	VCCR	Setzen Sie den Zähler für beschädigte, replizierte Objektdaten zurück, die während der Hintergrundüberprüfung gefunden wurden. Mit dieser Option können Sie den Alarmzustand der beschädigten Objekte löschen, die erkannt wurden (OCOR).
Objekte In Quarantäne Löschen	OQRT	<p>Löschen Sie beschädigte Objekte aus dem Quarantäneverzeichnis, setzen Sie die Anzahl der isolierten Objekte auf Null zurück und löschen Sie den Alarm „Quarantäne Objekte erkannt“ (OQRT). Diese Option wird verwendet, nachdem beschädigte Objekte vom StorageGRID-System automatisch wiederhergestellt wurden.</p> <p>Wenn ein Alarm „Lost Objects“ ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen. In manchen Fällen können isolierte Objekte für die Datenwiederherstellung oder das Debuggen der zugrunde liegenden Probleme, die die beschädigten Objektkopien verursacht haben, nützlich sein.</p>

LDR > Erasure Coding

Attributname	Codieren	Beschreibung
Zurücksetzen Der Fehleranzahl Für Schreibvorgänge	RWF.	Setzen Sie den Zähler auf Schreibfehler von Objektdaten mit Erasure-Coding-Verfahren auf den Storage-Node zurück.
Anzahl Der Fehlgeschlagene Lesevorgänge Zurücksetzen	RSRF	Setzen Sie den Zähler für Leseausfälle von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.
Zurücksetzen Löschen Fehleranzahl	RSDF	Setzen Sie den Zähler für Löscherfehler von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.
Beschädigte Kopien Erkannte Anzahl Zurücksetzen	RSCC	Setzen Sie den Zähler für die Anzahl beschädigter Kopien von Objektdaten, die nach dem Erasure-Coding-Verfahren codiert wurden, auf dem Storage-Node zurück.

Attributname	Codieren	Beschreibung
Beschädigte Fragmente Erkannte Anzahl Zurücksetzen	RCD	Setzen Sie den Zähler auf beschädigte Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage-Node zurück.
Fehlende Fragmente Erkannt Anzahl Zurücksetzen	RSMD	Setzen Sie den Zähler auf fehlende Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage Node zurück. Nur nach Abschluss der Objektprüfung verwenden.

LDR > Replikation

Attributname	Codieren	Beschreibung
Fehleranzahl Inbound Replication Zurücksetzen	RICR	Setzen Sie den Zähler auf Fehler bei eingehender Replikation zurück. Dies kann verwendet werden, um den RIRF-Alarm (Inbound Replication — failed) zu löschen.
Fehleranzahl Für Ausgehende Replikation Zurücksetzen	ROCR	Setzen Sie den Zähler auf Fehler bei ausgehenden Replikationen zurück. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
Deaktivieren Sie Inbound Replication	DSIR	<p>Wählen Sie diese Option aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.</p> <p>Wenn die eingehende Replikation deaktiviert ist, können Objekte vom Speicherknoten abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Objekte können jedoch nicht von anderen Speicherorten auf diesen Speicherknoten kopiert werden: Der LDR-Dienst ist schreibgeschützt.</p>
Deaktivieren Sie Ausgehende Replikation	DSOR	<p>Wählen Sie diese Option aus, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abrufvorgänge) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.</p> <p>Wenn die ausgehende Replikation deaktiviert ist, können Objekte auf diesen Speicherknoten kopiert werden. Objekte können jedoch nicht vom Speicherknoten abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Der LDR-Service ist schreibgeschützt.</p>

Management vollständiger Storage-Nodes

Wenn Storage-Nodes die Kapazität erreichen, müssen Sie das StorageGRID System durch Hinzufügen eines neuen Storage erweitern. Es sind drei Optionen verfügbar: Das Hinzufügen von Storage Volumes, das Hinzufügen von Shelves zur Storage-Erweiterung und das Hinzufügen von Storage-Nodes.

Hinzufügen von Storage-Volumes

Jeder Storage-Node unterstützt eine maximale Anzahl an Storage-Volumes. Der definierte Höchstwert variiert je nach Plattform. Wenn ein Storage-Node weniger als die maximale Anzahl an Storage-Volumes enthält, können Sie Volumes hinzufügen, um seine Kapazität zu erhöhen. Siehe Anweisungen für "[Erweitern eines StorageGRID Systems](#)".

Hinzufügen von Shelves zur Storage-Erweiterung

Einige Storage-Nodes von StorageGRID Appliances, z. B. SG6060, können zusätzliche Storage-Shelves unterstützen. Bei StorageGRID Appliances mit Erweiterungsfunktionen, die nicht bereits auf die maximale Kapazität erweitert wurden, können Sie Storage-Shelves zur Steigerung der Kapazität hinzufügen. Siehe Anweisungen für "[Erweitern eines StorageGRID Systems](#)".

Storage-Nodes Hinzufügen

Sie können die Storage-Kapazität durch Hinzufügen von Storage-Nodes erhöhen. Beim Hinzufügen von Storage müssen die aktuell aktiven ILM-Regeln und Kapazitätsanforderungen sorgfältig berücksichtigt werden. Siehe Anweisungen für "[Erweitern eines StorageGRID Systems](#)".

Managen Sie Admin-Nodes

Was ist ein Admin-Node?

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Jedes Grid muss einen primären Admin-Node haben und kann eine beliebige Anzahl nicht primärer Admin-Nodes für Redundanz aufweisen.

Wenn Sie sich beim Grid Manager oder dem Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID-Systems an. Wartungsverfahren müssen jedoch mit dem primären Admin-Node durchgeführt werden.

Admin-Nodes können auch verwendet werden, um den S3- und Swift-Client-Datenverkehr auszugleichen.

Was ist der bevorzugte Absender

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Nachrichten, SNMP-Traps und -Benachrichtigungen sowie ältere Alarmmeldungen.

Im normalen Systembetrieb sendet nur der bevorzugte Sender Benachrichtigungen. Alle anderen Admin-Knoten überwachen jedoch den bevorzugten Sender. Wenn ein Problem erkannt wird, fungieren andere Admin-Nodes als *Standby-Sender*.

In den folgenden Fällen können mehrere Benachrichtigungen gesendet werden:

- Wenn Admin-Knoten voneinander „islanded“ werden, versuchen sowohl der bevorzugte Sender als auch der Standby-Sender, Benachrichtigungen zu senden, und es können mehrere Kopien von Benachrichtigungen empfangen werden.
- Wenn der Standby-Sender Probleme mit dem bevorzugten Sender erkennt und mit dem Senden von Benachrichtigungen beginnt, kann der bevorzugte Sender möglicherweise wieder Benachrichtigungen senden. In diesem Fall können doppelte Benachrichtigungen gesendet werden. Der Standby-Sender hört auf, Benachrichtigungen zu senden, wenn Fehler auf dem bevorzugten Sender nicht mehr erkannt werden.



Wenn Sie AutoSupport-Meldungen testen, senden alle Administratorknoten die Test-E-Mail. Wenn Sie die Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Verbindung zu überprüfen.

Primäre Dienste für Admin-Nodes

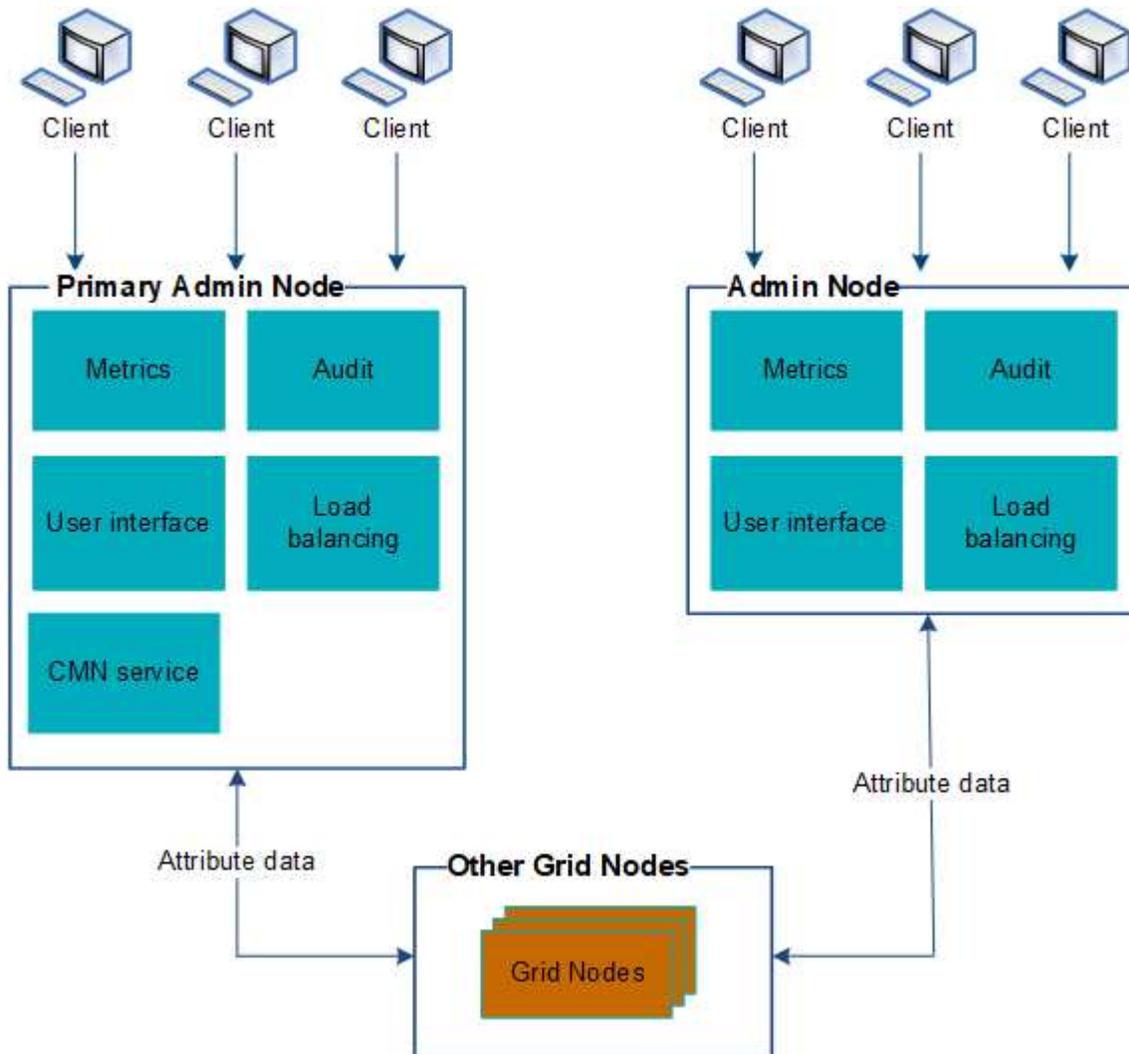
Die folgende Tabelle zeigt die primären Dienste für Admin-Nodes. Diese Tabelle enthält jedoch nicht alle Node-Services.

Service	Tastenfunktion
Audit Management System (AMS)	Verfolgt Systemaktivitäten und -Ereignisse.
Configuration Management Node (CMN)	Verwaltet die systemweite Konfiguration. Nur primärer Admin-Node.
Management-Applikations-Programmierschnittstelle (Management-API)	Verarbeitet Anforderungen aus der Grid-Management-API und der Mandantenmanagement-API.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. Hinweis: dieser Service befindet sich auch auf Gateway Nodes.
Lastausgleich	Sorgt für einen Lastenausgleich des S3- und Swift-Datenverkehrs von Clients zu Storage Nodes. Hinweis: dieser Service befindet sich auch auf Gateway Nodes.
Netzwerk-Management-System (NMS)	Bietet Funktionen für den Grid Manager.
Prometheus	Sammelt und speichert Zeitreihenmetriken von den Services auf allen Knoten.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Verwenden Sie mehrere Admin-Nodes

Ein StorageGRID-System kann mehrere Admin-Knoten enthalten, damit Sie Ihr StorageGRID-System kontinuierlich überwachen und konfigurieren können, auch wenn ein Admin-Knoten ausfällt.

Wenn ein Admin-Knoten nicht mehr verfügbar ist, wird die Attributverarbeitung fortgesetzt, Alarme und Alarme (Legacy-System) werden immer noch ausgelöst und E-Mail-Benachrichtigungen und AutoSupport-Meldungen werden weiterhin gesendet. Das Vorhandensein mehrerer Admin-Nodes bietet jedoch keinen Failover-Schutz außer Benachrichtigungen und AutoSupport-Meldungen. Insbesondere werden Alarmbestätigungen von einem Admin-Knoten nicht in andere Admin-Knoten kopiert.



Es gibt zwei Optionen, um das StorageGRID-System weiterhin anzuzeigen und zu konfigurieren, wenn ein Admin-Knoten ausfällt:

- Webclients können sich mit jedem anderen verfügbaren Admin-Node verbinden.
- Wenn ein Systemadministrator eine Hochverfügbarkeitsgruppe von Admin-Nodes konfiguriert hat, können Webclients unter Verwendung der virtuellen IP-Adresse der HA-Gruppe weiterhin auf den Grid Manager oder den Mandanten Manager zugreifen. Siehe "[Management von Hochverfügbarkeitsgruppen](#)".



Bei Verwendung einer HA-Gruppe wird der Zugriff unterbrochen, wenn der aktive Admin-Node ausfällt. Benutzer müssen sich erneut anmelden, nachdem die virtuelle IP-Adresse der HA-Gruppe auf einen anderen Admin-Node in der Gruppe Failover erfolgt.

Einige Wartungsarbeiten können nur mit dem primären Admin-Node ausgeführt werden. Wenn der primäre Admin-Node ausfällt, muss er wiederhergestellt werden, bevor das StorageGRID System wieder voll funktionsfähig ist.

Identifizieren Sie den primären Admin-Node

Der primäre Admin-Node hostet den CMN-Service. Einige Wartungsarbeiten können nur mit dem primären Admin-Node durchgeführt werden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Site > Admin-Node**, und wählen Sie dann aus  So erweitern Sie die Topologiestruktur und zeigen die auf diesem Admin-Node gehosteten Services an.

Der primäre Admin-Node hostet den CMN-Service.

3. Wenn dieser Admin-Node den CMN-Dienst nicht hostet, prüfen Sie die anderen Admin-Nodes.

Benachrichtigungsstatus und -Warteschlangen anzeigen

Der NMS-Dienst (Network Management System) auf Admin Nodes sendet Benachrichtigungen an den Mail-Server. Sie können den aktuellen Status des NMS-Dienstes und die Größe der Benachrichtigungswarteschlange auf der Seite Interface Engine anzeigen.

Um auf die Seite Interface Engine zuzugreifen, wählen Sie **SUPPORT > Tools > Grid-Topologie**. Wählen Sie schließlich **site > Admin Node > NMS > Interface Engine** aus.

Overview | Alarms | Reports | Configuration

Main

 **Overview: NMS (170-176) - Interface Engine**
 Updated: 2009-03-09 10:12:17 PDT

NMS Interface Engine Status:	Connected	 
Connected Services:	15	 

E-mail Notification Events

E-mail Notifications Status:	No Errors	 
E-mail Notifications Queued:	0	 

Database Connection Pool

Maximum Supported Capacity:	100	 
Remaining Capacity:	95 %	 
Active Connections:	5	 

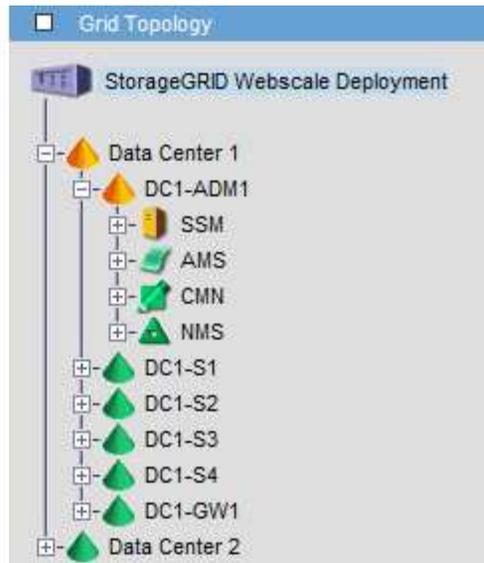
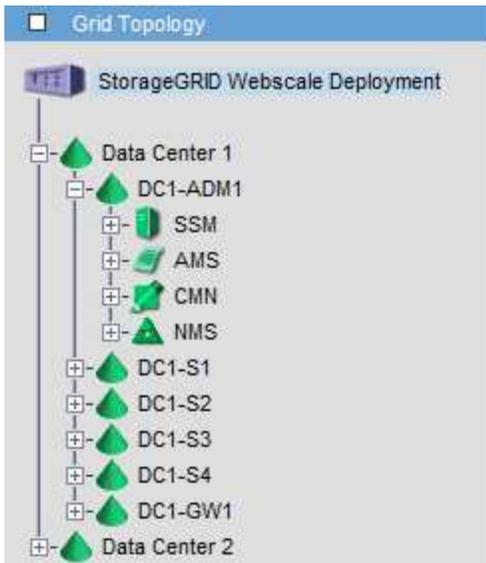
Benachrichtigungen werden über die E-Mail-Benachrichtigungswarteschlange verarbeitet und an den Mail-Server gesendet, einer nach dem anderen in der Reihenfolge, in der sie ausgelöst werden. Wenn ein Problem auftritt (z. B. ein Netzwerkverbindungsfehler) und der Mail-Server nicht verfügbar ist, wenn versucht wird, die Benachrichtigung zu senden, wird der Versuch unternommen, die Benachrichtigung an den Mailserver erneut zu senden, 60 Sekunden lang fortgesetzt. Wenn die Benachrichtigung nach 60 Sekunden nicht an den Mailserver gesendet wird, wird die Benachrichtigung aus der Benachrichtigungswarteschlange gelöscht und es wird versucht, die nächste Benachrichtigung in der Warteschlange zu senden.

Da Benachrichtigungen aus der Benachrichtigungswarteschlange gelöscht werden können, ohne gesendet zu werden, ist es möglich, dass ein Alarm ausgelöst werden kann, ohne dass eine Benachrichtigung gesendet wird. Wenn eine Benachrichtigung aus der Warteschlange gelöscht wird, ohne gesendet zu werden, wird der geringfügige ALARM MIN (E-Mail-Benachrichtigungsstatus) ausgelöst.

So zeigen Admin-Knoten bestätigte Alarmer an (Legacy-System)

Wenn Sie einen Alarm an einem Admin-Knoten bestätigen, wird der bestätigte Alarm nicht auf einen anderen Admin-Knoten kopiert. Da Bestätigungen nicht in andere Admin-Knoten kopiert werden, sieht die Struktur der Grid-Topologie für jeden Admin-Knoten möglicherweise nicht gleich aus.

Dieser Unterschied kann nützlich sein, wenn Web-Clients verbunden werden. Web-Clients können je nach Administratoranforderungen unterschiedliche Ansichten des StorageGRID-Systems haben.



Beachten Sie, dass Benachrichtigungen vom Admin-Knoten gesendet werden, wo die Bestätigung erfolgt.

Konfigurieren des Zugriffs auf Audit-Clients

Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS

Der Admin-Knoten protokolliert über den Service Audit Management System (AMS) alle überprüften Systemereignisse in eine Protokolldatei, die über die Revisionsfreigabe verfügbar ist und die zu jedem Admin-Knoten bei der Installation hinzugefügt wird. Die Revisionsfreigabe wird automatisch als schreibgeschützte Freigabe aktiviert.

Für den Zugriff auf Audit-Protokolle können Sie den Clientzugriff auf Audit-Freigaben für NFS konfigurieren. Sie können es auch ["Verwenden Sie einen externen Syslog-Server"](#).

Das StorageGRID System verwendet eine positive Bestätigung, um den Verlust von Audit-Meldungen zu verhindern, bevor sie in die Protokolldatei geschrieben werden. Eine Meldung bleibt an einem Dienst in der Warteschlange, bis der AMS-Dienst oder ein Zwischenaudit-Relaisdienst die Kontrolle über ihn bestätigt hat. Weitere Informationen finden Sie unter ["Prüfung von Audit-Protokollen"](#).

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

Über diese Aufgabe

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführten Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „verifiziert“ aufweisen. Geben Sie Ein: `storagegrid-status`

Wenn Services nicht als „aktiv“ oder „geprüft“ aufgeführt sind, beheben Sie Probleme, bevor Sie fortfahren.

3. Zurück zur Kommandozeile. Drücken Sie **Strg+C**.

4. Starten Sie das NFS-Konfigurationsprogramm. Geben Sie Ein: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share       | add-ip-to-share       | validate-config      |  
| enable-disable-share  | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

5. Fügen Sie den Audit-Client hinzu: `add-audit-share`

a. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: `client_IP_address`

b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

6. Wenn mehr als ein Audit-Client auf die Revisionsfreigabe zugreifen darf, fügen Sie die IP-Adresse des zusätzlichen Benutzers hinzu: `add-ip-to-share`

a. Geben Sie die Nummer der Revisionsfreigabe ein: `audit_share_number`

b. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: `client_IP_address`

c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

d. Wiederholen Sie diese Teilschritte für jeden zusätzlichen Audit-Client, der Zugriff auf die Revisionsfreigabe hat.

7. Überprüfen Sie optional Ihre Konfiguration.

a. Geben Sie Folgendes ein: `validate-config`

Die Dienste werden überprüft und angezeigt.

b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

c. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`

8. Legen Sie fest, ob die Revisionsfreigaben an anderen Standorten aktiviert werden müssen.

- Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.
- Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie die folgenden Audit-Freigaben nach Bedarf:
 - i. Remote-Anmeldung beim Admin-Node des Standorts:
 - A. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - B. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - C. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - D. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - ii. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden zusätzlichen Admin-Node zu konfigurieren.
 - iii. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node. Geben Sie Ein:
`exit`

9. Melden Sie sich aus der Befehlsshell ab: `exit`

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie der Freigabe ihre IP-Adresse hinzufügen oder einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie dessen IP-Adresse zur Revisionsfreigabe hinzufügen.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Passwort für das Root-/Administratorkonto.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

Schritte

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie das NFS-Konfigurationsprogramm: `config_nfs.rb`

Shares	Clients	Config
add-audit-share	add-ip-to-share	validate-config
enable-disable-share	remove-ip-from-share	refresh-config
		help
		exit

3. Geben Sie Ein: `add-ip-to-share`

Es wird eine Liste der auf dem Admin-Knoten aktivierten NFS-Audit-Freigaben angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer der Revisionsfreigabe ein: `audit_share_number`

5. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: `client_IP_address`

Der Audit-Client wird der Revisionsfreigabe hinzugefügt.

6. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

7. Wiederholen Sie die Schritte für jeden Audit-Client, der zur Revisionsfreigabe hinzugefügt werden soll.

8. Überprüfen Sie optional die Konfiguration: `validate-config`

Die Dienste werden überprüft und angezeigt.

a. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

9. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`

10. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie andernfalls optional diese Audit-Shares nach Bedarf:

a. Remote-Anmeldung beim Admin-Node eines Standorts:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden Admin-Knoten zu konfigurieren.

c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`

11. Melden Sie sich aus der Befehlsshell ab: `exit`

Prüfung der NFS-Audit-Integration

Nachdem Sie eine Audit-Freigabe konfiguriert und einen NFS-Audit-Client hinzugefügt haben, können Sie die Audit-Client-Freigabe mounten und überprüfen, ob die Dateien über die Audit-Freigabe verfügbar sind.

Schritte

1. Überprüfen Sie die Konnektivität (oder Variante für das Clientsystem) mithilfe der clientseitigen IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet. Geben Sie Ein: `ping IP_address`

Stellen Sie sicher, dass der Server antwortet, und geben Sie die Konnektivität an.

2. Mounten Sie die schreibgeschützte Revisionsfreigabe mit einem dem Client-Betriebssystem entsprechenden Befehl. Ein Beispiel für Linux lautet (geben Sie in einer Zeile ein):

```
mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export  
myAudit
```

Verwenden Sie die IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet, und den vordefinierten Freigabennamen für das Audit-System. Der Mount-Punkt kann ein beliebiger Name sein, der vom Client ausgewählt wurde (z. B. `myAudit` im vorherigen Befehl).

3. Stellen Sie sicher, dass die Dateien über die Revisionsfreigabe verfügbar sind. Geben Sie Ein: `ls myAudit /*`

Wo `myAudit` ist der Bereitstellungspunkt der Revisionsfreigabe. Es sollte mindestens eine Protokolldatei aufgeführt sein.

Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Sie können einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Passwort für das Root-/Administratorkonto.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).

Über diese Aufgabe

Sie können die letzte IP-Adresse, die für den Zugriff auf die Überwachungsfreigabe zulässig ist, nicht entfernen.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie das NFS-Konfigurationsprogramm: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share       | add-ip-to-share       | validate-config      |  
| enable-disable-share  | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

3. Entfernen Sie die IP-Adresse aus der Revisionsfreigabe: `remove-ip-from-share`

Eine nummerierte Liste der auf dem Server konfigurierten Audit-Freigaben wird angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer für die Revisionsfreigabe ein: `audit_share_number`

Eine nummerierte Liste mit IP-Adressen, die Zugriff auf die Revisionsfreigabe ermöglichen, wird angezeigt.

5. Geben Sie die Nummer für die IP-Adresse ein, die Sie entfernen möchten.

Die Revisionsfreigabe wird aktualisiert, und der Zugriff ist von keinem Audit-Client mit dieser IP-Adresse mehr gestattet.

6. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

7. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`

8. Wenn es sich bei Ihrer StorageGRID-Bereitstellung um mehrere Datacenter-Standortimplementierungen mit zusätzlichen Admin-Nodes an anderen Standorten handelt, deaktivieren Sie diese Revisionsfreigaben nach Bedarf:

a. Remote-Anmeldung bei jedem Standort Admin-Node:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden zusätzlichen Admin-Node zu konfigurieren.

c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`

9. Melden Sie sich aus der Befehlsshell ab: `exit`

Ändern der IP-Adresse eines NFS-Audit-Clients

Führen Sie diese Schritte aus, wenn Sie die IP-Adresse eines NFS-Audit-Clients ändern müssen.

Schritte

1. Fügen Sie einer vorhandenen NFS-Revisionsfreigabe eine neue IP-Adresse hinzu.
2. Entfernen Sie die ursprüngliche IP-Adresse.

Verwandte Informationen

- ["Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu"](#)
- ["Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe"](#)

Archiv-Nodes Managen

Was ist ein Archivknoten?

Optional kann jeder StorageGRID Datacenter-Standort mit einem Archiv-Node implementiert werden, sodass eine Verbindung zu einem externen Archiv-Storage-System wie Tivoli Storage Manager (TSM) hergestellt werden kann.

Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Siehe:



- ["Migrieren von Objekten in einen Cloud-Storage-Pool"](#)
- ["Verwendung Von Cloud Storage Pools"](#)

Darüber hinaus sollten Sie Archivknoten aus der aktiven ILM-Richtlinie in StorageGRID 11.7 oder früher entfernen. Das Entfernen von Objektdaten, die auf Archive Nodes gespeichert sind, vereinfacht zukünftige Upgrades. Siehe ["Arbeiten mit ILM-Regeln und ILM-Richtlinien"](#).

Der Archive Node bietet eine Schnittstelle, über die Sie ein externes Archiv-Storage-System zur langfristigen Speicherung von Objektdaten gezielt einsetzen können. Der Archivknoten überwacht darüber hinaus diese Verbindung und die Übertragung von Objektdaten zwischen dem StorageGRID System und dem angestrebten externen Archiv-Storage-System.

Nachdem Sie Verbindungen zum externen Ziel konfiguriert haben, können Sie den Archiv-Node so konfigurieren, dass die TSM-Performance optimiert wird, einen Archiv-Node offline schalten, wenn sich ein TSM-Server der Kapazität nähert oder nicht mehr verfügbar ist, und Einstellungen für Replikation und Abruf konfigurieren. Sie können auch benutzerdefinierte Alarme für den Knoten Archiv einstellen.

Objektdaten, auf die nicht gelöscht werden können, aber nicht regelmäßig zugegriffen wird, können jederzeit von den rotierenden Festplatten eines Storage-Nodes auf externen Archiv-Storage wie die Cloud oder auf Tapes verschoben werden. Diese Archivierung von Objektdaten erfolgt durch die Konfiguration des Archiv-Nodes eines Datacenter-Standorts und anschließend die Konfiguration von ILM-Regeln, bei denen dieser

Archivknoten als „Ziel“ für Anweisungen zur Content-Platzierung ausgewählt wird. Der Archivknoten verwaltet die archivierten Objektdaten nicht selbst; dies wird durch das externe Archivgerät erreicht.



Objektmetadaten werden nicht archiviert, bleiben aber auf Storage-Nodes erhalten.

Was der ARC-Service ist

Der ARC-Dienst (Archive Nodes) stellt die Managementoberfläche bereit, über die Sie Verbindungen zu externen Archivspeichern konfigurieren können, z. B. Bandmedien über TSM Middleware.

Der ARC-Service interagiert mit einem externen Archivspeichersystem, sendet Objektdaten für Nearline-Speicherung und führt Abrufvorgänge durch, wenn eine Client-Anwendung ein archiviertes Objekt anfordert. Wenn eine Client-Anwendung ein archiviertes Objekt anfordert, fordert ein Storage Node die Objektdaten vom ARC-Service an. Der ARC-Dienst stellt eine Anfrage an das externe Archiv-Speichersystem, das die angeforderten Objektdaten abrufen und diese an den ARC-Dienst sendet. Der ARC-Dienst überprüft die Objektdaten und leitet sie an den Speicherknoten weiter, der wiederum das Objekt an die anfordernde Client-Anwendung zurückgibt.

Anfragen nach über TSM Middleware auf Tape archivierten Objektdaten werden für eine effiziente Abrufvorgänge verwaltet. Anfragen können so bestellt werden, dass Objekte, die nacheinander auf Band gespeichert sind, in derselben sequenziellen Reihenfolge angefordert werden. Anforderungen werden dann in die Warteschlange gestellt, um sie an das Speichergerät zu übertragen. Je nach Archivgerät können mehrere Anfragen für Objekte auf verschiedenen Volumes gleichzeitig verarbeitet werden.

Archivierung in der Cloud über die S3-API

Ein Archivierungs-Node kann so konfiguriert werden, dass er eine direkte Verbindung zu Amazon Web Services (AWS) oder einem anderen System herstellt, das über die S3-API mit dem StorageGRID-System verbunden werden kann.



Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Siehe "[Verwendung Von Cloud Storage Pools](#)".

Konfigurieren Sie die Verbindungseinstellungen für die S3-API

Wenn Sie über die S3-Schnittstelle eine Verbindung zu einem Archiv-Node herstellen, müssen Sie die Verbindungseinstellungen für die S3-API konfigurieren. Bis diese Einstellungen konfiguriert sind, bleibt der ARC-Dienst in einem wichtigen Alarmzustand, da er nicht mit dem externen Archivspeichersystem kommunizieren kann.



Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

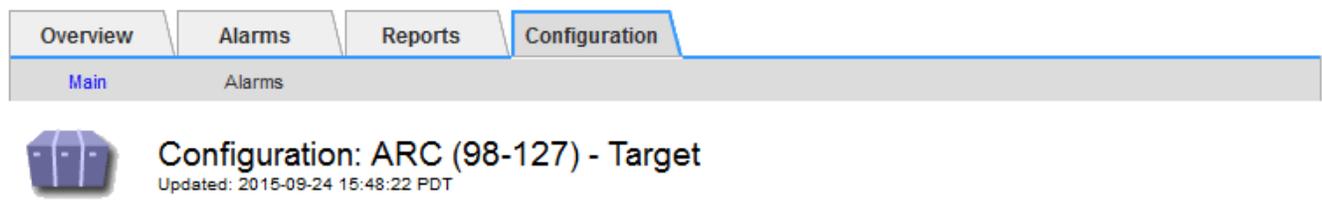
Siehe "[Verwendung Von Cloud Storage Pools](#)".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben auf dem Ziel-Archiv-Storage-System einen Bucket erstellt:
 - Der Bucket ist einem einzelnen Archiv-Node zugewiesen. Sie kann nicht von anderen Archivierungs-Knoten oder anderen Anwendungen verwendet werden.
 - Der Bucket hat die für Ihren Standort ausgewählte Region.
 - Der Bucket sollte mit der Versionierung als ausgesetzt konfiguriert werden.
- Objektsegmentierung ist aktiviert, und die maximale Segmentgröße beträgt weniger als oder gleich 4.5 gib (4,831,838,208 Byte). S3-API-Anfragen, die diesen Wert überschreiten, schlagen fehl, wenn S3 als externes Archiv-Storage-System verwendet wird.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Ziel**.
3. Wählen Sie **Konfiguration > Main**.



Target Type:

Cloud Tiering (S3) Account

Bucket Name:	<input type="text" value="name"/>
Region:	<input type="text" value="Virginia or Pacific Northwest (us-east-1)"/>
Endpoint:	<input type="text" value="https://10.10.10.123:8082"/> <input type="checkbox"/> Use AWS
Endpoint Authentication:	<input type="checkbox"/>
Access Key:	<input type="text" value="ABCD123EFG45AB"/>
Secret Access Key:	<input type="text" value="•••••"/>
Storage Class:	<input type="text" value="Standard (Default)"/>

Apply Changes

4. Wählen Sie in der Dropdown-Liste Zieltyp * Cloud Tiering - Simple Storage Service (S3)* aus.



Konfigurationseinstellungen sind erst verfügbar, wenn Sie einen Zieltyp auswählen.

5. Konfigurieren Sie das Cloud-Tiering-Konto (S3), über das der Archive-Node eine Verbindung zum externen S3-fähigen Archiv-Storage-System herstellen soll.

Die meisten Felder auf dieser Seite sind selbsterklärend. Im folgenden werden die Felder beschrieben, für die Sie möglicherweise Hinweise benötigen.

- **Region:** Nur verfügbar, wenn **AWS verwenden** ausgewählt ist. Die ausgewählte Region muss mit der Region des Buckets übereinstimmen.
- **Endpunkt** und **AWS verwenden:** Für Amazon Web Services (AWS) wählen Sie **AWS verwenden**. **Endpunkt** wird dann automatisch mit einer Endpunkt-URL auf der Grundlage der Attribute Bucket-Name und Region ausgefüllt. Beispiel:

```
https://bucket.region.amazonaws.com
```

Geben Sie bei einem nicht von AWS stammenden Ziel die URL des Systems ein, das den Bucket hostet, einschließlich der Portnummer. Beispiel:

```
https://system.com:1080
```

- **Endpunktauthentifizierung:** Standardmäßig aktiviert. Wenn das Netzwerk zum externen Archivspeichersystem vertrauenswürdig ist, können Sie das Kontrollkästchen deaktivieren, um die Überprüfung von SSL-Zertifikaten und Hostnamen für das Zielspeichersystem für die externe Archivierung zu deaktivieren. Wenn eine andere Instanz eines StorageGRID-Systems das Archiv-Zielspeichergerät ist und das System mit öffentlich signierten Zertifikaten konfiguriert ist, können Sie das Kontrollkästchen aktivieren.
- **Speicherklasse:** Wählen Sie **Standard (Standard)** für die normale Lagerung. Wählen Sie **reduzierte Redundanz** nur für Objekte, die einfach neu erstellt werden können. **Reduzierte Redundanz** bietet kostengünstige Speicherung mit weniger Zuverlässigkeit. Wenn das zielgerichtete Archivspeichersystem eine weitere Instanz des StorageGRID-Systems ist, steuert **Speicherklasse**, wie viele Zwischenkopien des Objekts bei der Aufnahme auf das Zielsystem erstellt werden, wenn bei Aufnahme von Objekten Dual Commit verwendet wird.

6. Wählen Sie **Änderungen Anwenden**.

Die angegebenen Konfigurationseinstellungen werden validiert und auf Ihr StorageGRID System angewendet. Nach der Konfiguration kann das Ziel nicht mehr geändert werden.

Ändern der Verbindungseinstellungen für die S3-API

Nachdem der Archivknoten über die S3 API für die Verbindung zu einem externen Archiv-Storage-System konfiguriert wurde, können Sie einige Einstellungen ändern, wenn sich die Verbindung ändert.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Sie das Cloud Tiering (S3) Konto ändern, müssen Sie sicherstellen, dass die Anmeldedaten für Benutzerzugriff auch auf den Bucket Lese-/Schreibzugriff haben, einschließlich aller Objekte, die zuvor vom Archiv-Node in den Bucket aufgenommen wurden.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.

2. Wählen Sie **Archivknoten** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.

Target Type: Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name: name

Region: Virginia or Pacific Northwest (us-east-1)

Endpoint: https://10.10.10.123:8082 Use AWS

Endpoint Authentication:

Access Key: ABCD123EFG45AB

Secret Access Key: ●●●●●●

Storage Class: Standard (Default)

Apply Changes

4. Ändern Sie ggf. die Kontoinformationen.

Wenn Sie die Storage-Klasse ändern, werden neue Objektdaten mit der neuen Storage-Klasse gespeichert. Vorhandene Objekte werden bei der Aufnahme weiterhin unter dem Storage-Klassensatz gespeichert.



Bucket-Name, Region und Endpunkt: Verwenden Sie AWS-Werte und können nicht geändert werden.

5. Wählen Sie **Änderungen Anwenden**.

Ändern Sie den Status des Cloud Tiering Service

Sie können die Lese- und Schreibvorgänge des Archiv-Nodes auf das externe Archiv-Storage-System steuern, das über die S3 API verbunden ist, indem Sie den Status des Cloud Tiering Service ändern.

Bevor Sie beginnen

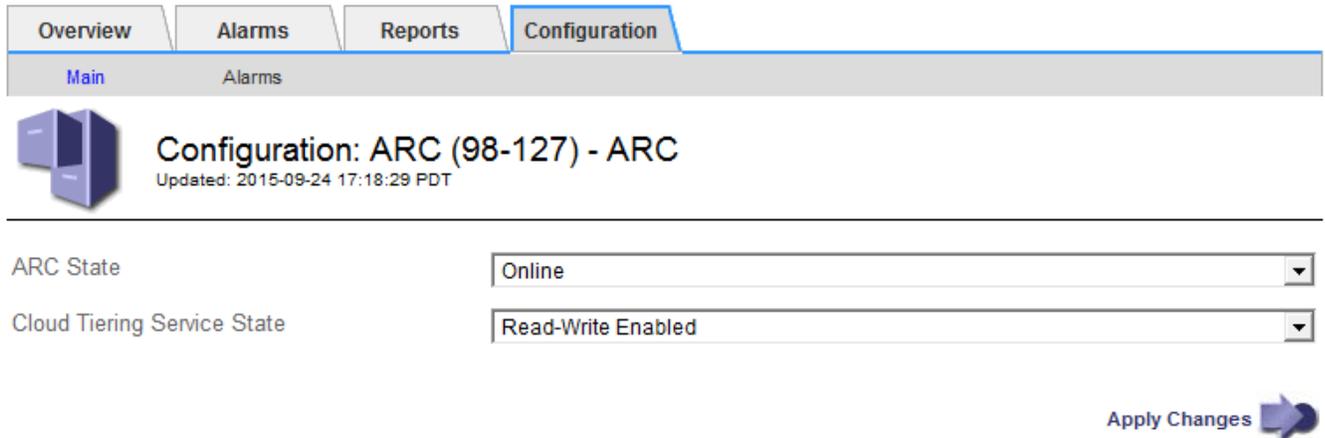
- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der Archivknoten muss konfiguriert sein.

Über diese Aufgabe

Sie können den Archiv-Knoten effektiv offline setzen, indem Sie den Cloud-Tiering-Servicezustand in **Lesen-Schreiben deaktiviert** ändern.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC** aus.
3. Wählen Sie **Konfiguration > Main**.



Overview Alarms Reports Configuration

Main Alarms

 Configuration: ARC (98-127) - ARC
Updated: 2015-09-24 17:18:29 PDT

ARC State

Cloud Tiering Service State

Apply Changes 

4. Wählen Sie einen **Cloud Tiering Service-Status** aus.
5. Wählen Sie **Änderungen Anwenden**.

Zurücksetzen der Speicherfehler-Anzahl für S3-API-Verbindung

Wenn Ihr Archiv-Node über die S3-API eine Verbindung zu einem Archivspeichersystem herstellt, können Sie die Anzahl der Speicherfehler zurücksetzen, die zum Löschen des ARVF-Alarms (Store Failures) verwendet werden kann.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Store** aus.
3. Wählen Sie **Konfiguration > Main**.

Overview | Alarms | Reports | **Configuration**

Main | Alarms

 **Configuration: ARC (98-127) - Store**
Updated: 2015-09-29 17:54:42 PDT

Reset Store Failure Count

Apply Changes 

4. Wählen Sie **Anzahl Der Fehler Im Store Zurücksetzen** Aus.
5. Wählen Sie **Änderungen Anwenden**.

Das Attribut Fehler speichern wird auf Null zurückgesetzt.

Migrieren Sie Objekte von Cloud Tiering – S3 zu einem Cloud-Storage-Pool

Wenn Sie derzeit die Funktion **Cloud Tiering - Simple Storage Service (S3)** verwenden, um Objektdaten in einen S3-Bucket zu verschieben, sollten Sie stattdessen Ihre Objekte in einen Cloud-Storage-Pool migrieren. Cloud Storage Pools bieten einen skalierbaren Ansatz, der alle Storage-Nodes in Ihrem StorageGRID System nutzt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben bereits Objekte im S3-Bucket gespeichert, der für Cloud Tiering konfiguriert ist.



Vor der Migration von Objektdaten sollten Sie den NetApp Ansprechpartner kontaktieren, um die damit verbundenen Kosten zu verstehen und zu managen.

Über diese Aufgabe

Aus einer ILM-Perspektive ähnelt ein Cloud-Storage-Pool einem Storage-Pool. Während Storage-Pools jedoch aus Storage-Nodes oder Archiv-Nodes innerhalb des StorageGRID Systems bestehen, besteht ein Cloud Storage-Pool aus einem externen S3-Bucket.

Vor der Migration von Objekten aus Cloud Tiering – S3 zu einem Cloud-Storage-Pool müssen Sie zuerst einen S3-Bucket erstellen und dann den Cloud-Storage-Pool in StorageGRID erstellen. Dann können Sie eine neue ILM-Richtlinie erstellen und die ILM-Regel ersetzen, die zum Speichern von Objekten im Cloud Tiering Bucket verwendet wird, durch eine geklonte ILM-Regel, die dieselben Objekte im Cloud-Storage-Pool speichert.



Wenn Objekte in einem Cloud-Storage-Pool gespeichert sind, können Kopien dieser Objekte nicht auch in StorageGRID gespeichert werden. Wenn die ILM-Regel, die Sie derzeit für Cloud Tiering verwenden, so konfiguriert ist, um Objekte an mehreren Standorten gleichzeitig zu speichern, sollten Sie bedenken, ob Sie diese optionale Migration dennoch durchführen möchten, da diese Funktion verloren geht. Wenn Sie mit dieser Migration fortfahren, müssen Sie neue Regeln erstellen, anstatt die vorhandenen zu klonen.

Schritte

1. Erstellen Sie einen Cloud-Storage-Pool.

Verwenden Sie einen neuen S3-Bucket für den Cloud-Storage-Pool, um sicherzustellen, dass er nur die Daten enthält, die vom Cloud-Storage-Pool gemanagt werden.

2. Suchen Sie alle ILM-Regeln der aktiven ILM-Richtlinie, die dazu führen, dass Objekte im Cloud Tiering Bucket gespeichert werden.
3. Jede dieser Regeln klonen.
4. Ändern Sie in den geklonten Regeln den Speicherort in den neuen Cloud-Storage-Pool.
5. Speichern Sie die geklonten Regeln.
6. Erstellen Sie eine neue Richtlinie, die die neuen Regeln verwendet.
7. Simulieren und aktivieren Sie die neue Richtlinie.

Wenn die neue Richtlinie aktiviert ist und eine ILM-Bewertung erfolgt, werden die Objekte vom für Cloud Tiering konfigurierten S3-Bucket in den für den Cloud-Storage-Pool konfigurierten S3-Bucket verschoben. Der nutzbare Speicherplatz im Raster ist nicht betroffen. Nachdem die Objekte in den Cloud Storage Pool verschoben wurden, werden sie aus dem Cloud Tiering Bucket entfernt.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

Archivierung auf Band über TSM Middleware

Sie können einen Archiv-Node so konfigurieren, dass er als Ziel für einen Tivoli Storage Manager (TSM)-Server dient, der eine logische Schnittstelle zum Speichern und Abrufen von Objektdaten an Random- oder Sequential-Access-Speichergeräten, einschließlich Tape Libraries, bereitstellt.

Der ARC-Service des Archivknotens fungiert als Client zum TSM-Server und verwendet Tivoli Storage Manager als Middleware zur Kommunikation mit dem Archivspeichersystem.



Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Siehe ["Verwendung Von Cloud Storage Pools"](#).

TSM Management-Klassen

Durch die TSM Middleware definierte Managementklassen beschreiben, wie die TSM's Backup- und Archivierungsvorgänge funktionieren und können verwendet werden, um Regeln für Inhalte festzulegen, die vom TSM-Server angewendet werden. Diese Regeln laufen unabhängig von der ILM-Richtlinie des StorageGRID Systems und müssen im Einklang mit der Anforderung des StorageGRID Systems stehen, dass Objekte dauerhaft gespeichert und für den Abruf durch den Archivierungs-Node immer verfügbar sind. Nachdem die Objektdaten vom Archiv-Node an einen TSM-Server gesendet wurden, werden die Regeln für den TSM Lebenszyklus und die Aufbewahrung angewendet, während die Objektdaten auf dem vom TSM-Server verwalteten Band gespeichert werden.

Die TSM-Managementklasse wird vom TSM-Server verwendet, um Regeln für den Datenspeicherort oder die

Aufbewahrung anzuwenden, nachdem Objekte vom Archiv-Node an den TSM-Server gesendet wurden. So können beispielsweise als Datenbank-Backups identifizierte Objekte (temporärer Content, der mit neueren Daten überschrieben werden kann) anders behandelt werden als Applikationsdaten (unveränderlicher Inhalt, der unendlich lange aufbewahrt werden muss).

Konfigurieren Sie Verbindungen zur TSM Middleware

Bevor der Archive Node mit der Tivoli Storage Manager (TSM) Middleware kommunizieren kann, müssen Sie mehrere Einstellungen konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Bis diese Einstellungen konfiguriert sind, bleibt der ARC-Dienst in einem wichtigen Alarmzustand, da er nicht mit dem Tivoli Storage Manager kommunizieren kann.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Ziel** aus.
3. Wählen Sie **Konfiguration > Main**.

The screenshot shows the configuration page for an ARC target in the TSM console. The navigation tabs at the top are Overview, Alarms, Reports, and Configuration. The sub-navigation shows Main and Alarms. The main heading is "Configuration: ARC (DC1-ARC1-98-165) - Target" with a timestamp "Updated: 2015-09-28 09:56:36 PDT". Below this, there are two dropdown menus: "Target Type" set to "Tivoli Storage Manager (TSM)" and "Tivoli Storage Manager State" set to "Online". A section titled "Target (TSM) Account" contains several input fields: "Server IP or Hostname" (10.10.10.123), "Server Port" (1500), "Node Name" (ARC-USER), "User Name" (arc-user), "Password" (masked with dots), "Management Class" (sg-mgmtclass), "Number of Sessions" (2), "Maximum Retrieve Sessions" (1), and "Maximum Store Sessions" (1). At the bottom right, there is an "Apply Changes" button with a right-pointing arrow.

4. Wählen Sie aus der Dropdown-Liste **Zieltyp** die Option **Tivoli Storage Manager (TSM)** aus.

5. Wählen Sie für den **Tivoli Storage Manager State Offline** aus, um Rückrufe vom TSM Middleware-Server zu verhindern.

Standardmäßig ist der Status von Tivoli Storage Manager auf Online eingestellt, was bedeutet, dass der Archive Node Objektdaten vom TSM Middleware-Server abrufen kann.

6. Geben Sie die folgenden Informationen an:

- **Server IP oder Hostname:** Geben Sie die IP-Adresse oder den vollqualifizierten Domännennamen des TSM Middleware-Servers an, der vom ARC-Dienst verwendet wird. Die Standard-IP-Adresse ist 127.0.0.1.
- **Server-Port:** Geben Sie die Portnummer auf dem TSM Middleware-Server an, mit dem der ARC-Dienst eine Verbindung herstellen wird. Der Standardwert ist 1500.
- **Knotenname:** Geben Sie den Namen des Archiv-Knotens an. Sie müssen den Namen (Arc-user) eingeben, den Sie auf dem TSM Middleware-Server registriert haben.
- **Benutzername:** Geben Sie den Benutzernamen an, den der ARC-Dienst zur Anmeldung am TSM-Server verwendet. Geben Sie den Standardbenutzernamen (Arc-user) oder den administrativen Benutzer ein, den Sie für den Archiv-Node angegeben haben.
- **Passwort:** Geben Sie das Passwort an, das der ARC-Dienst zur Anmeldung am TSM-Server verwendet.
- **Managementklasse:** Geben Sie die Standardverwaltungsklasse an, die verwendet werden soll, wenn beim Speichern des Objekts auf dem StorageGRID-System keine Managementklasse angegeben ist oder die angegebene Managementklasse nicht auf dem TSM Middleware-Server definiert ist.
- **Anzahl der Sitzungen:** Geben Sie die Anzahl der Bandlaufwerke auf dem TSM Middleware-Server an, die dem Archiv-Knoten gewidmet sind. Der Archivknoten erstellt gleichzeitig maximal eine Sitzung pro Bereitstellungspunkt plus eine kleine Anzahl zusätzlicher Sitzungen (weniger als fünf).

Sie müssen diesen Wert ändern, um den für MAXNUMMP festgelegten Wert (maximale Anzahl von Mount-Punkten) zu erhalten, wenn der Archivknoten registriert oder aktualisiert wurde. (Im Register-Befehl ist der Standardwert von MAXNUMMP verwendet 1, wenn kein Wert festgelegt ist.)

Außerdem müssen Sie den Wert von MAXSESSIONS für den TSM-Server auf eine Zahl ändern, die mindestens so groß ist wie die Anzahl der Sitzungen, die für den ARC-Dienst festgelegt wurden. Der Standardwert von MAXSESSIONS auf dem TSM-Server ist 25.

- **Maximum Retrieve Sessions:** Geben Sie die maximale Anzahl von Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Abrufvorgänge öffnen kann. In den meisten Fällen ist der entsprechende Wert die Anzahl der Sitzungen abzüglich der maximalen Speichersitzungen. Wenn Sie ein Bandlaufwerk für die Speicherung und den Abruf freigeben möchten, geben Sie einen Wert an, der der Anzahl der Sitzungen entspricht.
- **Maximum Store Sessions:** Geben Sie die maximale Anzahl gleichzeitiger Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Archivierungsvorgänge öffnen kann.

Dieser Wert sollte auf eins gesetzt werden, außer wenn das gezielte Archivspeichersystem voll ist und nur Abrufvorgänge durchgeführt werden können. Setzen Sie diesen Wert auf Null, um alle Sitzungen für Abrufvorgänge zu verwenden.

7. Wählen Sie **Änderungen Anwenden**.

Optimieren Sie einen Archiv-Node für TSM Middleware-Sitzungen

Sie können die Performance eines Archivierungs-Knotens, der sich mit Tivoli Server Manager (TSM) verbindet, optimieren, indem Sie die Sitzungen des Archivierungs-Nodes konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

In der Regel ist die Anzahl der gleichzeitigen Sitzungen, die der Archivknoten für den TSM Middleware-Server offen hat, auf die Anzahl der Bandlaufwerke eingestellt, die der TSM-Server dem Archiv-Node zugewiesen hat. Ein Bandlaufwerk wird für den Speicher zugewiesen, während der Rest für den Abruf zugewiesen wird. Wenn jedoch ein Speicherknoten aus Archive Node Kopien neu aufgebaut wird oder der Archivknoten im schreibgeschützten Modus arbeitet, können Sie die TSM-Serverleistung optimieren, indem Sie die maximale Anzahl der Abrufsitzungen so einstellen, dass sie mit der Anzahl der gleichzeitigen Sitzungen identisch sind. Das Ergebnis ist, dass alle Laufwerke gleichzeitig für den Abruf genutzt werden können. Höchstens kann eines dieser Laufwerke zur Lagerung verwendet werden.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Ziel** aus.
3. Wählen Sie **Konfiguration > Main**.
4. Ändern Sie **Maximum Retrieve Sessions** als **Anzahl der Sitzungen**.

Overview	Alarms	Reports	Configuration
Main	Alarms		



Configuration: ARC (DC1-ARC1-98-165) - Target

Updated: 2015-09-28 09:56:36 PDT

Target Type:

Tivoli Storage Manager State:

Target (TSM) Account

Server IP or Hostname:	<input type="text" value="10.10.10.123"/>
Server Port:	<input type="text" value="1500"/>
Node Name:	<input type="text" value="ARC-USER"/>
User Name:	<input type="text" value="arc-user"/>
Password:	<input type="password" value="•••••"/>
Management Class:	<input type="text" value="sg-mgmtclass"/>
Number of Sessions:	<input type="text" value="2"/>
Maximum Retrieve Sessions:	<input type="text" value="2"/>
Maximum Store Sessions:	<input type="text" value="1"/>

[Apply Changes](#) 

5. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie den Archivierungsstatus und die Zähler für TSM

Wenn der Archivknoten eine Verbindung zu einem TSM Middleware-Server herstellt, können Sie den Status des Archivspeichers eines Archiv-Knotens in Online oder Offline konfigurieren. Sie können den Archivspeicher auch deaktivieren, wenn der Archivknoten zum ersten Mal gestartet wird, oder die Fehleranzahl, die für den zugehörigen Alarm nachverfolgt wird, zurücksetzen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Store** aus.
3. Wählen Sie **Konfiguration > Main**.

Overview Alarms Reports **Configuration**

Main Alarms

 **Configuration: ARC (DC1-ARC1-98-165) - Store**
Updated: 2015-09-29 17:10:12 PDT

Store State

Archive Store Disabled on Startup

Reset Store Failure Count

Apply Changes 

4. Ändern Sie bei Bedarf die folgenden Einstellungen:

- Speicherstatus: Legen Sie den Komponentenstatus auf entweder:
 - Online: Der Archiv-Node ist zur Verarbeitung von Objektdaten zum Speichern im Archiv-Storage-System verfügbar.
 - Offline: Der Archiv-Node ist nicht verfügbar, um Objektdaten zum Speichern im Archiv-Storage-System zu verarbeiten.
- Archivspeicher beim Start deaktiviert: Wenn diese Option ausgewählt ist, bleibt die Komponente Archivspeicher beim Neustart im schreibgeschützten Zustand. Wird verwendet, um Speicher dauerhaft für das Zielspeichersystem zu deaktivieren. Nützlich, wenn das ausgewählte Archivspeichersystem keine Inhalte akzeptieren kann.
- Reset Store Failure Count: Setzt den Zähler für Store Failures zurück. Dies kann verwendet werden, um den ARVF-Alarm (Stores Failure) zu löschen.

5. Wählen Sie **Änderungen Anwenden**.

Verwandte Informationen

["Verwalten Sie einen Archiv-Node, wenn der TSM-Server die Kapazität erreicht"](#)

Verwalten Sie einen Archiv-Node, wenn der TSM-Server die Kapazität erreicht

Der TSM-Server hat keine Möglichkeit, den Archiv-Node zu benachrichtigen, wenn sich die Kapazität der TSM-Datenbank oder des vom TSM-Server verwalteten Archivmedienspeichers befindet. Dies kann durch proaktive Überwachung des TSM-Servers vermieden werden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Der Archivknoten akzeptiert weiterhin Objektdaten für die Übertragung an den TSM-Server, nachdem der TSM-Server keine neuen Inhalte mehr akzeptiert. Dieser Inhalt kann nicht auf Medien geschrieben werden, die vom TSM-Server verwaltet werden. In diesem Fall wird ein Alarm ausgelöst.

Verhindern, dass der ARC-Dienst Inhalte an den TSM-Server sendet

Um zu verhindern, dass der ARC-Service weitere Inhalte an den TSM-Server sendet, können Sie den Archiv-Node offline schalten, indem Sie die **ARC > Store**-Komponente offline schalten. Dieses Verfahren kann auch nützlich sein, um Alarime zu vermeiden, wenn der TSM-Server nicht zur Wartung verfügbar ist.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Store** aus.
3. Wählen Sie **Konfiguration > Main**.



4. Ändern Sie **Store State** in *Offline*.
5. Wählen Sie * Archivspeicher beim Start deaktiviert* aus.
6. Wählen Sie **Änderungen Anwenden**.

Stellen Sie Archive Node auf „Read-Only“ ein, wenn die TSM Middleware die Kapazität erreicht

Wenn der angestrebte TSM Middleware-Server seine Kapazität erreicht, kann der Archivknoten optimiert werden, um nur die Abrufvorgänge durchzuführen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Ziel** aus.
3. Wählen Sie **Konfiguration > Main**.
4. Ändern Sie die maximale Anzahl der Abruf-Sitzungen auf dieselbe Weise wie die Anzahl der gleichzeitigen Sitzungen, die in der Anzahl der Sitzungen aufgeführt sind.
5. Ändern Sie die maximale Anzahl von Sitzungen im Store auf 0.



Das Ändern der maximalen Speichersitzungen auf 0 ist nicht erforderlich, wenn der Archivknoten schreibgeschützt ist. Speichersitzungen werden nicht erstellt.

6. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie die Einstellungen für den Abruf von Archivknoten

Sie können die Einstellungen für den Abruf eines Archiv-Knotens so konfigurieren, dass

der Status auf Online oder Offline gesetzt wird, oder die Fehleranzahl, die für die zugehörigen Alarme nachverfolgt wird, zurücksetzen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Abruf**.
3. Wählen Sie **Konfiguration > Main**.

Overview Alarms Reports Configuration

Main Alarms

Configuration: ARC (DC1-ARC1-98-165) - Retrieve
Updated: 2015-05-07 12:24:45 PDT

Retrieve State

Reset Request Failure Count

Reset Verification Failure Count

Apply Changes

4. Ändern Sie bei Bedarf die folgenden Einstellungen:
 - **Retrieve Status:** Den Komponentenzustand auf entweder einstellen:
 - Online: Der Grid-Node ist verfügbar, um Objektdaten vom Archivierungsmedium abzurufen.
 - Offline: Der Grid-Node ist zum Abrufen von Objektdaten nicht verfügbar.
 - Anzahl der fehlgeschlagenen Anfragen zurücksetzen: Aktivieren Sie das Kontrollkästchen, um den Zähler für Anforderungsfehler zurückzusetzen. Dieser kann verwendet werden, um den ARRF-Alarm (Request Failures) zu löschen.
 - Anzahl der fehlgeschlagenen Verifizierungen zurücksetzen: Aktivieren Sie das Kontrollkästchen, um den Zähler für Überprüfungsfehler bei abgerufenen Objektdaten zurückzusetzen. Dies kann verwendet werden, um den ARRV-Alarm (Verifizierungsfehler) zu löschen.
5. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie die Replikation des Archivierungs-Knotens

Sie können die Replikationseinstellungen für einen Archivknoten konfigurieren und die ein- und ausgehende Replikation deaktivieren oder die für die zugehörigen Alarme zu protokollierenden Fehlerzählungen zurücksetzen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Replikation** aus.
3. Wählen Sie **Konfiguration > Main**.

Configuration: ARC (DC1-ARC1-98-165) - Replication
Updated: 2015-05-07 12:21:53 PDT

Reset Inbound Replication Failure Count

Reset Outbound Replication Failure Count

Inbound Replication

Disable Inbound Replication

Outbound Replication

Disable Outbound Replication

Apply Changes

4. Ändern Sie bei Bedarf die folgenden Einstellungen:
 - **Fehleranzahl Inbound Replication zurücksetzen:** Wählen Sie, um den Zähler für eingehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RIRF-Alarm (eingehende Replikationen — fehlgeschlagen) zu löschen.
 - **Fehleranzahl bei ausgehenden Replikationsfehlern zurücksetzen:** Wählen Sie, um den Zähler für ausgehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
 - **Inbound Replication deaktivieren:** Wählen Sie aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs löschen lassen.

Wenn die eingehende Replikation deaktiviert ist, können Objektdaten vom ARC-Dienst zur Replikation an andere Standorte im StorageGRID-System abgerufen werden. Objekte können jedoch nicht von anderen Systemstandorten auf diesen ARC-Dienst repliziert werden. Der ARC-Dienst wird-only gelesen.

- **Ausgehende Replikation deaktivieren:** Aktivieren Sie das Kontrollkästchen, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abfragen) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.

Wenn die ausgehende Replikation deaktiviert ist, können Objektdaten zu diesem ARC-Dienst kopiert werden, um ILM-Regeln zu erfüllen. Objektdaten können jedoch nicht vom ARC-Dienst abgerufen werden, um an andere Orte im StorageGRID-System kopiert zu werden. Der ARC-Dienst ist nur schreiben-.

5. Wählen Sie **Änderungen Anwenden**.

Legen Sie benutzerdefinierte Alarme für den Knoten Archiv fest

Sie sollten benutzerdefinierte Alarme für die ARQL- und ARRL-Attribute einrichten, die zur Überwachung der Geschwindigkeit und Effizienz des Datenabrufs von Objektdaten vom Archivspeichersystem durch den Knoten Archiv verwendet werden.

- ARQL: Durchschnittliche Warteschlangenlänge. Die durchschnittliche Zeit in Mikrosekunden dieser Objektdaten wird zum Abruf aus dem Archivspeichersystem in die Warteschlange verschoben.
- ARRL: Durchschnittliche Anfragelatenz. Die durchschnittliche Zeit in Mikrosekunden, die der Archive-Node benötigt, um Objektdaten aus dem Archiv-Storage-System abzurufen.

Die akzeptablen Werte dieser Attribute hängen davon ab, wie das Archivspeichersystem konfiguriert und verwendet wird. (Gehen Sie zu **ARC > Abrufen > Übersicht > Haupt.**) Die Werte, die für die Timeouts von Anfragen festgelegt sind, und die Anzahl der Sitzungen, die für Abrufanfragen zur Verfügung gestellt werden, haben einen besonderen Einfluss.

Nach Abschluss der Integration überwachen Sie die Abfrage der Objektdaten des Archivknoten, um Werte für die normalen Abrufzeiten und Warteschlangenlänge zu ermitteln. Erstellen Sie dann benutzerdefinierte Alarme für ARQL und ARRL, die ausgelöst werden, wenn eine anormale Betriebsbedingung auftritt. Siehe Anweisungen für "[Verwalten von Alarmen \(Altsystem\)](#)".

Integration Von Tivoli Storage Manager

Konfiguration und Betrieb des Archivierungs-Node

Ihr StorageGRID-System managt den Archiv-Node als Speicherort, an dem Objekte unendlich gespeichert werden und stets zugänglich sind.

Bei der Aufnahme eines Objekts werden auf Basis der für das StorageGRID System definierten Regeln für das Information Lifecycle Management Kopien an allen erforderlichen Speicherorten, einschließlich Archiv-Nodes, erstellt. Der Archivknoten fungiert als Client auf einem TSM-Server, und die TSM-Clientbibliotheken sind auf dem Archiv-Knoten durch den Installationsvorgang der StorageGRID-Software installiert. Objektdaten, die zum Archiv-Node für Speicher geleitet werden, werden beim Empfang direkt auf dem TSM-Server gespeichert. Der Archivknoten stellt keine Objektdaten vor dem Speichern auf dem TSM-Server dar und führt auch keine Objekttaggregation durch. Der Archivknoten kann jedoch in einer einzigen Transaktion mehrere Kopien an den TSM-Server senden, wenn die Datenraten dies erfordern.

Nachdem der Archivknoten Objektdaten auf dem TSM-Server speichert, werden die Objektdaten unter Anwendung der Lifecycle-/Aufbewahrungsrichtlinien vom TSM-Server gemanagt. Diese Aufbewahrungsrichtlinien müssen definiert werden, damit sie mit dem Vorgang des Archivierungs-Nodes kompatibel sind. Das bedeutet, dass vom Archiv-Node gespeicherte Objektdaten unbegrenzt gespeichert werden müssen und vom Archiv-Node immer darauf zugegriffen werden muss, es sei denn, sie werden vom Archiv-Node gelöscht.

Es besteht keine Verbindung zwischen den ILM-Regeln des StorageGRID Systems und den Lifecycle-/Aufbewahrungsrichtlinien des TSM Servers. Jeder arbeitet unabhängig voneinander. Wenn jedoch jedes Objekt in das StorageGRID System aufgenommen wird, kann ihm eine TSM Management-Klasse zugewiesen werden. Diese Managementklasse wird gemeinsam mit Objektdaten an den TSM Server übergeben. Durch das Zuweisen verschiedener Managementklassen zu unterschiedlichen Objekttypen können Sie den TSM-Server so konfigurieren, dass Objektdaten in verschiedenen Storage-Pools gespeichert werden, oder unterschiedliche Migrations- oder Aufbewahrungsrichtlinien anwenden. Beispielsweise können als Datenbank-Backups identifizierte Objekte (temporärer Content als mit neueren Daten überschrieben werden kann) anders als Applikationsdaten behandelt werden (unveränderlicher Inhalt, der für unbegrenzte Zeit aufbewahrt werden

muss).

Der Archivknoten kann in einen neuen oder vorhandenen TSM-Server integriert werden; es ist kein dedizierter TSM-Server erforderlich. TSM-Server können mit anderen Clients gemeinsam genutzt werden, vorausgesetzt, der TSM-Server ist für die erwartete maximale Last angemessen dimensioniert. TSM muss auf einem vom Archiv-Node getrennten Server oder einer virtuellen Maschine installiert sein.

Es ist möglich, mehr als einen Archivknoten zu konfigurieren, um auf denselben TSM-Server zu schreiben; diese Konfiguration wird jedoch nur empfohlen, wenn die Archiv-Knoten unterschiedliche Datensätze auf den TSM-Server schreiben. Die Konfiguration von mehr als einem Archiv-Node zum Schreiben auf denselben TSM-Server wird nicht empfohlen, wenn jeder Archiv-Node Kopien derselben Objektdaten in das Archiv schreibt. Bei einem letzteren Szenario unterliegen beide Kopien einem Single Point of Failure (dem TSM-Server), da sie unabhängige, redundante Kopien von Objektdaten sind.

Archive Nodes verwenden die hierarchische Speicherverwaltung (HSM)-Komponente von TSM nicht.

Best Practices für die Konfiguration

Wenn Sie den TSM-Server dimensionieren und konfigurieren, gibt es Best Practices, die Sie anwenden sollten, um ihn für die Arbeit mit dem Archiv-Knoten zu optimieren.

Bei der Dimensionierung und Konfiguration des TSM-Servers sollten folgende Faktoren berücksichtigt werden:

- Da der Archivknoten keine Objekte aggregiert, bevor sie auf dem TSM-Server gespeichert werden, muss die TSM-Datenbank so dimensioniert sein, dass sie Verweise auf alle Objekte enthält, die auf den Archiv-Node geschrieben werden.
- Archive Node-Software kann die Latenz beim Schreiben von Objekten direkt auf Band oder andere Wechselmedien nicht tolerieren. Daher muss der TSM-Server mit einem Festplatten-Speicherpool für den ursprünglichen Speicher der Daten konfiguriert werden, die vom Archiv-Node gespeichert werden, wenn Wechseldatenträger verwendet werden.
- Sie müssen TSM-Aufbewahrungsrichtlinien konfigurieren, um die ereignisbasierte Aufbewahrung zu verwenden-. Der Archivierungs-Node unterstützt keine auf der Erstellung basierenden TSM-Aufbewahrungsrichtlinien. Verwenden Sie in der Aufbewahrungsrichtlinie die folgenden empfohlenen Einstellungen von `remin=0` und `rever=0` (dies bedeutet, dass die Aufbewahrung beginnt, wenn der Archivknoten ein Archivierungsereignis auslöst und danach 0 Tage lang aufbewahrt wird). Diese Werte für `Remin` und `Rever` sind jedoch optional.

Der Laufwerk-Pool muss so konfiguriert sein, dass Daten in den Bandpool migriert werden (das heißt, der Bandpool muss `NXTSTGPOOL` des Laufwerk-Pools sein). Der Bandpool darf nicht als Kopierpool des Laufwerkspools konfiguriert werden, der gleichzeitig in beide Pools schreibt (d. h. der Bandpool kann kein `COPYSTGPOOL` für den Laufwerkspool sein). Um Offline-Kopien der Bänder zu erstellen, die Daten von Archivierungs-Nodes enthalten, konfigurieren Sie den TSM-Server mit einem zweiten Bandpool, der ein Kopie-Pool des für Archiv-Node-Daten verwendeten Bandpools ist.

Schließen Sie die Konfiguration des Archivierungs-Knotens ab

Der Archivknoten funktioniert nicht, nachdem Sie den Installationsprozess abgeschlossen haben. Bevor das StorageGRID-System Objekte auf dem TSM-Archivknoten speichern kann, müssen Sie die Installation und Konfiguration des TSM-Servers abschließen und den Archivknoten für die Kommunikation mit dem TSM-Server konfigurieren.

Beachten Sie bei Bedarf die folgende IBM-Dokumentation, wenn Sie Ihren TSM-Server für die Integration mit dem Archiv-Node in einem StorageGRID-System vorbereiten:

- ["IBM Bandgerätetreiber – Installations- und Benutzerhandbuch"](#)
- ["Programmierreferenz für IBM Bandgerätetreiber"](#)

Installieren Sie einen neuen TSM-Server

Sie können den Archiv-Knoten entweder mit einem neuen oder einem vorhandenen TSM-Server integrieren. Wenn Sie einen neuen TSM-Server installieren, befolgen Sie die Anweisungen in der TSM-Dokumentation, um die Installation abzuschließen.



Ein Archive Node kann nicht mit einem TSM-Server gemeinsam gehostet werden.

Konfigurieren Sie den TSM-Server

Dieser Abschnitt enthält Beispielanweisungen zur Vorbereitung eines TSM-Servers gemäß den Best Practices von TSM.

Die folgenden Anweisungen führen Sie durch den Prozess von:

- Definieren eines Festplatten-Speicherpools und eines Bandspeicherpools (falls erforderlich) auf dem TSM-Server
- Definieren einer Domänenrichtlinie, die die TSM-Managementklasse für die Daten verwendet, die im Knoten Archiv gespeichert sind, und Registrieren eines Knotens für diese Domänenrichtlinie

Diese Anweisungen dienen nur zu Ihrer Orientierung; sie sind nicht als Ersatz für die TSM-Dokumentation gedacht oder als vollständige und umfassende Anweisungen, die für alle Konfigurationen geeignet sind. Eine Anleitung zur Implementierung sollte von einem TSM-Administrator bereitgestellt werden, der sowohl mit Ihren detaillierten Anforderungen als auch mit dem vollständigen Satz der TSM-Server-Dokumentation vertraut ist.

Definieren Sie TSM Tape- und Festplatten-Storage-Pools

Der Archivknoten schreibt in einen Festplatten-Speicherpool. Um Inhalte auf Band zu archivieren, müssen Sie den Festplatten-Speicherpool konfigurieren, um Inhalte in einen Bandspeicher-Pool zu verschieben.

Über diese Aufgabe

Bei einem TSM-Server müssen Sie einen Bandspeicher-Pool und einen Festplatten-Speicherpool in Tivoli Storage Manager definieren. Erstellen Sie nach Definition des Laufwerk-Pools ein Laufwerk-Volume und weisen Sie es dem Laufwerk-Pool zu. Ein Bandpool nicht erforderlich, wenn Ihr TSM-Server nur Festplatten-Storage verwendet.

Sie müssen mehrere Schritte auf dem TSM-Server durchführen, bevor Sie einen Bandspeicherpool erstellen können. (Erstellen Sie eine Bandbibliothek und mindestens ein Laufwerk in der Bandbibliothek. Definieren Sie einen Pfad vom Server zur Bibliothek und vom Server zu den Laufwerken und definieren Sie dann eine Geräteklasse für die Laufwerke.) Die Details dieser Schritte können je nach Hardwarekonfiguration und Storage-Anforderungen des Standorts variieren. Weitere Informationen finden Sie in der TSM-Dokumentation.

Die folgenden Anweisungen veranschaulichen den Prozess. Sie sollten beachten, dass die Anforderungen an Ihren Standort je nach Bereitstellungsanforderungen unterschiedlich sein können. Weitere Informationen zur Konfiguration und zu Anweisungen finden Sie in der TSM-Dokumentation.



Sie müssen sich beim Server mit Administratorrechten anmelden und das `dsmadm`-Tool verwenden, um die folgenden Befehle auszuführen.

Schritte

1. Erstellen einer Tape Library

```
define library tapelibrary libtype=scsi
```

Wo *tapelibrary* ist ein willkürlicher Name, der für die Bandbibliothek und den Wert von ausgewählt wurde *libtype*. Je nach Art der Tape Library kann es variieren.

2. Definieren Sie einen Pfad vom Server zur Bandbibliothek.

```
define path servername tapelibrary srctype=server desttype=library device=lib-devicename
```

- *servername* ist der Name des TSM-Servers
- *tapelibrary* ist der von Ihnen definierte Bandbibliothek
- *lib-devicename* ist der Gerätenamen für die Bandbibliothek

3. Legen Sie ein Laufwerk für die Bibliothek fest.

```
define drive tapelibrary drivename
```

- *drivename* ist der Name, den Sie für das Laufwerk angeben möchten
- *tapelibrary* ist der von Ihnen definierte Bandbibliothek

Je nach Hardwarekonfiguration möchten Sie möglicherweise ein zusätzliches Laufwerk oder weitere Laufwerke konfigurieren. (Wenn beispielsweise der TSM-Server mit einem Fibre Channel-Switch verbunden ist, der über zwei Eingaben aus einer Bandbibliothek verfügt, sollten Sie für jede Eingabe möglicherweise ein Laufwerk definieren.)

4. Definieren Sie einen Pfad vom Server zum Laufwerk, das Sie definiert haben.

```
define path servername drivename srctype=server desttype=drive  
library=tapelibrary device=drive-dname
```

- *drive-dname* ist der Gerätenamen für das Laufwerk
- *tapelibrary* ist der von Ihnen definierte Bandbibliothek

Wiederholen Sie diesen Vorgang für jedes Laufwerk, das Sie für die Bandbibliothek definiert haben, mit einem separaten Laufwerk *drivename* Und *drive-dname* Für jedes Laufwerk.

5. Definieren Sie eine Geräteklasse für die Laufwerke.

```
define devclass DeviceClassName devtype=lto library=tapelibrary  
format=tapetype
```

- *DeviceClassName* ist der Name der Geräteklasse
- *lto* ist der Laufwerkstyp, der mit dem Server verbunden ist

◦ *tapelibrary* Ist der von Ihnen definierte Bandbibliothek

◦ *tapetype* Ist der Tape-Typ, z. B. ultrium3

6. Fügen Sie dem Bestand der Bibliothek Bandvolumen hinzu.

```
checkin libvolume tapelibrary
```

tapelibrary Ist der von Ihnen definierte Bandbibliothek.

7. Erstellen Sie den primären Bandspeicherpool.

```
define stgpool SGWSTapePool DeviceClassName description=description  
collocate=filespace maxscratch=XX
```

- *SGWSTapePool* Ist der Name des Bandspeicherpools des Archiv-Nodes. Sie können einen beliebigen Namen für den Bandspeicher-Pool auswählen (sofern der Name die vom TSM-Server erwarteten Syntaxkonventionen verwendet).
- *DeviceClassName* Ist der Name des Klassennamens für die Bandbibliothek.
- *description* Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „Bandspeicher-Pool für den Archiv-Node“
- *collocate=filespace* Gibt an, dass der TSM-Server Objekte aus demselben Dateispeicher auf ein einzelnes Band schreiben soll.
- *XX* Ist eine der folgenden Optionen:
 - Die Anzahl der leeren Bänder in der Bandbibliothek (falls der Archivknoten die einzige Anwendung ist, die die Bibliothek verwendet).
 - Die Anzahl der vom StorageGRID System zugewiesenen Tapes (in Fällen, in denen die Tape-Bibliothek gemeinsam genutzt wird).

8. Erstellen Sie auf einem TSM-Server einen Festplatten-Speicherpool. Geben Sie an der Administrationskonsole des TSM-Servers ein

```
define stgpool SGWSDiskPool disk description=description  
maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high  
lowmig=percent_low
```

- *SGWSDiskPool* Ist der Name des Festplatten-Pools des Archiv-Nodes. Sie können einen beliebigen Namen für den Festplatten-Speicherpool auswählen (sofern der Name die vom TSM erwarteten Syntaxkonventionen verwendet).
- *description* Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „Festplatten-Storage-Pool für den Archiv-Node“
- *maximum_file_size* Zwingt das Schreiben von Objekten, die größer sind als diese Größe, direkt auf Tape, statt im Festplatten-Pool gespeichert zu werden. Es wird empfohlen, die Einstellung festzulegen *maximum_file_size* Bis 10 GB.
- *nextstgpool=SGWSTapePool* Bezeichnet den Festplatten-Speicherpool auf den für den Archiv-Node definierten Bandspeicher-Pool.
- *percent_high* Legt den Wert fest, mit dem der Laufwerk-Pool seine Inhalte in den Bandpool migriert.

Es wird empfohlen, die Einstellung festzulegen *percent_high* Zu 0, sodass sofort die Datenmigration beginnt

- *percent_low* Legt den Wert fest, mit dem die Migration zum Bandpool angehalten wird. Es wird empfohlen, die Einstellung festzulegen *percent_low* Zu 0, um den Laufwerk-Pool zu löschen.

9. Erstellen Sie auf einem TSM-Server ein Festplatten-Volume (oder Volumes) und weisen Sie es dem Festplatten-Pool zu.

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* Ist der Name des Disk-Pools.
- *volume_name* Ist der vollständige Pfad zum Speicherort des Volumes (z. B. */var/local/arc/stage6.dsm*) Auf dem TSM-Server, wo er den Inhalt des Laufwerk-Pools in Vorbereitung für die Übertragung auf Band schreibt.
- *size* Ist die Größe des Datenträgers in MB.

Wenn Sie beispielsweise ein einzelnes Laufwerk-Volume so erstellen möchten, dass der Inhalt eines Festplattenpools ein einzelnes Band enthält, setzen Sie den Wert der Größe auf 200000, wenn das Bandvolumen 200 GB hat.

Es könnte jedoch wünschenswert sein, mehrere Festplatten-Volumes einer kleineren Größe zu erstellen, da der TSM-Server auf jedes Volume im Festplatten-Pool schreiben kann. Wenn die Bandgröße beispielsweise 250 GB beträgt, erstellen Sie 25 Festplatten-Volumes mit jeweils 10 GB (10000).

Der TSM-Server weist im Verzeichnis für das Festplatten-Volume vorab Speicherplatz zu. Dies kann einige Zeit in Anspruch nehmen (mehr als drei Stunden für ein 200-GB-Laufwerk).

Definieren Sie eine Domänenrichtlinie und registrieren Sie einen Knoten

Sie müssen eine Domänenrichtlinie definieren, die die TSM-Managementklasse für die Daten verwendet, die vom Archiv-Node gespeichert wurden, und dann einen Knoten registrieren, um diese Domänenrichtlinie zu verwenden.



Archive Node-Prozesse können Speicher auslaufen, wenn das Clientpasswort für den Archive Node im Tivoli Storage Manager (TSM) abläuft. Stellen Sie sicher, dass der TSM-Server so konfiguriert ist, dass der Client-Benutzername/das Passwort für den Archiv-Node nie abläuft.

Wenn Sie einen Knoten auf dem TSM-Server für die Verwendung des Archiv-Knotens registrieren (oder einen vorhandenen Knoten aktualisieren), müssen Sie die Anzahl der Mount-Punkte angeben, die der Knoten für Schreibvorgänge verwenden kann, indem Sie den MAXNUMMP-Parameter für den BEFEHL REGISTER NODE angeben. Die Anzahl der Bereitstellungspunkte entspricht in der Regel der Anzahl der Bandlaufwerksköpfe, die dem Archiv-Node zugewiesen sind. Die für MAXNUMMP auf dem TSM-Server angegebene Zahl muss mindestens so groß sein wie der für den **ARC > Ziel > Konfiguration > Haupt > maximale Store Sessions** für den Archive Node festgelegte Wert, Der auf den Wert 0 oder 1 gesetzt ist, da gleichzeitige Speichersitzungen vom Archive Node nicht unterstützt werden.

Der Wert des MAXSESSIONS-Satzes für den TSM-Server steuert die maximale Anzahl von Sitzungen, die für den TSM-Server von allen Client-Anwendungen geöffnet werden können. Der auf dem TSM angegebene MAXSESSIONS-Wert muss mindestens so groß sein wie der für **ARC > Ziel > Konfiguration > Main > Anzahl Sitzungen** im Grid Manager für den Archiv-Node angegebene Wert. Der Archivknoten erstellt gleichzeitig höchstens eine Sitzung pro Bereitstellungspunkt plus eine kleine Zahl (< 5) zusätzlicher Sitzungen.

Der dem Archiv-Node zugewiesene TSM-Node verwendet eine benutzerdefinierte Domänenrichtlinie `tsm-domain`. Die Domänenrichtlinie ist eine geänderte Version der Domänenrichtlinie „standard“, die auf Band geschrieben und als Speicherpool des StorageGRID Systems das Archivziel festgelegt wurde (`SGWSDiskPool`).



Sie müssen sich am TSM-Server mit Administratorrechten anmelden und das `dsmadm`-Tool verwenden, um die Domänenrichtlinie zu erstellen und zu aktivieren.

Erstellen und aktivieren Sie die Domänenrichtlinie

Sie müssen eine Domänenrichtlinie erstellen und diese dann aktivieren, um den TSM-Server so zu konfigurieren, dass die vom Archiv-Node gesendeten Daten gespeichert werden.

Schritte

1. Eine Domänenrichtlinie erstellen.

```
copy domain standard tsm-domain
```

2. Wenn Sie keine vorhandene Management-Klasse verwenden, geben Sie eine der folgenden Optionen ein:

```
define policyset tsm-domain standard
```

```
define mgmtclass tsm-domain standard default
```

default ist die Standard-Managementklasse für die Bereitstellung.

3. Erstellen Sie eine Copygroup in den entsprechenden Speicherpool. Geben Sie (in einer Zeile) ein:

```
define copygroup tsm-domain standard default type=archive  
destination=SGWSDiskPool retinit=event retmin=0 retver=0
```

default ist die Standard-Managementklasse für den Archivknoten. Die Werte von `retinit`, `retmin`, und `retver` wurden ausgewählt, um das Aufbewahrungsverhalten wiederzugeben, das derzeit vom Archiv-Knoten verwendet wird



Nicht einstellen `retinit` Bis `retinit=create`. Einstellung `retinit=create` blockiert das Löschen von Inhalten durch den Archivknoten, da Aufbewahrungseignisse zum Entfernen von Inhalten vom TSM-Server verwendet werden.

4. Weisen Sie die Managementklasse als Standard zu.

```
assign defmgmtclass tsm-domain standard default
```

5. Legen Sie den neuen Richtlinienatz als aktiv fest.

```
activate policyset tsm-domain standard
```

Ignorieren Sie die Warnung „no Backup copy Group“, die beim Eingeben des Befehls `activate` angezeigt wird.

6. Registrieren Sie einen Knoten, um den neuen Richtlinienatz auf dem TSM-Server zu verwenden. Geben Sie auf dem TSM-Server (in einer Zeile) Folgendes ein:

```
register node arc-user arc-password passexp=0 domain=tsm-domain  
MAXNUMMP=number-of-sessions
```

Arc-user und Arc-password sind der Name und das Kennwort des Client-Knotens, den Sie auf dem Archiv-Node definieren, und der Wert von MAXNUMMP ist auf die Anzahl der Bandlaufwerke festgelegt, die für Archive Node Store-Sessions reserviert sind.



Durch die Registrierung eines Knotens wird standardmäßig eine Administrator-Benutzer-ID mit der Berechtigung des Clienteigentümers erstellt, wobei das für den Knoten definierte Passwort angegeben ist.

Datenmigration zu StorageGRID

Sie können große Datenmengen bei gleichzeitigem Einsatz des StorageGRID Systems auf das StorageGRID System migrieren.

Verwenden Sie diesen Leitfaden, wenn Sie eine Migration großer Datenmengen in das StorageGRID System planen. Sie ist kein allgemeiner Leitfaden für die Datenmigration und enthält keine detaillierten Schritte zur Durchführung einer Migration. Befolgen Sie die Richtlinien und Anweisungen in diesem Abschnitt, um sicherzustellen, dass Daten effizient in das StorageGRID System migriert werden, ohne den täglichen Betrieb zu beeinträchtigen und dass die migrierten Daten vom StorageGRID System entsprechend gehandhabt werden.

Bestätigen Sie die Kapazität des StorageGRID Systems

Bevor Sie große Datenmengen in das StorageGRID System migrieren, vergewissern Sie sich, dass das StorageGRID System über die Festplattenkapazität verfügt, um das erwartete Volume zu verwalten.

Wenn das StorageGRID-System einen Archivknoten enthält und eine Kopie der migrierten Objekte im Nearline-Speicher (z. B. Band) gespeichert wurde, stellen Sie sicher, dass der Speicher des Archivknotens über genügend Kapazität für das erwartete Volumen der migrierten Daten verfügt.

Sehen Sie sich als Teil der Kapazitätsbewertung das Datenprofil der zu migrierenden Objekte an und berechnen Sie die erforderliche Festplattenkapazität. Weitere Informationen zum Monitoring der Festplattenkapazität Ihres StorageGRID Systems finden Sie unter "[Managen Sie Storage-Nodes](#)" Und die Anweisungen für "[Monitoring von StorageGRID](#)".

ILM-Richtlinie für migrierte Daten bestimmen

Die ILM-Richtlinie von StorageGRID bestimmt, wie viele Kopien erstellt werden, an welchen Standorten Kopien gespeichert werden und wie lange diese Kopien aufbewahrt werden. Eine ILM-Richtlinie besteht aus mehreren ILM-Regeln, die die Filterung von Objekten und das Managen von Objektdaten über einen längeren Zeitraum beschreiben.

Je nachdem, wie migrierte Daten verwendet werden und Ihre Anforderungen für migrierte Daten erfüllt werden, können Sie eindeutige ILM-Regeln für migrierte Daten definieren, die sich von den ILM-Regeln unterscheiden, die für tägliche Betriebsabläufe verwendet werden. Wenn z. B. für das tägliche Datenmanagement unterschiedliche gesetzliche Anforderungen gelten als für die in der Migration enthaltenen Daten, möchten Sie möglicherweise eine andere Anzahl von Kopien der zu migrierenden Daten in einer anderen Storage-Klasse nutzen.

Sie können Regeln konfigurieren, die ausschließlich für migrierte Daten gelten, wenn es möglich ist, zwischen migrierten Daten und Objektdaten, die von den täglichen Abläufen gespeichert werden, eindeutig zu unterscheiden.

Wenn Sie mit einem der Metadatenkriterien zuverlässig zwischen den Datentypen unterscheiden können, können Sie anhand dieser Kriterien eine ILM-Regel definieren, die nur für migrierte Daten gilt.

Bevor Sie mit der Datenmigration beginnen, sollten Sie sich mit der ILM-Richtlinie des StorageGRID Systems und der Anwendung auf die migrierten Daten vertraut machen und alle Änderungen an der ILM-Richtlinie vorgenommen und getestet haben. Siehe "[Objektmanagement mit ILM](#)".



Eine falsch angegebene ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Überprüfen Sie alle Änderungen an einer ILM-Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass die Richtlinie wie vorgesehen funktioniert.

Bewerten der Auswirkung der Migration auf den Betrieb

Ein StorageGRID System wurde entwickelt, um einen effizienten Objekt-Storage- und -Abruf-Service zu ermöglichen. Durch die nahtlose Erstellung redundanter Kopien von Objektdaten und Metadaten ist ein hervorragender Schutz vor Datenverlust gewährleistet.

Die Datenmigration muss jedoch gemäß den Anweisungen in diesem Leitfaden sorgfältig durchgeführt werden, um Auswirkungen auf den täglichen Systembetrieb oder, in Extremfällen, die Gefahr eines Datenverlusts bei einem Ausfall im StorageGRID-System zu vermeiden.

Die Migration großer Datenmengen belastet das System zusätzlich. Bei starker Beladung des StorageGRID Systems reagiert das System langsamer auf Anfragen zum Speichern und Abrufen von Objekten. Dies beeinträchtigt das Speichern und Abrufen von Anfragen, die von wesentlicher Bedeutung für die täglichen Betriebsabläufe sind. Die Migration kann auch andere betriebliche Probleme verursachen. Wenn sich beispielsweise ein Storage-Node der Kapazität nähert, kann die hohe intermittierende Last aufgrund der Batch-Aufnahme dazu führen, dass der Storage Node zwischen Lese- und Schreibvorgängen wechseln und Meldungen generieren kann.

Bei hoher Auslastung können sich Warteschlangen für verschiedene Vorgänge entwickeln, die das StorageGRID System durchführen muss, um vollständige Redundanz von Objektdaten und -Metadaten sicherzustellen.

Die Datenmigration muss entsprechend den Richtlinien in diesem Dokument sorgfältig gemanagt werden, um einen sicheren und effizienten Betrieb des StorageGRID Systems während der Migration sicherzustellen. Nehmen Sie bei der Datenmigration Objekte in Batches auf oder drosseln Sie kontinuierlich die Aufnahme. Überwachen Sie dann kontinuierlich das StorageGRID-System, um sicherzustellen, dass verschiedene Attributwerte nicht überschritten werden.

Planung und Überwachung der Datenmigration

Die Datenmigration muss bei Bedarf geplant und überwacht werden, um sicherzustellen, dass die Daten gemäß der ILM-Richtlinie innerhalb der erforderlichen Frist abgelegt werden.

Planen Sie die Datenmigration

Vermeiden Sie die Datenmigration während der wichtigsten Geschäftszeiten. Begrenzen Sie die Datenmigration auf Abende, Wochenenden und andere Zeiten, in denen die Systemauslastung knapp ist.

Planen Sie nach Möglichkeit keine Datenmigration in Phasen mit hoher Aktivität ein. Wenn es jedoch nicht

sinnvoll ist, den hohen Aktivitätszeitraum vollständig zu vermeiden, ist es sicher, so lange vorzugehen, wie Sie die relevanten Attribute genau überwachen und Maßnahmen ergreifen, wenn sie akzeptable Werte überschreiten.

Monitoring der Datenmigration

In dieser Tabelle sind die Attribute aufgeführt, die während der Datenmigration überwacht werden müssen, und die jeweiligen Probleme aufgeführt.

Wenn Sie Traffic-Klassifizierungsrichtlinien mit Geschwindigkeitsbegrenzungen zur Drosselung verwenden, können Sie die beobachtete Rate in Verbindung mit den in der folgenden Tabelle beschriebenen Statistiken überwachen und die Grenzwerte bei Bedarf reduzieren.

Überwachen	Beschreibung
Anzahl an Objekten, die auf die ILM-Bewertung warten	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. 2. Wählen Sie Deployment > Übersicht > Main. 3. Überwachen Sie im Abschnitt ILM-Aktivität die Anzahl der für die folgenden Attribute angezeigten Objekte: <ul style="list-style-type: none"> ◦ Ausstehend - alles (XQUZ): Die Gesamtzahl der Objekte, die auf die ILM-Bewertung warten. ◦ Ausstehend - Client (XCQZ): Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aus Client-Operationen warten (zum Beispiel Aufnahme). 4. Wenn die Anzahl der für eines dieser Attribute angezeigten Objekte 100,000 überschreitet, drosseln Sie die Aufnahmegeschwindigkeit von Objekten, um die Last auf dem StorageGRID-System zu verringern.
Storage-Kapazität eines Targeted Archivsystems	Wenn durch die ILM-Richtlinie eine Kopie der migrierten Daten auf ein zielgerichtetes Storage-System (Band oder Cloud) gespeichert wird, überwachen Sie die Kapazität des Zielspeichersystems, um sicherzustellen, dass genügend Kapazität für die migrierten Daten vorhanden ist.
Archiv-Knoten > ARC > Store	Wenn ein Alarm für das Attribut Store Failures (ARVF) ausgelöst wird, hat das zielgerichtete Archivspeichersystem möglicherweise die Kapazität erreicht. Überprüfen Sie das ausgewählte Archivspeichersystem, und beheben Sie alle Probleme, die einen Alarm ausgelöst haben.

Objektmanagement mit ILM

Objekte mit ILM managen: Übersicht

Sie managen die Objekte in einem StorageGRID System, indem Sie eine ILM-Richtlinie (Information Lifecycle Management) konfigurieren, die aus einer oder mehreren ILM-Regeln besteht. Die ILM-Regeln erklären StorageGRID, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien über einen längeren Zeitraum gemanagt

werden.

Informationen zu diesen Anweisungen

Für die Entwicklung und Implementierung von ILM-Regeln und der ILM-Richtlinie ist eine sorgfältige Planung erforderlich. Betriebliche Anforderungen, die Topologie des StorageGRID Systems, die Anforderungen an die Objektsicherung und die verfügbaren Storage-Typen sind unbedingt bekannt. Anschließend müssen Sie festlegen, wie unterschiedliche Objekttypen kopiert, verteilt und gespeichert werden sollen.

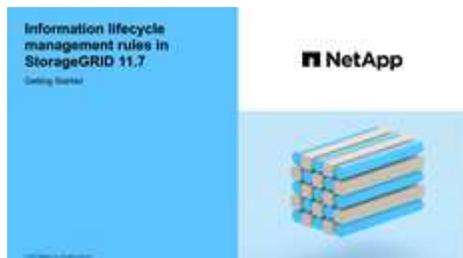
Mithilfe dieser Anweisungen können Sie:

- Erfahren Sie mehr über StorageGRID ILM, einschließlich ["Wie ILM im gesamten Leben eines Objekts funktioniert"](#).
- Erfahren Sie mehr über die Konfiguration ["Storage-Pools"](#), ["Cloud-Storage-Pools"](#), und ["ILM-Regeln"](#).
- Erfahren Sie, wie Sie ["Erstellen, Simulieren und Aktivieren einer ILM-Richtlinie"](#) Auf diese Weise werden Objektdaten an einem oder mehreren Standorten gesichert.
- Erfahren Sie, wie Sie ["Managen von Objekten mit S3 Object Lock"](#), Wodurch sichergestellt wird, dass Objekte in bestimmten S3 Buckets nicht für einen bestimmten Zeitraum gelöscht oder überschrieben werden.

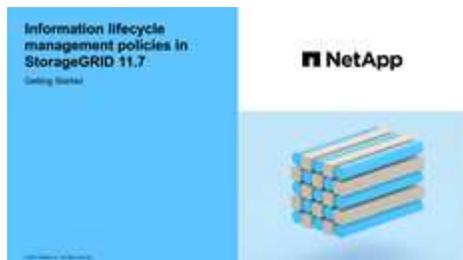
Weitere Informationen .

Sehen Sie sich die folgenden Videos an, um mehr zu erfahren:

- ["Video: Information Lifecycle Management Regeln in StorageGRID 11.7"](#).



- ["Video: Information Lifecycle Management Policies in StorageGRID 11.7"](#)



ILM und Objekt-Lebenszyklus

Wie ILM im gesamten Leben eines Objekts funktioniert

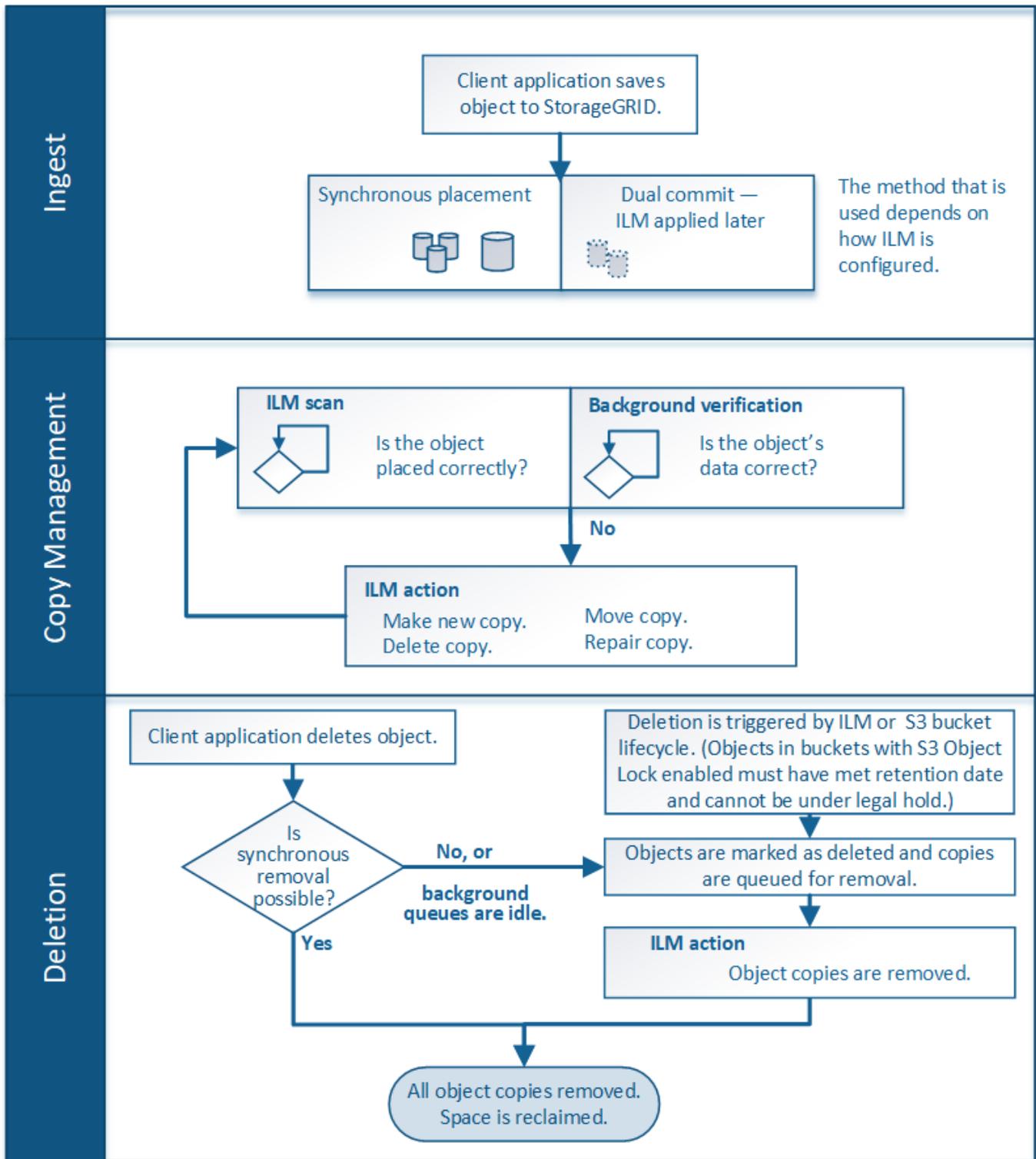
Wenn Sie verstehen, wie StorageGRID ILM für das Management von Objekten in jeder Lebensphase verwendet, können Sie eine effektivere Richtlinie entwickeln.

- **Aufnahme:** Aufnahme beginnt, wenn eine S3- oder Swift-Client-Anwendung eine Verbindung zum Speichern eines Objekts in das StorageGRID-System herstellt und abgeschlossen ist, wenn StorageGRID eine „Aufnahme erfolgreich“-Nachricht an den Client zurückgibt. Objektdaten werden bei der Aufnahme entweder durch sofortiges Anwenden von ILM-Anweisungen (synchrone Platzierung) oder durch Erstellen von zwischenzeitlichen Kopien und spätere Anwendung von ILM (Dual Commit) gesichert, je nachdem, wie die ILM-Anforderungen angegeben wurden.
- **Kopierverwaltung:** Nach dem Erstellen der Anzahl und des Typs der Objektkopien, die in den Anweisungen zur Platzierung des ILM angegeben sind, verwaltet StorageGRID Objektorte und schützt Objekte vor Verlust.
 - ILM-Scan und -Bewertung: StorageGRID scannt kontinuierlich die Liste der im Grid gespeicherten Objekte und überprüft, ob die aktuellen Kopien den ILM-Anforderungen entsprechen. Wenn unterschiedliche Typen, Ziffern oder Standorte von Objektkopien erforderlich sind, erstellt, löscht oder verschiebt StorageGRID Kopien nach Bedarf.
 - Hintergrundüberprüfung: StorageGRID führt kontinuierlich Hintergrundüberprüfung durch, um die Integrität von Objektdaten zu überprüfen. Wenn ein Problem gefunden wird, erstellt StorageGRID automatisch eine neue Objektkopie oder ein durch Löschung codiertes Objektfragment für den Austausch, das die aktuellen ILM-Anforderungen erfüllt. Siehe ["Überprüfen Sie die Objektintegrität"](#).
- **Objektlöschung:** Verwaltung eines Objekts endet, wenn alle Kopien aus dem StorageGRID-System entfernt werden. Objekte können als Ergebnis einer Löschanforderung durch einen Client oder als Ergebnis eines Löschvorgangs durch ILM oder Löschung aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus entfernt werden.



Objekte in einem Bucket, für den die S3-Objektsperrung aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einer Legal Hold befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.

Das Diagramm fasst die Funktionsweise von ILM im gesamten Lebenszyklus eines Objekts zusammen.



Aufnahme von Objekten

Aufnahmeoptionen

Wenn Sie eine ILM-Regel erstellen, geben Sie eine von drei Optionen zum Schutz der Objekte bei der Aufnahme an: Doppelter Commit, strenger oder ausgeglichener Storage.

Je nach Ihrer Wahl erstellt StorageGRID später vorläufige Kopien und Warteschlangen für die ILM-Bewertung.

Alternativ nutzt es die synchrone Platzierung und erstellt sofort Kopien zur Erfüllung der ILM-Anforderungen.

Flussdiagramm der Aufnahmeoptionen

Das Flussdiagramm zeigt, was passiert, wenn Objekte mit einer ILM-Regel abgeglichen werden, die jede der drei Aufnahmeoptionen nutzt.

Doppelte Provisionierung

Wenn Sie die Option Dual Commit auswählen, erstellt StorageGRID sofort interim-Objektkopien auf zwei verschiedenen Storage-Nodes und gibt dem Client eine „Ingest Successful“-Nachricht zurück. Das Objekt wird zur ILM-Evaluierung in eine Warteschlange gestellt und Kopien, die den Anweisungen zur Platzierung der Regel entsprechen, werden später erstellt.

Wann sollten Sie die Option Dual Commit verwenden

Verwenden Sie in einem der folgenden Fälle die Dual-Commit-Option:

- Die wichtigsten Überlegungen dabei sind die Verwendung von ILM-Regeln für mehrere Standorte und die Client-Erfassungs-Latenz. Wenn Sie Dual Commit verwenden, müssen Sie sicherstellen, dass Ihr Grid die zusätzliche Arbeit beim Erstellen und Entfernen der Dual-Commit-Kopien ausführen kann, wenn sie ILM nicht erfüllen. Im Detail:
 - Die Last am Grid muss so gering sein, dass kein ILM-Rückstand mehr vorhanden ist.
 - Das Grid muss über überschüssige Hardware-Ressourcen verfügen (IOPS, CPU, Arbeitsspeicher, Netzwerkbandbreite usw.).
- Sie verwenden ILM-Regeln für mehrere Standorte und die WAN-Verbindung zwischen den Standorten weist normalerweise eine hohe Latenz oder eine begrenzte Bandbreite auf. In diesem Szenario kann die Verwendung der Dual-Commit-Option dazu beitragen, Client-Timeouts zu verhindern. Bevor Sie sich für die Dual Commit-Option entscheiden, sollten Sie die Client-Applikation mit realistischen Workloads testen.

Streng

Wenn Sie die strenge Option auswählen, verwendet StorageGRID bei der Aufnahme eine synchrone Platzierung und erstellt sofort alle Objektkopien, die in der Platzierung der Regel angegeben sind. Die Aufnahme schlägt fehl, wenn StorageGRID nicht alle Kopien erstellen kann, z. B. weil ein erforderlicher Speicherort vorübergehend nicht verfügbar ist. Der Client muss den Vorgang wiederholen.

Wann die strenge Option verwendet werden soll

Verwenden Sie die Option streng, wenn Sie eine betriebliche oder gesetzliche Anforderung haben, Objekte sofort nur an den in der ILM-Regel aufgeführten Standorten zu speichern. Um beispielsweise eine gesetzliche Vorgabe zu erfüllen, müssen Sie möglicherweise die Option „Strict“ und einen erweiterten Filter „Speicherortbeschränkung“ verwenden, um sicherzustellen, dass Objekte niemals in bestimmten Rechenzentren gespeichert werden.

Siehe ["Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"](#).

Ausgeglichen (Standard)

Wenn Sie die Option „Ausgleich“ auswählen, verwendet StorageGRID bei der Aufnahme auch die synchrone Platzierung und erstellt sofort alle Kopien, die in den Anweisungen zur Platzierung der Regel angegeben sind. Wenn StorageGRID nicht sofort alle Kopien erstellen kann, verwendet man im Gegensatz zur strengen Option

„Dual Commit“.

Wann sollte die Option „Balance“ verwendet werden

Die ausgewogene Option erzielt die beste Kombination aus Datensicherung, Grid-Performance und Aufnahme-Erfolg. Ausgeglichen ist die Standardoption im Assistenten zum Erstellen von ILM-Regeln.

Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen

Wenn Sie die vor- und Nachteile der drei Optionen zum Schutz von Daten bei der Aufnahme (ausgewogen, streng oder Dual-Commit) kennen, können Sie leichter entscheiden, welche für eine ILM-Regel ausgewählt werden soll.

Eine Übersicht über die Aufnahmeoptionen finden Sie unter ["Aufnahmeoptionen"](#).

Vorteile der ausgewogenen und strengen Optionen

Im Vergleich zu Dual-Commit, das während der Aufnahme zwischenzeitliche Kopien erstellt, bieten die zwei Optionen zur synchronen Platzierung folgende Vorteile:

- **Bessere Datensicherheit:** Objektdaten werden sofort gemäß den Anweisungen zur Platzierung der ILM-Regel geschützt, die so konfiguriert werden können, dass sie vor einer Vielzahl von Ausfallszenarien, einschließlich des Ausfalls von mehr als einem Speicherort, geschützt werden. Bei zwei Daten kann nur der Schutz vor dem Verlust einer einzelnen lokalen Kopie geschützt werden.
- **Effizienterer Netzbetrieb:** Jedes Objekt wird nur einmal verarbeitet, wie es aufgenommen wird. Da das StorageGRID System die Interimskopien nicht nachverfolgen oder löschen muss, sinkt der Verarbeitungsbedarf und der Datenbankspeicherplatz wird verringert.
- **(ausgewogen) Empfohlen:** Die ausgewogene Option bietet optimale ILM-Effizienz. Die Verwendung der Balanced-Option wird empfohlen, es sei denn, es ist ein striktes Aufnahmeverhalten erforderlich oder das Grid erfüllt alle Kriterien für die Verwendung von Dual Commit.
- **(strikt) Gewissheit über Objektstandorte:** Die strenge Option garantiert, dass Objekte sofort nach den Platzierungsanweisungen in der ILM-Regel gespeichert werden.

Nachteile der ausgewogenen und strengen Optionen

Im Vergleich zu Dual Commit haben die ausgewogenen und strengen Optionen einige Nachteile:

- **Längere Client-Ingest:** Client-Ingest-Latenzen können länger sein. Wenn Sie die Optionen „ausgeglichen“ oder „streng“ verwenden, wird die Meldung „Ingest successful“ erst an den Client zurückgegeben, wenn alle Fragmente, die nach der Löschung codiert wurden, oder replizierte Kopien erstellt und gespeichert werden. Objektdaten werden allerdings sehr wahrscheinlich die endgültige Platzierung viel schneller erreichen.
- **(streng) höhere Aufnahmeraten:** Bei der strengen Option schlägt die Aufnahme fehl, wenn StorageGRID nicht sofort alle in der ILM-Regel angegebenen Kopien erstellen kann. Falls ein benötigter Speicherplatz vorübergehend offline ist oder Netzwerkprobleme auftreten, die zu Verzögerungen beim Kopieren von Objekten zwischen Standorten führen, ist unter Umständen ein hoher Aufnahmefehler zu beobachten.
- **(strict) S3-Multipart-Upload-Platzierungen sind unter Umständen nicht wie erwartet:** Bei strikter Prüfung erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Bei einem S3-Multipart-Upload wird ILM für jeden aufgenommenen Teil des Objekts und für das gesamte Objekt evaluiert, wenn der mehrteilige Upload abgeschlossen ist. Unter den folgenden Umständen kann dies zu Platzierungen führen, die sich von Ihnen unterscheiden:

- **Wenn sich ILM ändert, während ein S3-Multipart-Upload im Gange ist:** Da jedes Teil gemäß der Regel platziert wird, die bei der Aufnahme des Teils aktiv ist, entsprechen einige Teile des Objekts möglicherweise nicht den aktuellen ILM-Anforderungen, wenn der mehrteilige Upload abgeschlossen ist. In diesen Fällen schlägt die Aufnahme des Objekts nicht fehl. Stattdessen wird jedes Teil, das nicht korrekt platziert wird, in die Warteschlange für eine erneute ILM-Bewertung eingereiht und später an den richtigen Speicherort verschoben.
- **Wenn ILM-Regeln Filter auf Größe:** Bei der Bewertung von ILM für ein Teil filtert StorageGRID die Größe des Teils, nicht die Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn z. B. eine Regel angibt, dass alle Objekte ab 10 GB auf DC1 gespeichert werden, während alle kleineren Objekte an DC2 gespeichert sind, wird bei Aufnahme jeder 1 GB-Teil eines 10-teiligen mehrteiligen Uploads auf DC2 gespeichert. Wenn ILM für das Objekt bewertet wird, werden alle Teile des Objekts auf DC1 verschoben.
- **(strict) Aufnahme scheitert nicht, wenn Objekt-Tags oder Metadaten aktualisiert werden und neu erforderliche Platzierungen nicht gemacht werden können:** Mit strikter, erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Wenn Sie jedoch Metadaten oder Tags für ein Objekt aktualisieren, das bereits im Raster gespeichert ist, wird das Objekt nicht erneut aufgenommen. Das bedeutet, dass Änderungen an der Objektplatzierung, die durch die Aktualisierung ausgelöst werden, nicht sofort vorgenommen werden. Änderungen an der Platzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird. Wenn erforderliche Platzierungsänderungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Standort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung bei, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei Objektplatzierungen mit den ausgewogenen und strengen Optionen

Die ausgewogenen oder strikten Optionen können nicht für ILM-Regeln verwendet werden, die über eine der folgenden Platzierungsanweisungen verfügen:

- Platzierung in einem Cloud-Storage-Pool am Tag 0
- Platzierung in einem Archiv-Knoten an Tag 0.
- Platzierungen in einem Cloud-Speicherpool oder einem Archiv-Node, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit hat.

Diese Einschränkungen bestehen, da StorageGRID nicht synchron Kopien auf einen Cloud-Speicherpool oder Archivknoten erstellen kann und eine benutzerdefinierte Erstellungszeit auf die Gegenwart aufgelöst werden kann.

Auswirkungen von ILM-Regeln und Konsistenzkontrollen auf die Datensicherung

Sowohl Ihre ILM-Regel als auch Ihre Wahl der Konsistenzkontrolle beeinflussen den Schutz von Objekten. Diese Einstellungen können interagieren.

Das für eine ILM-Regel ausgewählte Aufnahmeverhalten wirkt sich beispielsweise auf die anfängliche Platzierung von Objektkopien aus, während sich die beim Speichern eines Objekts verwendete Konsistenzkontrolle auf die anfängliche Platzierung von Objekt-Metadaten auswirkt. StorageGRID benötigt zur Erfüllung von Clientanforderungen sowohl Zugriff auf die Daten eines Objekts als auch auf die Metadaten. Durch die Auswahl der passenden Schutzstufen für die Konsistenzstufe und das Aufnahmeverhalten können die Daten anfangs besser gesichert und Systemantworten vorhersehbarer.

Hier finden Sie eine kurze Zusammenfassung der in StorageGRID verfügbaren Konsistenzkontrollen:

- **Alle:** Alle Knoten erhalten sofort Objektmetadaten oder die Anfrage schlägt fehl.

- **Stark-global:** Objektmetadaten werden sofort auf alle Seiten verteilt. Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
- **Strong-site:** Objektmetadaten werden sofort auf andere Knoten am Standort verteilt. Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
- **Read-after-New-write:** Sorgt für die Konsistenz von Read-after-write für neue Objekte und eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
- **Verfügbar:** Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.



Lesen Sie vor Auswahl einer Konsistenzstufe die vollständige Beschreibung der Consistency Controls in den Anweisungen für "[S3-REST-API VERWENDEN](#)". Vor dem Ändern des Standardwerts sollten Sie die Vorteile und Einschränkungen kennen.

Beispiel für die Interaktion zwischen Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel:** Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe:** "strong-global" (Objektmetadaten werden sofort auf alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „strong-Site“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten an den Remote Standort repliziert wurden, aber bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Verwandte Informationen

- "[Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten](#)"

Speicherung von Objekten (Replizierung oder Erasure Coding)

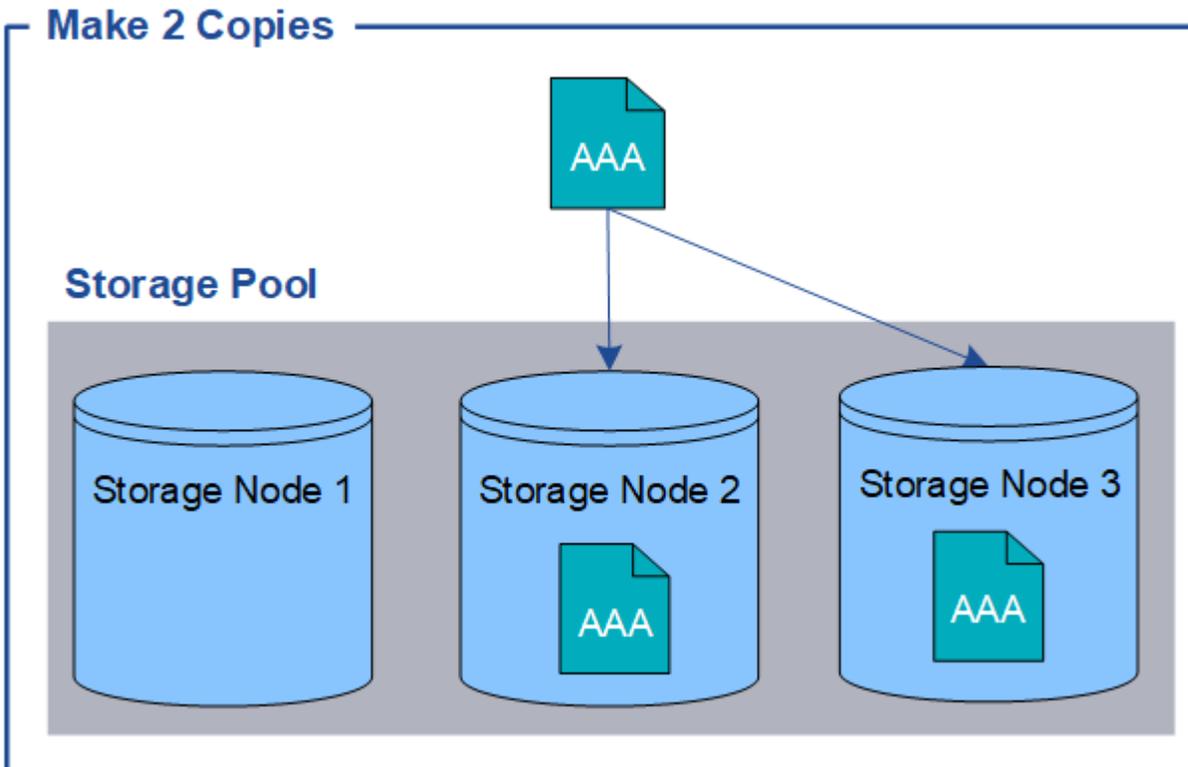
Was ist Replikation?

Die Replikierung ist eine von zwei Methoden, die von StorageGRID zum Speichern von Objektdaten verwendet werden. Wenn Objekte mit einer ILM-Regel übereinstimmen, die

Replizierung verwendet, erstellt das System exakte Kopien von Objektdaten und speichert die Kopien auf Storage-Nodes oder Archiv-Nodes.

Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien konfigurieren, geben Sie an, wie viele Kopien erstellt werden sollen, wo diese Kopien erstellt werden sollen und wie lange die Kopien an jedem Standort gespeichert werden sollen.

Im folgenden Beispiel gibt die ILM-Regel an, dass zwei replizierte Kopien jedes Objekts in einem Storage-Pool mit drei Storage-Nodes platziert werden.



Wenn StorageGRID Objekte mit dieser Regel übereinstimmt, werden zwei Kopien des Objekts erstellt, wobei jede Kopie auf einem anderen Storage-Node im Storage-Pool platziert wird. Die beiden Kopien können auf zwei der drei verfügbaren Storage-Nodes platziert werden. In diesem Fall wurden in der Regel Objektkopien auf Speicherknoten 2 und 3 platziert. Da es zwei Kopien gibt, kann das Objekt abgerufen werden, wenn einer der Nodes im Speicherpool ausfällt.



StorageGRID kann nur eine replizierte Kopie eines Objekts auf einem beliebigen Storage Node speichern. Wenn Ihr Grid drei Storage-Nodes enthält und Sie eine ILM-Regel mit 4 Kopien erstellen, werden nur drei Kopien erstellt: Eine Kopie für jeden Storage-Node. Die Warnung **ILM-Platzierung unerreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Verwandte Informationen

- ["Was ist Erasure Coding?"](#)
- ["Was ist ein Speicherpool?"](#)
- ["Schutz vor Standortausfällen durch Replizierung und Erasure Coding"](#)

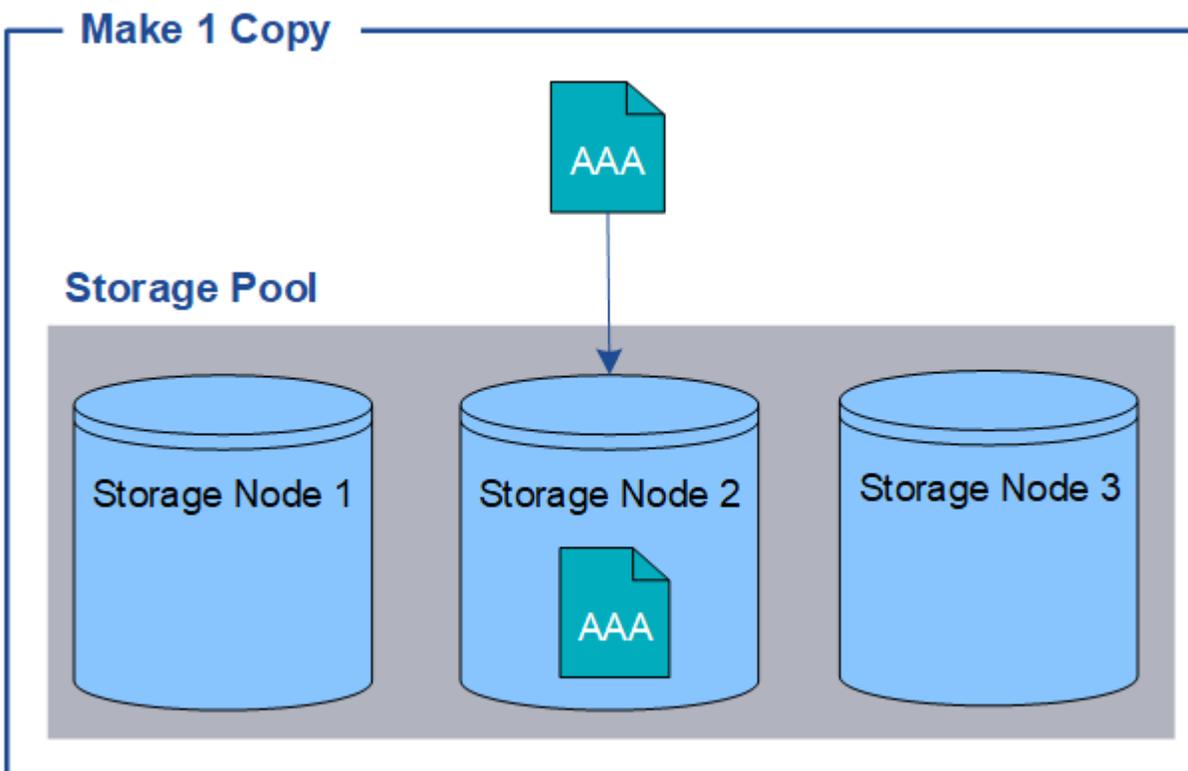
Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden

Beim Erstellen einer ILM-Regel zum Erstellen replizierter Kopien sollten Sie immer mindestens zwei Kopien für einen beliebigen Zeitraum in den Anweisungen zur Platzierung angeben.

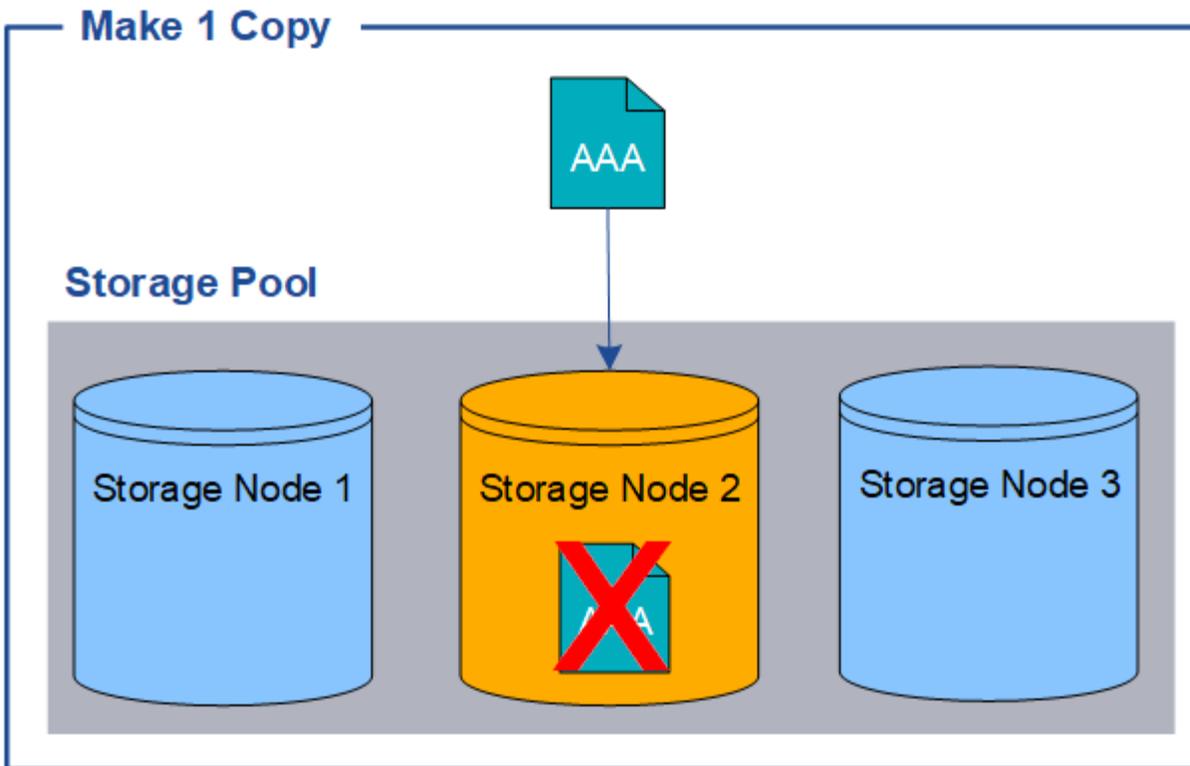


Verwenden Sie keine ILM-Regel, die nur eine replizierte Kopie für einen beliebigen Zeitraum erstellt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

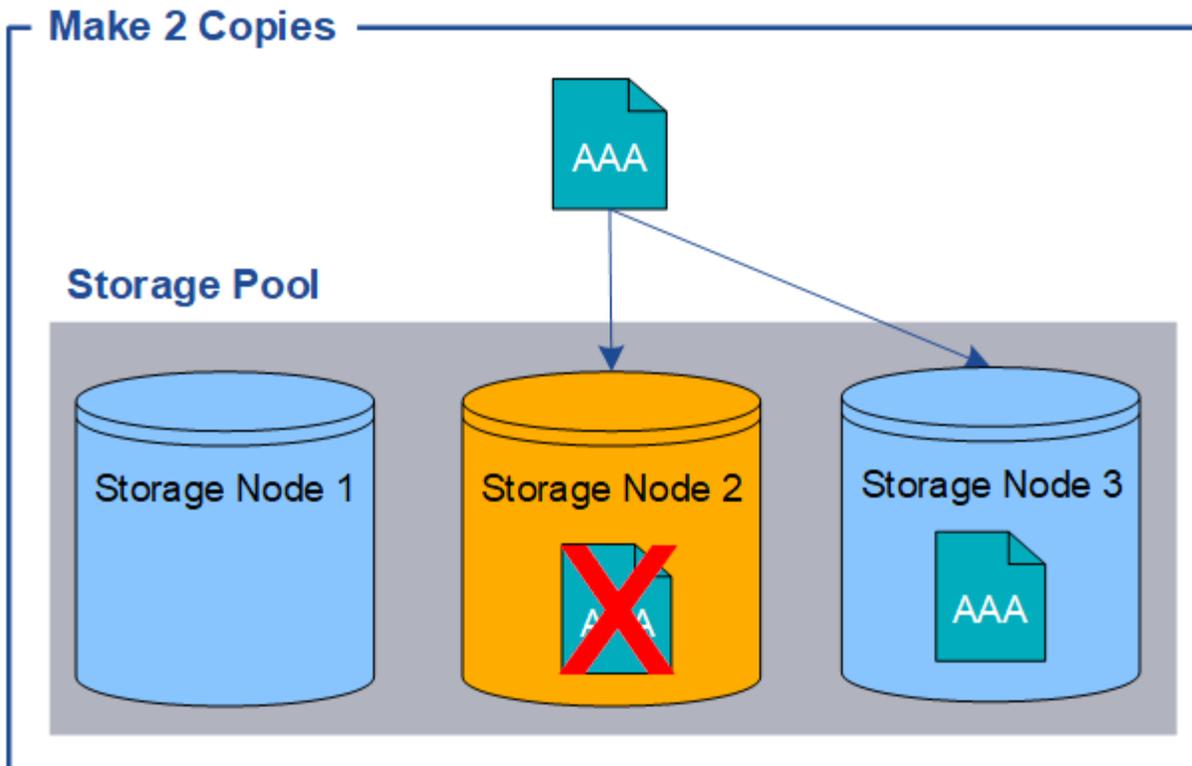
Im folgenden Beispiel gibt die ILM-Regel „1 Kopie erstellen“ an, dass eine replizierte Kopie eines Objekts in einem Speicherpool platziert wird, der drei Storage-Nodes enthält. Wenn ein Objekt aufgenommen wird, das dieser Regel entspricht, platziert StorageGRID eine einzelne Kopie auf nur einem Storage-Node.



Wenn eine ILM-Regel nur eine replizierte Kopie eines Objekts erstellt, ist der Zugriff auf das Objekt möglich, wenn der Storage-Node nicht verfügbar ist. In diesem Beispiel verlieren Sie vorübergehend den Zugriff auf das Objekt AAA, wenn Storage Node 2 offline ist, z. B. während eines Upgrades oder eines anderen Wartungsverfahrens. Sie verlieren das Objekt AAA vollständig, wenn Storage Node 2 ausfällt.



Um den Verlust von Objektdaten zu vermeiden, sollten immer mindestens zwei Kopien aller Objekte erstellt werden, die durch die Replizierung gesichert werden sollen. Wenn zwei oder mehr Kopien vorhanden sind, können Sie weiterhin auf das Objekt zugreifen, wenn ein Storage-Node ausfällt oder offline geht.



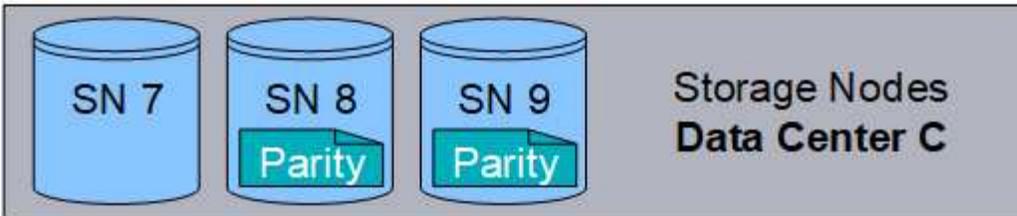
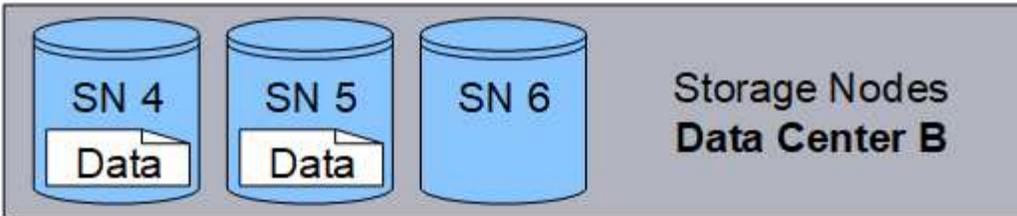
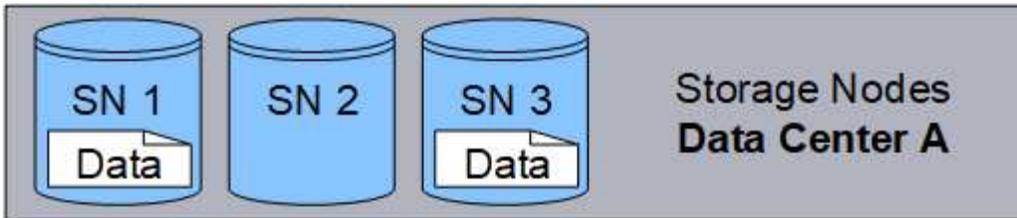
Was ist Erasure Coding?

Erasure Coding ist eine von zwei Methoden, die StorageGRID zum Speichern von Objektdaten verwendet. Wenn Objekte mit einer ILM-Regel übereinstimmen, die Erasure Coding verwendet, werden diese Objekte in Datenfragmente geteilt, weitere Paritätsfragmente werden berechnet und jedes Fragment wird auf einem anderen Storage Node gespeichert.

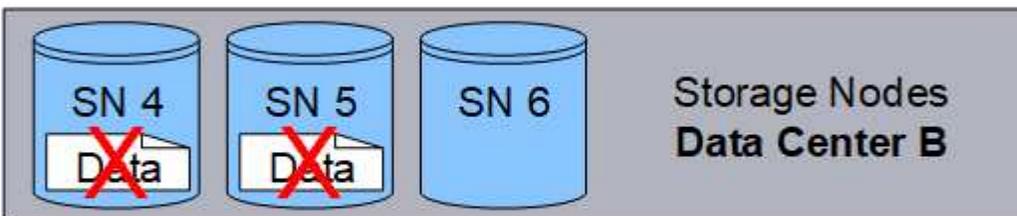
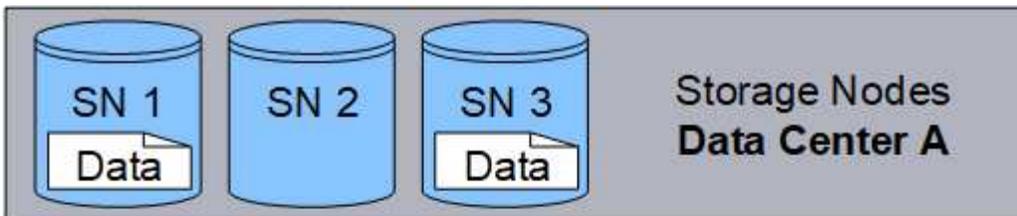
Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Daten oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zur Fehlerkorrektur dieses Fragment mit einer Teilmenge der verbleibenden Daten und Paritätsfragmente neu erstellen.

Beim Erstellen von ILM-Regeln erstellt StorageGRID Profile, die Erasure Coding unterstützen. Sie können eine Liste der Profile zum Erasure Coding anzeigen, "[Umbenennen eines Profils für die Erasure Coding](#)", Oder "[Deaktivieren Sie ein Erasure Coding-Profil, wenn es derzeit nicht in ILM-Regeln verwendet wird](#)".

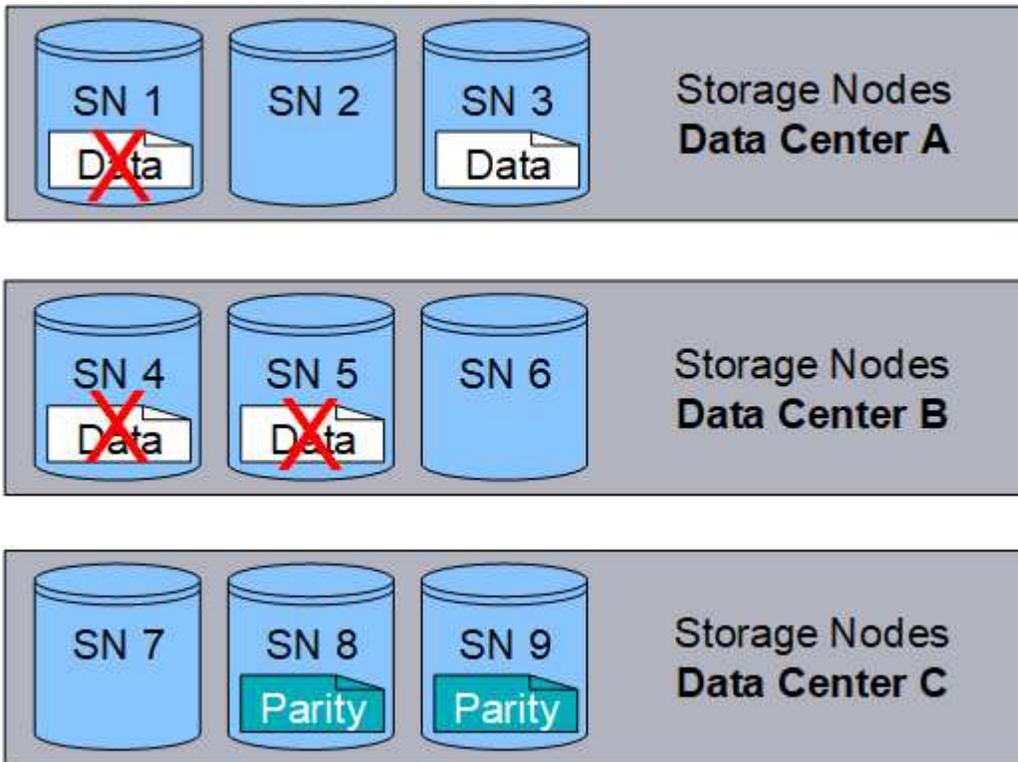
Im folgenden Beispiel wird der Algorithmus zur Einhaltung von Datenkonsistenz (Erasure Coding) für Objektdaten dargestellt. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Schema zur Einhaltung von Datenkonsistenz. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente wird auf einem anderen Node über drei Datacenter-Standorte gespeichert, um Daten bei Node-Ausfällen oder Standortausfällen zu sichern.



Das 4+2 Erasure Coding-Schema kann auf verschiedene Weise konfiguriert werden. Sie können beispielsweise einen Speicherpool mit einem Standort konfigurieren, der sechs Storage-Nodes enthält. Für "[Schutz vor Standortausfällen](#)", Sie können einen Speicherpool verwenden, der drei Standorte mit drei Storage Nodes an jedem Standort enthält. Ein Objekt kann abgerufen werden, solange vier der sechs Fragmente (Daten oder Parität) verfügbar sind. Bis zu zwei Fragmente können ohne Verlust der Objektdaten verloren gehen. Wenn ein ganzer Standort verloren geht, kann das Objekt dennoch abgerufen oder repariert werden, solange alle anderen Fragmente zugänglich bleiben.



Wenn mehr als zwei Speicherknoten verloren gehen, kann das Objekt nicht abgerufen werden.



Verwandte Informationen

- ["Was ist Replikation?"](#)
- ["Was ist ein Speicherpool?"](#)
- ["Was sind Erasure Coding-Systeme?"](#)
- ["Umbenennen eines Profils für die Erasure Coding"](#)
- ["Deaktivieren Sie ein Erasure Coding-Profil"](#)

Was sind Erasure Coding-Systeme?

Erasure Coding steuert die Anzahl von Datenfragmenten und die Anzahl der Parity-Fragmente für jedes Objekt.

Wenn Sie das Profil zur Einhaltung von Datenkonsistenz für eine ILM-Regel konfigurieren, wählen Sie ein verfügbares Erasure-Coding-Schema basierend auf der Anzahl der Storage-Nodes und -Standorte des Storage-Pools aus, den Sie verwenden möchten.

Das StorageGRID-System verwendet den Reed-Solomon-Erasure-Coding-Algorithmus. Der Algorithmus teilt ein Objekt in ein k Datenfragmente und m Paritätsfragmente. Der $k + m = n$ Fragmente werden verteilt n Storage-Nodes für die Datensicherung. Ein Objekt kann bis zu m Verlorene oder beschädigte Fragmente. Um ein Objekt abzurufen oder zu reparieren, k Fragmente werden benötigt.

Verwenden Sie bei der Auswahl des Speicherpools für eine Regel, die eine Kopie mit Verfahren zur Fehlerkorrektur erstellt, die folgenden Richtlinien für Speicherpools:

- Der Speicherpool muss drei oder mehr Standorte oder exakt einen Standort umfassen.



Sie können kein Erasure Coding verwenden, wenn der Storage-Pool zwei Standorte umfasst.

- [Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools mit drei oder mehr Standorten](#)
- [Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools an einem Standort](#)
- Verwenden Sie keinen Speicherpool, der den Standardstandort „Alle Standorte“ enthält.
- Der Speicherpool sollte mindestens enthalten $k+m + 1$ Storage-Nodes:

Die Mindestanzahl der erforderlichen Storage-Nodes ist $k+m$. Durch mindestens einen zusätzlichen Storage-Node können jedoch Ingest- oder ILM-Backlogs verhindert werden, wenn ein erforderlicher Storage-Node vorübergehend nicht verfügbar ist.

Der Storage-Overhead eines Erasure-Coding-Schemas wird durch Division der Anzahl der Paritätsfragmente berechnet (m) durch die Anzahl der Datenfragmente (k). Der Storage Overhead lässt sich ermitteln, wie viel Festplattenspeicher jedes mit Erasure-Coding-Objekt benötigt:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Wenn Sie beispielsweise ein Objekt mit 10 MB unter Verwendung des Schemas von 4+2 speichern (mit einem Mehraufwand von 50 %), verbraucht das Objekt 15 MB Grid Storage. Wenn Sie dasselbe 10 MB große Objekt mit dem Schema 6+2 speichern (mit einem Mehraufwand von 33 %), verbraucht das Objekt etwa 13.3 MB.

Wählen Sie das Erasure-Coding-Schema mit dem niedrigsten Gesamtwert von $k+m$. Das entspricht Ihren Bedürfnissen. Erasure-Coding-Schemata mit einer geringeren Anzahl von Fragmenten sind insgesamt recheneffizienter, da weniger Fragmente erstellt und verteilt (oder abgerufen) werden, aufgrund der größeren Fragmentgröße eine bessere Performance aufweisen und bei einer Erweiterung weniger Nodes hinzugefügt werden müssen, wenn mehr Storage benötigt wird. (Informationen zur Planung einer Speichererweiterung finden Sie im "[Anweisungen zur Erweiterung von StorageGRID](#)".)

Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools mit drei oder mehr Standorten

Die folgende Tabelle beschreibt die von StorageGRID derzeit unterstützten Erasure Coding-Schemata für Storage-Pools, die drei oder mehr Standorte umfassen. Alle diese Maßnahmen bieten einen Standortausfallschutz. Ein Standort kann verloren gehen, und das Objekt ist weiterhin verfügbar.

Für Erasure Coding-Schemata, die Schutz vor Standortausfällen bieten, ist die empfohlene Anzahl von Storage-Nodes im Speicherpool größer $k+m + 1$. Da jeder Standort mindestens drei Storage-Nodes erfordert.

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) ($k+m$)	Mindestanzahl der bereitgestellten Standorte	Empfohlene Anzahl von Storage-Nodes an jedem Standort	Insgesamt empfohlene Anzahl von Storage-Nodes	Schutz vor Standortausfällen?	Storage Overhead
4 + 2	3	3	9	Ja.	50 % erzielt
6 + 2	4	3	12	Ja.	33 % erzielt
8 + 2	5	3	15	Ja.	25 % erzielt

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) ($k+m$)	Mindestanzahl der bereitgestellten Standorte	Empfohlene Anzahl von Storage-Nodes an jedem Standort	Insgesamt empfohlene Anzahl von Storage-Nodes	Schutz vor Standortausfällen?	Storage Overhead
6 + 3	3	4	12	Ja.	50 % erzielt
9 + 3	4	4	16	Ja.	33 % erzielt
2+1	3	3	9	Ja.	50 % erzielt
4+1	5	3	15	Ja.	25 % erzielt
6+1	7	3	21	Ja.	17 % erzielt
7 + 5	3	5	15	Ja.	71 % erzielt



StorageGRID erfordert mindestens drei Storage-Nodes pro Standort. Für die Verwendung des Schemas 7+5 benötigt jeder Standort mindestens vier Speicherknoten. Es wird empfohlen, fünf Storage-Nodes pro Standort zu verwenden.

Bei der Auswahl eines Löschungsschemas, das Standortschutz bietet, sollte die relative Bedeutung der folgenden Faktoren in Einklang gestellt werden:

- **Anzahl der Fragmente:** Leistung und Expansionsflexibilität sind im Allgemeinen besser, wenn die Gesamtzahl der Fragmente geringer ist.
- **Fehlertoleranz:** Die Fehlertoleranz wird erhöht, indem mehr Paritätssegmente vorhanden sind (das heißt, wenn m hat einen höheren Wert.)
- **Netzwerkverkehr:** Bei der Wiederherstellung nach Ausfällen, mit einem Schema mit mehr Fragmenten (das heißt, eine höhere Summe für $k+m$) Erzeugt mehr Netzwerkverkehr.
- **Storage Overhead:** Bei Systemen mit höherem Overhead wird mehr Speicherplatz pro Objekt benötigt.

Wenn Sie beispielsweise zwischen einem Schema 4+2 und dem Schema 6+3 (mit jeweils 50 % Storage Overhead) entscheiden, wählen Sie das Schema 6+3 aus, wenn eine zusätzliche Fehlertoleranz erforderlich ist. Wählen Sie das Schema 4+2 aus, wenn die Netzwerkressourcen begrenzt sind. Wenn alle anderen Faktoren gleich sind, wählen Sie 4+2 aus, da die Gesamtzahl der Fragmente geringer ist.



Wenn Sie sich nicht sicher sind, welches Schema Sie verwenden möchten, wählen Sie 4+2 oder 6+3 aus, oder wenden Sie sich an den technischen Support.

Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools an einem Standort

Ein Storage-Pool an einem Standort unterstützt alle Erasure Coding-Schemata, die für drei oder mehr Standorte definiert sind, sofern der Standort über ausreichend Storage-Nodes verfügt.

Die Mindestanzahl der erforderlichen Storage-Nodes ist $k+m$, Aber ein Speicherpool mit $k+m + 1$ Storage-Nodes werden empfohlen. Zum Beispiel erfordert das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) 2+1 einen Speicherpool mit mindestens drei Storage-Nodes, es werden jedoch vier Storage-Nodes

empfohlen.

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) ($k+m$)	Mindestanzahl Storage-Nodes	Empfohlene Anzahl von Storage-Nodes	Storage Overhead
4 + 2	6	7	50 % erzielt
6 + 2	8	9	33 % erzielt
8 + 2	10	11	25 % erzielt
6 + 3	9	10	50 % erzielt
9 + 3	12	13	33 % erzielt
2+1	3	4	50 % erzielt
4+1	5	6	25 % erzielt
6+1	7	8	17 % erzielt
7 + 5	12	13	71 % erzielt

Vor- und Nachteile sowie Anforderungen für Erasure Coding

Bevor Sie sich entscheiden, ob Sie zum Schutz von Objektdaten mithilfe von Replizierungs- oder Erasure Coding vor Verlust schützen möchten, sollten Sie die Vorteile und Nachteile sowie die Anforderungen für Verfahren zur Einhaltung von Datenkonsistenz kennen.

Vorteile von Erasure Coding

Im Vergleich zur Replizierung bietet das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verbesserte Zuverlässigkeit, Verfügbarkeit und Storage-Effizienz.

- **Zuverlässigkeit:** Die Zuverlässigkeit wird in Bezug auf Fehlertoleranz gemessen - das ist die Anzahl der gleichzeitigen Ausfälle, die ohne Datenverlust aufrechterhalten werden können. Mithilfe der Replizierung werden mehrere identische Kopien auf unterschiedlichen Nodes und über mehrere Standorte hinweg gespeichert. Bei der Einhaltung von Datenkonsistenz wird ein Objekt in Daten- und Paritätsfragmente codiert und über viele Nodes und Standorte verteilt. Diese Verteilung bietet Schutz vor Standort- und Node-Ausfällen. Im Vergleich zur Replizierung bietet Erasure Coding eine höhere Zuverlässigkeit bei vergleichbaren Storage-Kosten.
- **Verfügbarkeit:** Verfügbarkeit kann definiert werden als die Möglichkeit, Objekte abzurufen, wenn Speicherknoten ausfallen oder unzugänglich werden. Im Vergleich zur Replizierung bietet Erasure Coding eine höhere Verfügbarkeit bei vergleichbaren Storage-Kosten.
- **Storage-Effizienz:** Für ein ähnliches Maß an Verfügbarkeit und Zuverlässigkeit benötigen die durch das Erasure Coding geschützten Objekte weniger Speicherplatz als die gleichen Objekte, wenn sie durch Replikation geschützt sind. Ein Objekt mit 10 MB, das an zwei Standorten repliziert wird, benötigt

beispielsweise 20 MB Festplattenspeicher (zwei Kopien), während ein Objekt, das über drei Standorte mit einem Erasure Coding-Schema mit 6+3 codiert wird, nur 15 MB Festplattenspeicher in Anspruch nimmt.



Der Festplattenspeicher für Objekte, die mit Erasure-Coding-Verfahren codiert wurden, wird als Objektgröße und als Storage Overhead berechnet. Der prozentuale Storage Overhead entspricht der Anzahl der Paritätsfragmente, geteilt durch die Anzahl an Datenfragmenten.

Nachteile des Erasure Coding

Im Vergleich zur Replizierung hat das Verfahren zur Einhaltung von Datenkonsistenz folgende Nachteile:

- Je nach Erasure Coding-Schema wird eine erhöhte Anzahl von Storage-Nodes und -Standorten empfohlen. Wenn Sie hingegen Objektdaten replizieren, benötigen Sie pro Kopie nur einen Storage Node. Siehe "[Erasure Coding für Storage-Pools mit drei oder mehr Standorten](#)" Und "[Erasure Coding für Storage-Pools an einem Standort](#)".
- Höhere Kosten und Komplexität der Storage-Erweiterungen. Um eine Implementierung zu erweitern, bei der Replizierung verwendet wird, fügen Sie an jedem Ort, an dem Objektkopien erstellt werden, Storage-Kapazitäten hinzu. Um eine Implementierung zu erweitern, bei der Erasure Coding zum Einsatz kommt, müssen Sie sowohl das verwendete Verfahren zur Einhaltung von Datenkonsistenz als auch die Kapazität vorhandener Storage-Nodes in Betracht ziehen. Wenn Sie beispielsweise warten, bis die vorhandenen Nodes zu 100 % voll sind, müssen Sie mindestens $k+m$ Storage-Nodes hinzufügen: Wenn Sie jedoch erweitern, wenn vorhandene Nodes zu 70 % ausgelastet sind, können Sie zwei Nodes pro Standort hinzufügen und gleichzeitig die nutzbare Storage-Kapazität maximieren. Weitere Informationen finden Sie unter "[Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden](#)".
- Wenn Erasure Coding über geografisch verteilte Standorte hinweg verwendet wird, erhöht sich die Latenzzeiten beim Abruf. Die Objektfragmente für ein Objekt, das mit Erasure-Coding und Verteilung auf Remote-Standorte codiert und über WAN-Verbindungen verteilt ist, dauern länger, bis es über ein Objekt abgerufen wird, das repliziert und lokal verfügbar ist (derselbe Standort, an dem der Client eine Verbindung herstellt).
- Bei Verwendung von Erasure Coding für geografisch verteilte Standorte kommt ein höherer WAN-Netzwerkverkehr für Abrufvorgänge und Reparaturen zum Einsatz, insbesondere bei häufig abgerufenen Objekten oder bei Objektreparaturen über WAN-Netzwerkverbindungen.
- Wenn Sie standortübergreifend Erasure Coding verwenden, nimmt der maximale Objektdurchsatz ab, da die Netzwerklatenz zwischen Standorten zunimmt. Diese Abnahme ist auf die entsprechende Abnahme des TCP-Netzwerkdurchsatzes zurückzuführen, was sich darauf auswirkt, wie schnell das StorageGRID-System Objektfragmente speichern und abrufen kann.
- Höhere Auslastung von Computing-Ressourcen:

Wann sollte das Erasure Coding verwendet werden

Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für folgende Anforderungen:

- Objekte größer als 1 MB.



Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

- Langfristige oder kalte Storage-Lösung für selten abgerufene Inhalte

- Hohe Datenverfügbarkeit und -Zuverlässigkeit
- Schutz vor vollständigem Standort- und Node-Ausfall.
- Storage-Effizienz:
- Implementierungen an einem einzigen Standort, die eine effiziente Datensicherung benötigen und nur eine einzige Kopie mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) als mehrere replizierte Kopien benötigen
- Implementierungen an mehreren Standorten, bei denen die Latenz zwischen den Standorten weniger als 100 ms beträgt

Wie die Aufbewahrung von Objekten bestimmt wird

StorageGRID bietet sowohl Grid-Administratoren als auch einzelnen Mandantenbenutzer Optionen, um die Speicherdauer von Objekten festzulegen. Im Allgemeinen haben alle von einem Mandantenbenutzer bereitgestellten Aufbewahrungsanweisungen Vorrang vor den Aufbewahrungsanweisungen, die vom Grid-Administrator bereitgestellt werden.

Wie Mandantenbenutzer die Aufbewahrung von Objekten steuern

Mandantenbenutzer haben drei primäre Möglichkeiten, um zu steuern, wie lange ihre Objekte in StorageGRID gespeichert sind:

- Wenn die globale S3-Objektsperreinstellung für das Grid aktiviert ist, können Nutzer von S3-Mandanten Buckets erstellen, deren S3-Objektsperre aktiviert ist. Anschließend können sie über die S3-REST-API Aufbewahrungseinstellungen für jede zu diesem Bucket hinzugefügte Objektversion festlegen.
 - Eine Objektversion, die sich unter einem Legal Hold befindet, kann mit keiner Methode gelöscht werden.
 - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version nicht mit einer Methode gelöscht werden.
 - Objekte in Buckets mit aktivierter S3-Objektsperre werden durch ILM „Forever“ beibehalten. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-Anfrage oder den Ablauf des Bucket-Lebenszyklus gelöscht werden. Siehe "[Objekte managen mit S3 Object Lock](#)".
- Benutzer von S3-Mandanten können ihren Buckets eine Lifecycle-Konfiguration hinzufügen, für die eine Ablaufaktion festgelegt ist. Wenn ein Bucket-Lebenszyklus vorhanden ist, speichert StorageGRID ein Objekt, bis das Datum oder die Anzahl der Tage, die im Verfallsvorgang angegeben sind, erreicht ist, es sei denn, der Client löscht das Objekt zuerst. Siehe "[S3-Lebenszykluskonfiguration erstellen](#)".
- Ein S3- oder Swift-Client kann eine delete-Objektanforderung ausgeben. StorageGRID priorisiert Löschanfragen von Clients immer über den S3-Bucket-Lebenszyklus oder ILM, wenn sie bestimmen, ob ein Objekt gelöscht oder aufbewahrt werden soll.

Grid-Administratoren steuern die Objektaufbewahrung

Grid-Administratoren steuern mithilfe von ILM-Speicheranweisungen, wie lange Objekte gespeichert werden. Wenn Objekte mit einer ILM-Regel abgeglichen werden, speichert StorageGRID diese Objekte bis zum letzten Zeitraum der ILM-Regel verstrichen ist. Objekte werden unbefristet aufbewahrt, wenn „forever“ für die Platzierungsanweisungen angegeben ist.

Unabhängig davon, wer die Aufbewahrung von Objekten steuert, steuern ILM-Einstellungen, welche Arten von Objektkopien (repliziert oder Erasure Coding) gespeichert werden und wo sich die Kopien befinden (Storage-

Nodes, Cloud Storage Pools oder Archiv-Nodes).

Interaktion von S3-Bucket-Lebenszyklus und ILM

Die Aktion „Ablaufdatum“ in einem S3-Bucket-Lebenszyklus überschreibt immer die ILM-Einstellungen. Aus diesem Grund kann ein Objekt auch dann im Grid verbleiben, wenn ILM-Anweisungen zum Auflegen des Objekts verfallen sind.

Beispiele für die Aufbewahrung von Objekten

Die folgenden Beispiele sollten zur besseren Übersicht über die Interaktionen zwischen S3 Objektsperre, Bucket-Lebenszykluseinstellungen, Clientlöschanforderungen und ILM verwendet werden.

Beispiel 1: S3-Bucket-Lebenszyklus hält Objekte länger als ILM

ILM

Speichern von zwei Kopien für 1 Jahr (365 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Ergebnis

StorageGRID speichert das Objekt 730 Tage lang. StorageGRID verwendet die Bucket-Lifecycle-Einstellungen, um zu bestimmen, ob ein Objekt gelöscht oder aufbewahrt werden soll.



Wenn im Bucket-Lebenszyklus angegeben wird, dass Objekte länger aufbewahrt werden sollen als durch ILM angegeben, verwendet StorageGRID beim Bestimmen der Anzahl und des Typs der zu speichernden Kopien weiterhin die Anweisungen zur ILM-Platzierung. In diesem Beispiel werden zwei Kopien des Objekts von 366 bis 730 Tagen im StorageGRID gespeichert.

Beispiel 2: S3-Bucket-Lebenszyklus läuft Objekte vor ILM ab

ILM

Speichern von zwei Kopien für 2 Jahre (730 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 1 Jahr (365 Tage)

Ergebnis

StorageGRID löscht beide Kopien des Objekts nach Tag 365.

Beispiel 3: Beim Löschen von Clients wird der Bucket-Lebenszyklus und ILM überschrieben

ILM

Speichern von zwei Kopien auf Storage-Nodes „Forever“

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Anforderung zum Löschen des Clients

Ausgestellt am 400. Tag

Ergebnis

StorageGRID löscht beide Kopien des Objekts am Tag 400 als Antwort auf die Anforderung zum Löschen des Clients.

Beispiel 4: S3 Object Lock überschreibt die Anforderung zum Löschen des Clients

S3-Objektsperre

Aufbewahrung bis zum Datum für eine Objektversion ist 2026-03-31. Eine gesetzliche Aufbewahrungspflichten sind nicht in Kraft.

Kompatible ILM-Regel

Speichern Sie zwei Kopien auf Storage-Nodes „Forever.“

Anforderung zum Löschen des Clients

Ausgestellt am 2024-03-31.

Ergebnis

StorageGRID wird die Objektversion nicht löschen, da die Aufbewahrung bis zum Datum noch zwei Jahre entfernt ist.

So werden Objekte gelöscht

StorageGRID kann Objekte entweder als direkte Antwort auf eine Client-Anfrage oder automatisch aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus oder der Anforderungen der ILM-Richtlinie löschen. Wenn Sie verstehen, auf welche Weise Objekte gelöscht werden können und wie StorageGRID Löschanfragen verarbeitet, können Sie Objekte effizienter managen.

StorageGRID kann Objekte auf eine von zwei Methoden löschen:

- Synchrones Löschen: Erhält StorageGRID eine Client-Löschanforderung, werden alle Objektkopien sofort entfernt. Der Client wird informiert, dass das Löschen nach dem Entfernen der Kopien erfolgreich war.
- Objekte werden zum Löschen in die Warteschlange eingereiht: Wenn StorageGRID eine Löschanforderung empfängt, wird das Objekt zum Löschen in die Warteschlange verschoben. Der Client wird umgehend darüber informiert, dass das Löschen erfolgreich war. Objektkopien werden später durch ILM-Verarbeitung im Hintergrund entfernt.

Beim Löschen von Objekten verwendet StorageGRID die Methode, die das Löschen der Performance optimiert, mögliche Rückprotokolle für das Löschen minimiert und Speicherplatz am schnellsten freigegeben wird.

Die Tabelle fasst zusammen, wann StorageGRID die einzelnen Methoden verwendet.

Löschmethode	Wenn verwendet
Objekte werden zum Löschen in eine Warteschlange eingereiht	<p>Wenn eine der folgenden Bedingungen zutrifft:</p> <ul style="list-style-type: none"> • Das automatische Löschen von Objekten wurde von einem der folgenden Ereignisse ausgelöst: <ul style="list-style-type: none"> ◦ Das Ablaufdatum oder die Anzahl der Tage in der Lebenszykluskonfiguration für einen S3-Bucket erreicht ist. ◦ Der letzte in einer ILM-Regel angegebene Zeitraum ist abgelaufen. <p>Hinweis: Objekte in einem Bucket, für den S3 Object Lock aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einem Legal Hold befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.</p> <ul style="list-style-type: none"> • Ein S3- oder Swift-Client fordert eine Löschung an. Eine oder mehrere der folgenden Bedingungen gilt: <ul style="list-style-type: none"> ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, da z. B. ein Objektspeicherort vorübergehend nicht verfügbar ist. ◦ Löschwarteschlangen im Hintergrund sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	<p>Wenn ein S3- oder Swift-Client eine Löschanfrage erstellt und alle der folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Warteschlangen zum Löschen im Hintergrund enthalten Objekte, die verarbeitet werden sollen.

Wenn S3- oder Swift-Clients Löschanforderungen durchführen, beginnt StorageGRID, indem Objekte der Löschwarteschlange hinzugefügt werden. Anschließend wechselt er zur Durchführung des synchronen Löschvorgangs. Wenn sichergestellt wird, dass in der Warteschlange zum Löschen im Hintergrund Objekte verarbeitet werden, kann StorageGRID das Löschen von Löschungen effizienter verarbeiten, insbesondere bei Clients mit geringer Parallelität. Gleichzeitig wird verhindert, dass die Backlogs von Clients gelöscht werden.

Erforderliche Zeit zum Löschen von Objekten

Die Art und Weise, wie StorageGRID Objekte löscht, kann sich auf die Ausführung des Systems auswirken:

- Wenn StorageGRID das synchrone Löschen durchführt, kann StorageGRID bis zu 30 Sekunden dauern, bis ein Ergebnis an den Client zurückgegeben wird. Das heißt, das Löschen kann scheinbar langsamer erfolgen, auch wenn Kopien tatsächlich schneller entfernt werden als wenn StorageGRID Objekte zum Löschen Warteschlangen.
- Falls Sie die Löschrategie während eines Massenslöschs genau überwachen, kann es vorkommen, dass sich die Löschrategie nach dem Löschen einer bestimmten Anzahl von Objekten verlangsamt. Diese Änderung tritt auf, wenn StorageGRID von Objekten aus der Warteschlange zum Löschen auf das synchrone Löschen verschiebt. Die offensichtliche Reduzierung der Löschrategie bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil: Er zeigt an, dass durchschnittlich Speicherplatz schneller freigegeben wird.

Wenn Sie eine große Anzahl von Objekten löschen und Ihre Priorität darin besteht, Speicherplatz schnell freizugeben, ziehen Sie in Betracht, Objekte mithilfe einer Client-Anfrage zu löschen, anstatt sie mit ILM oder anderen Methoden zu löschen. Im Allgemeinen wird Speicherplatz schneller freigegeben, wenn das Löschen durch Clients durchgeführt wird, da StorageGRID das synchrone Löschen verwenden kann.

Die Zeit, die erforderlich ist, um nach dem Löschen eines Objekts Speicherplatz freizugeben, hängt von mehreren Faktoren ab:

- Gibt an, ob Objektkopien synchron entfernt werden oder später zur Entfernung in die Warteschlange verschoben werden (für Client-Löschanfragen).
- Weitere Faktoren wie die Anzahl der Objekte im Grid oder die Verfügbarkeit von Grid-Ressourcen, wenn Objektkopien zur Entfernung in eine Warteschlange verschoben werden (für Clientlöschanfragen und andere Methoden).

Löschen von S3-versionierten Objekten

Wenn die Versionierung für einen S3-Bucket aktiviert ist, befolgt StorageGRID das Verhalten von Amazon S3, wenn es auf Löschanfragen reagiert, unabhängig davon, ob diese Anfragen von einem S3-Client, dem Ablauf eines S3-Bucket-Lebenszyklus oder den Anforderungen der ILM-Richtlinie stammen.

Wenn Objekte versioniert sind, löschen Objekt-Löschanforderungen nicht die aktuelle Version des Objekts und geben keinen Speicherplatz frei. Stattdessen erzeugt eine Anfrage zum Löschen eines Objekts eine Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts „noncurrent“ wird.

Auch wenn das Objekt nicht entfernt wurde, verhält sich StorageGRID so, als ob die aktuelle Version des Objekts nicht mehr verfügbar ist. Anfragen an dieses Objekt geben 404 nicht gefunden zurück. Da jedoch nicht aktuelle Objektdaten nicht entfernt wurden, können Anforderungen, die eine nicht aktuelle Version des Objekts angeben, erfolgreich ausgeführt werden.

Um beim Löschen versionierter Objekte Speicherplatz freizugeben, verwenden Sie eine der folgenden Optionen:

- **S3 Client Request:** Geben Sie die Objektversion-ID in der S3 DELETE Object Anfrage an (DELETE /object?versionId=ID). Beachten Sie, dass diese Anforderung nur Objektkopien für die angegebene Version entfernt (die anderen Versionen belegen noch Speicherplatz).
- **Bucket-Lebenszyklus:** Verwenden Sie das NoncurrentVersionExpiration Aktionen in der Bucket-Lifecycle-Konfiguration Wenn die angegebene Anzahl von nicht-currentDays erreicht ist, entfernt StorageGRID dauerhaft alle Kopien nicht aktueller Objektversionen. Diese Objektversionen können nicht wiederhergestellt werden.

Der `NewerNoncurrentVersions` Durch die Aktion in der Bucket-Lebenszykluskonfiguration wird die Anzahl der nicht-aktuellen Versionen angegeben, die in einem versionierten S3-Bucket aufbewahrt wurden. Wenn mehr nicht aktuelle Versionen als vorhanden sind `NewerNoncurrentVersions` Gibt an, dass StorageGRID die älteren Versionen entfernt, sobald der Wert „nicht-currentDays“ abgelaufen ist. Der `NewerNoncurrentVersions` Schwellenwert überschreibt Lebenszyklusregeln, die von ILM bereitgestellt werden. Das bedeutet, dass ein nicht aktuelles Objekt mit einer Version im vorliegt `NewerNoncurrentVersions` Der Schwellenwert wird beibehalten, wenn ILM die Löschung anfordert.

- **ILM: "Klont die aktive Richtlinie"** Und fügen Sie der neuen vorgeschlagenen Richtlinie zwei ILM-Regeln hinzu:
 - Erste Regel: Verwenden Sie "nicht aktuelle Zeit" als Referenzzeit, um mit den nicht aktuellen Versionen des Objekts zu übereinstimmen. In ["Schritt 1 \(Details eingeben\) des Assistenten zum Erstellen einer](#)

ILM-Regel", Wählen Sie **Ja** für die Frage "Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?"

- Zweite Regel: Verwenden Sie **Ingest time**, um die aktuelle Version anzupassen. Die Regel „Noncurrent time“ muss in der Richtlinie über der Regel **Ingest Time** angezeigt werden.

Löschen von S3-Löschmarkierungen

Wenn ein versioniertes Objekt gelöscht wird, erstellt StorageGRID als aktuelle Version des Objekts eine Löschmarkierung. Um die Null-Byte-Löschmarkierung aus dem Bucket zu entfernen, muss der S3-Client die Objektversion explizit löschen. Löschmarkierungen werden nicht durch ILM, Bucket-Lebenszyklusregeln oder Objekte in Bucket-Operationen gelöscht.

Verwandte Informationen

- ["S3-REST-API VERWENDEN"](#)
- ["Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"](#)

Speicherklassen erstellen und zuweisen

Speicherklassen identifizieren den Speichertyp, der von einem Speicherknoten verwendet wird. Sie können Storage-Klassen erstellen, wenn ILM-Regeln bestimmte Objekte auf bestimmten Storage-Nodes platzieren sollen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Sie StorageGRID zum ersten Mal installieren, wird die Speicherklasse **Default** automatisch jedem Speicherknoten in Ihrem System zugewiesen. Nach Bedarf können Sie optional benutzerdefinierte Storage-Klassen definieren und sie verschiedenen Storage-Nodes zuweisen.

Mit benutzerdefinierten Speicherqualitäten können Sie ILM-Speicherpools erstellen, die nur einen bestimmten Typ von Speicher-Node enthalten. Möglicherweise möchten Sie beispielsweise bestimmte Objekte auf Ihren schnellsten Storage-Nodes wie z. B. StorageGRID All-Flash Storage Appliances speichern.

Wenn es nicht um die Speichergüte geht (zum Beispiel sind alle Speicher-Nodes identisch), können Sie dieses Verfahren überspringen und die Auswahl **includes all Storage Grade** für die Speicherklasse verwenden, wenn Sie ["Erstellen von Speicherpools"](#). Mit dieser Auswahl wird sichergestellt, dass der Speicherpool jeden Storage Node am Standort umfasst, unabhängig von seiner Speicherklasse.



Erstellen Sie nicht mehr Storage-Klassen als erforderlich. Erstellen Sie beispielsweise keine Storage-Klasse für jeden Storage-Node. Weisen Sie jede Storage-Klasse zwei oder mehr Nodes zu. Storage-Klassen, die nur einem Node zugewiesen sind, können ILM-Backlogs verursachen, wenn der Node nicht mehr verfügbar ist.

Schritte

1. Wählen Sie **ILM > Speicherklassen**.
2. Benutzerdefinierte Storage-Klassen definieren:
 - a. Wählen Sie für jede benutzerdefinierte Speicherklasse, die Sie hinzufügen möchten, **Einfügen aus**

b. Geben Sie eine beschreibende Bezeichnung ein.

 **Storage Grades**
Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	<input type="text" value="disk"/>	 

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes 

c. Wählen Sie **Änderungen Anwenden**.

d. Wenn Sie ein gespeichertes Label ändern möchten, wählen Sie optional **Bearbeiten**  Und wählen Sie **Änderungen übernehmen**.



Speicherqualitäten können nicht gelöscht werden.

3. Storage-Nodes neue Storage-Klassen zuweisen:

a. Suchen Sie den Storage Node in der LDR-Liste, und wählen Sie dessen Symbol * Bearbeiten* aus .

b. Wählen Sie den entsprechenden Speichergrad aus der Liste aus.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Weisen Sie einem bestimmten Speicherknoten nur einmal eine Speicherklasse zu. Bei einem nach einem Ausfall wiederhergestellten Storage-Node wird die zuvor zugewiesene Storage-Klasse erhalten. Ändern Sie diese Zuweisung nicht, nachdem die ILM-Richtlinie aktiviert wurde. Wenn die Zuweisung geändert wird, werden die Daten auf Basis der neuen Speicherklasse gespeichert.

- a. Wählen Sie **Änderungen Anwenden**.

Nutzung von Speicherpools

Was ist ein Speicherpool?

Ein Speicherpool ist eine logische Gruppierung von Storage-Nodes oder Archiv-Nodes.

Bei der Installation von StorageGRID wird automatisch ein Speicherpool pro Standort erstellt. Sie können zusätzliche Speicherpools je nach Bedarf konfigurieren.



Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Siehe "[Verwendung Von Cloud Storage Pools](#)".

Storage-Pools haben zwei Attribute:

- **Speicherklasse:** Für Storage-Nodes, die relative Performance beim Sichern von Speicher.
- **Standort:** Das Rechenzentrum, in dem Objekte gespeichert werden.

Storage-Pools werden in ILM-Regeln verwendet, um zu bestimmen, wo Objektdaten gespeichert werden und welcher Storage-Typ verwendet wird. Wenn Sie ILM-Regeln für die Replikation konfigurieren, wählen Sie einen oder mehrere Storage-Pools aus, die entweder Storage-Nodes oder Archiv-Nodes enthalten. Wenn Sie Profile

für das Erasure Coding erstellen, wählen Sie einen Storage-Pool aus, der Storage-Nodes umfasst.

Richtlinien zur Erstellung von Speicherpools

Konfiguration und Verwendung von Speicherpools zur Absicherung gegen Datenverluste durch Verteilung von Daten über mehrere Standorte hinweg Für replizierte Kopien und Kopien, die zur Fehlerkorrektur codiert wurden, sind unterschiedliche Konfigurationen von Storage-Pools erforderlich.

Siehe "[Beispiele für den Schutz vor Standortausfällen durch Replikation und Erasure Coding](#)".

Richtlinien für alle Speicherpools

- Halten Sie Storage-Pool-Konfigurationen so einfach wie möglich. Erstellen Sie nicht mehr Speicherpools als nötig.
- Erstellung von Storage-Pools mit so vielen Nodes wie möglich Jeder Storage-Pool sollte zwei oder mehr Nodes enthalten. Ein Storage-Pool mit unzureichenden Nodes kann ILM-Backlogs verursachen, wenn ein Node nicht mehr verfügbar ist.
- Vermeiden Sie es, Storage-Pools zu erstellen oder zu verwenden, die sich überlappen (einen oder mehrere derselben Nodes enthalten). Bei Überschneidungen von Storage-Pools kann es sein, dass mehrere Kopien von Objektdaten auf demselben Node gespeichert werden.
- Verwenden Sie im Allgemeinen nicht den Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) oder den Standort Alle Standorte. Diese Elemente werden automatisch aktualisiert, um alle neuen Sites, die Sie einer Erweiterung hinzufügen, aufzunehmen, was möglicherweise nicht das gewünschte Verhalten ist.

Richtlinien für Storage-Pools, die für replizierte Kopien verwendet werden

- Zum Schutz vor Standortausfällen mit "[Replizierung](#)", Geben Sie einen oder mehrere standortspezifische Speicherpools im an "[Anweisungen zur Platzierung der einzelnen ILM-Regeln](#)".

Während der StorageGRID-Installation wird für jeden Standort automatisch ein Storage-Pool erstellt.

Durch die Verwendung eines Storage Pools für jeden Standort wird sichergestellt, dass replizierte Objektkopien genau an den erwarteten Ort platziert werden (z. B. eine Kopie jedes Objekts an jedem Standort zum Site-Loss-Schutz).

- Wenn Sie einer Erweiterung einen Standort hinzufügen, erstellen Sie einen neuen Speicherpool, der nur den neuen Standort enthält. Dann, "[Aktualisieren Sie die ILM-Regeln](#)" Um zu steuern, welche Objekte auf der neuen Site gespeichert werden.
- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Speicherpools, verteilt das System die Kopien, um die Festplattennutzung zwischen den Pools auszugleichen.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Sie müssen sicherstellen, dass die ausgewählten Speicherpools nicht dieselben Speicher-Nodes enthalten.

Richtlinien für Storage-Pools, die für Kopien mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verwendet werden

- Zum Schutz vor Standortausfällen mit "[Erasure Coding](#)" Erstellen Sie Speicherpools, die aus mindestens drei Standorten bestehen. Wenn ein Storage-Pool nur zwei Standorte umfasst, kann dieser Storage-Pool nicht für Erasure Coding verwendet werden. Für einen Speicherpool mit zwei Standorten stehen keine

Erase Coding-Schemata zur Verfügung.

- Die Anzahl der im Speicherpool enthaltenen Storage-Nodes und -Standorte bestimmt, welche ["Erase Coding-Schemata"](#) Verfügbar sind.
- Wenn möglich, sollte ein Speicherpool mehr als die Mindestanzahl an Speicherknoten enthalten, die für das ausgewählte Erasure-Coding-Schema erforderlich ist. Wenn Sie beispielsweise ein 6+3-Schema zur Codierung von Lösungsverfahren verwenden, müssen Sie mindestens neun Storage-Nodes haben. Es wird jedoch empfohlen, mindestens einen zusätzlichen Storage-Node pro Standort zu haben.
- Verteilen Sie Storage Nodes so gleichmäßig wie möglich auf Standorte. Um beispielsweise ein 6+3 Erasure Coding-Schema zu unterstützen, konfigurieren Sie einen Storage-Pool, der mindestens drei Storage-Nodes an drei Standorten enthält.
- Wenn Sie hohe Durchsatzanforderungen haben, wird die Verwendung eines Speicherpools mit mehreren Standorten nicht empfohlen, wenn die Netzwerklatenz zwischen Standorten mehr als 100 ms beträgt. Mit steigender Latenz sinkt auch die Rate, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des geringeren TCP-Netzwerkdurchsatzes erheblich.

Der Rückgang des Durchsatzes wirkt sich auf die maximal erreichbaren Raten bei der Aufnahme und dem Abruf von Objekten aus (wenn Balance oder Strict als Aufnahmeverhalten ausgewählt werden) oder kann zu ILM-Warteschlangen-Backlogs führen (wenn Dual Commit als Aufnahmeverhalten ausgewählt wird). Siehe ["ILM-Regel Aufnahme-Verhalten"](#).



Wenn Ihr Grid nur einen Standort umfasst, können Sie den Speicherpool Alle Storage-Nodes (StorageGRID 11.6 und früher) oder den Standardstandort aller Standorte in einem Erasure Coding-Profil nicht verwenden. Dieses Verhalten verhindert, dass das Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.

- Archivierungs-Nodes können nicht für Daten verwendet werden, die nach der Datenlöschung codiert wurden.

Richtlinien für Speicherpools, die für archivierte Kopien verwendet werden



Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Siehe ["Migrieren von Objekten in einen Cloud-Storage-Pool"](#).

Darüber hinaus sollten Sie Archivknoten aus der aktiven ILM-Richtlinie in StorageGRID 11.7 oder früher entfernen. Das Entfernen von Objektdaten, die auf Archive Nodes gespeichert sind, vereinfacht zukünftige Upgrades. Siehe ["Arbeiten mit ILM-Regeln und ILM-Richtlinien"](#).

- Sie können keinen Speicherpool erstellen, der sowohl Storage-Nodes als auch Archive Nodes umfasst. Für archivierte Kopien ist ein Storage-Pool erforderlich, der nur Archiv-Nodes enthält.
- Wenn Sie einen Speicherpool verwenden, der Archivierungs-Nodes enthält, sollten Sie außerdem mindestens eine replizierte oder mit Erasure Coding versehende Kopie in einem Speicherpool mit Storage-Nodes verwalten.
- Wenn die globale S3-Objektsperre aktiviert ist und Sie eine konforme ILM-Regel erstellen, können Sie keinen Speicherpool verwenden, der Archive Nodes umfasst. Anweisungen zum Verwalten von Objekten mit S3 Object Lock finden Sie in den Anleitungen.
- Wenn der Zieltyp eines Archiv-Node Cloud Tiering - Simple Storage Service (S3) lautet, muss sich der Archiv-Node im eigenen Storage-Pool befinden.

Schutz vor Standortausfällen

Wenn die Implementierung von StorageGRID mehrere Standorte umfasst, können Sie für den Schutz vor Standortausfällen Replizierung und Erasure Coding mit entsprechend konfigurierten Storage-Pools verwenden.

Für Replizierung und Erasure Coding sind unterschiedliche Storage-Pool-Konfigurationen erforderlich:

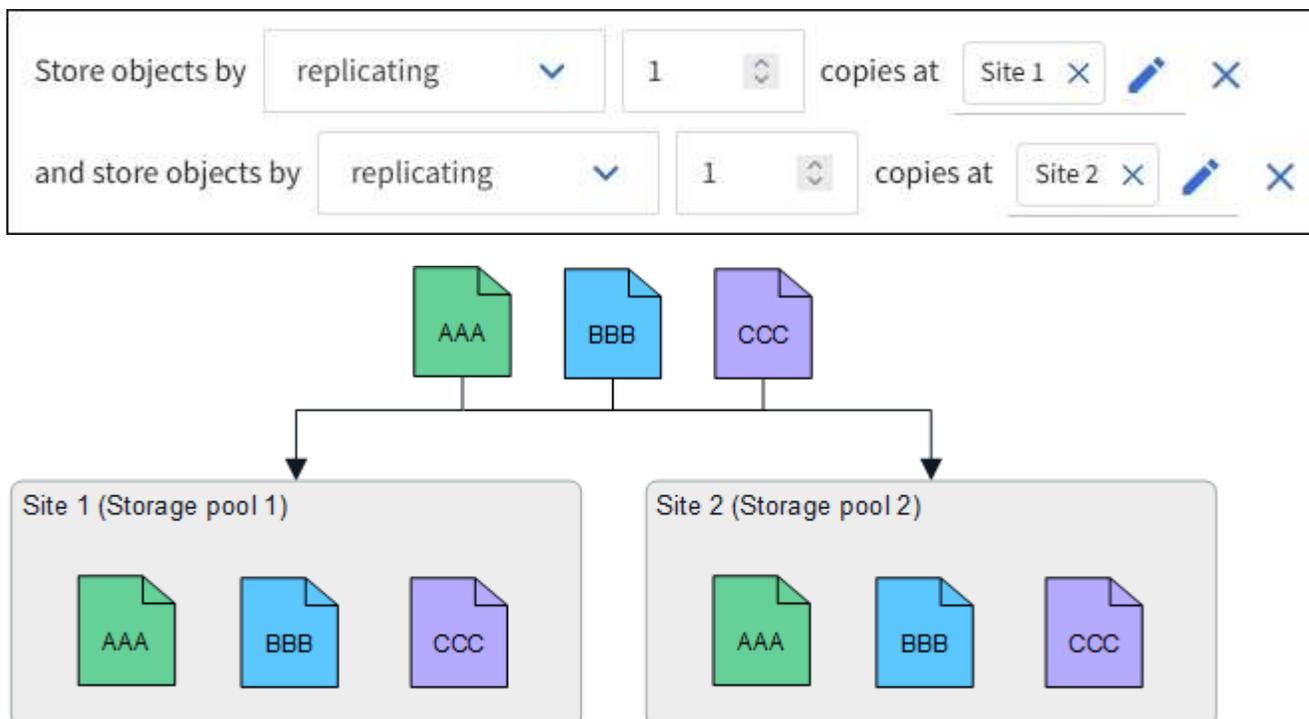
- Um die Replikation zum Schutz vor Standortausfällen zu verwenden, verwenden Sie die standortspezifischen Speicherpools, die bei der StorageGRID-Installation automatisch erstellt werden. Erstellen Sie dann ILM-Regeln mit ["Anweisungen zur Platzierung"](#) Die mehrere Speicherpools angeben, sodass eine Kopie jedes Objekts an jedem Standort platziert wird.
- Um Erasure Coding für Site-Loss-Schutz zu verwenden, ["Erstellen Sie Speicherpools, die aus mehreren Standorten bestehen"](#). Erstellen Sie dann ILM-Regeln, die einen Storage-Pool verwenden, der aus mehreren Standorten und einem beliebigen verfügbaren Erasure-Coding-Schema besteht.

Beispiel für die Replikation

Standardmäßig wird während der StorageGRID-Installation ein Speicherpool für jeden Standort erstellt. Wenn Speicherpools nur aus einem Standort bestehen, können Sie ILM-Regeln konfigurieren, die die Replikation für den Schutz vor Standortausfällen verwenden. In diesem Beispiel:

- Speicherpool 1 enthält Standort 1
- Speicherpool 2 enthält Standort 2
- Die ILM-Regel enthält zwei Platzierungen:
 - Speichern Sie Objekte, indem Sie 1 Kopie an Standort 1 replizieren
 - Speichern Sie Objekte, indem Sie 1 Kopie an Standort 2 replizieren

ILM-Regelplatzierungen:



Wenn ein Standort verloren geht, sind Kopien der Objekte am anderen Standort verfügbar.

Beispiel für Erasure Coding

Wenn Storage-Pools aus mehr als einem Standort pro Storage-Pool bestehen, können Sie ILM-Regeln konfigurieren, die Erasure Coding für Site-Loss-Schutz verwenden. In diesem Beispiel:

- Speicherpool 1 enthält die Standorte 1 bis 3
- Die ILM-Regel enthält eine Platzierung: Speichern Sie Objekte mithilfe eines Erasure Coding mithilfe eines 4+2 EC-Schemas in Storage Pool 1, das drei Standorte enthält

ILM-Regelplatzierungen:



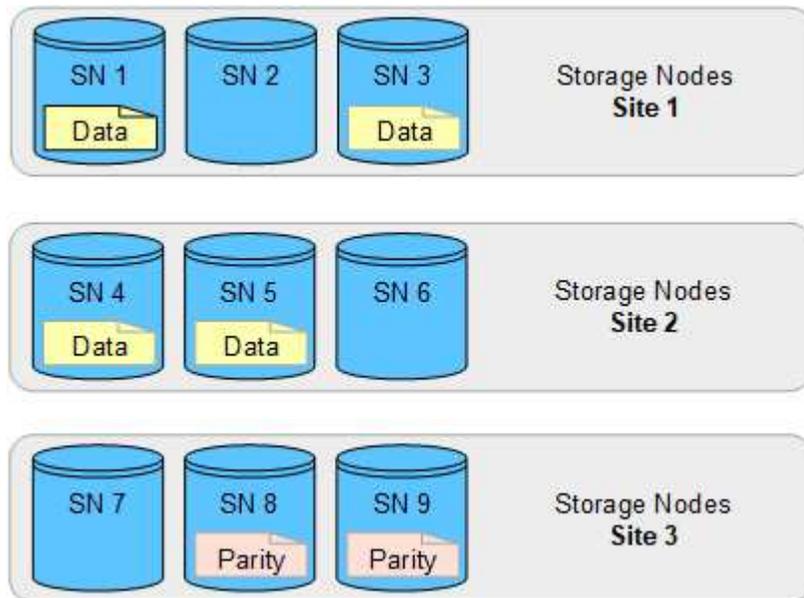
In diesem Beispiel:

- Die ILM-Regel verwendet ein 4+2 Erasure Coding-Schema.
- Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet.
- Jedes der sechs Fragmente wird auf einem anderen Node über drei Datacenter-Standorte gespeichert, um Daten bei Node-Ausfällen oder Standortausfällen zu sichern.

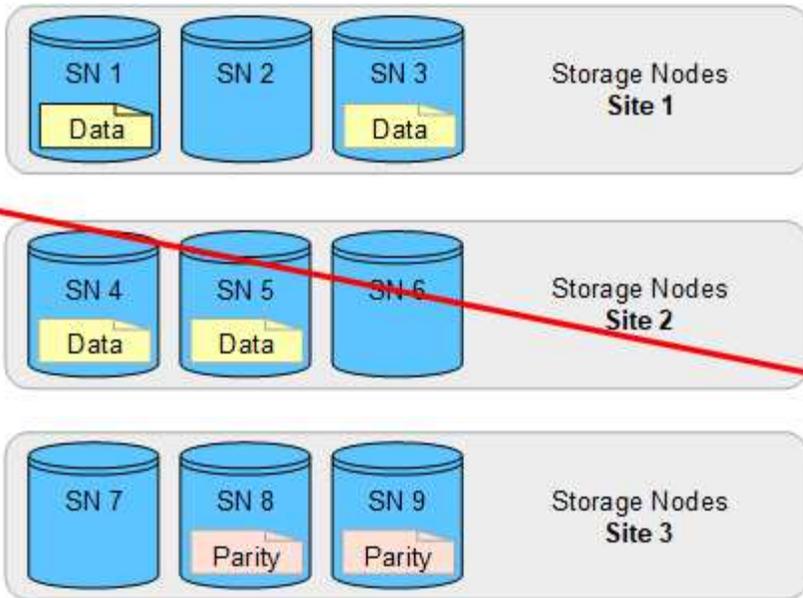


Erasure Coding ist in Speicherpools erlaubt, die eine beliebige Anzahl von Standorten mit Ausnahme von zwei Standorten enthalten.

ILM-Regel gemäß 4+2 Erasure-Coding-Schema:



Wenn ein Standort verloren geht, können die Daten immer noch wiederhergestellt werden:



Erstellen Sie einen Speicherpool

Sie erstellen Storage-Pools, um zu bestimmen, wo das StorageGRID-System Objektdaten und den verwendeten Storage-Typ speichert. Jeder Speicherpool umfasst einen oder mehrere Standorte und eine oder mehrere Speicherklassen.



Bei der Installation von StorageGRID 11.7 in einem neuen Grid werden automatisch Storage-Pools für jeden Standort erstellt, um die Anzahl der zum Erstellen neuer ILM-Regeln erforderlichen Schritte zu verringern. Bei der Aktualisierung auf StorageGRID 11.7 werden jedoch keine Speicherpools für jeden Standort erstellt.

Wenn Sie Cloud-Speicherpools erstellen möchten, um Objektdaten außerhalb Ihres StorageGRID-Systems zu speichern, finden Sie Informationen im ["Informationen zur Verwendung von Cloud Storage Pools"](#).

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die Richtlinien zum Erstellen von Speicherpools überprüft.

Über diese Aufgabe

Storage Pools legen fest, wo Objektdaten gespeichert sind. Die Anzahl der erforderlichen Storage-Pools hängt von der Anzahl der Standorte in Ihrem Grid und den gewünschten Kopien ab: Repliziert oder Erasure Coding.

- Für Replizierung und Erasure Coding für einen Standort erstellen Sie für jeden Standort einen Storage-Pool. Wenn Sie beispielsweise replizierte Objektkopien an drei Standorten speichern möchten, erstellen Sie drei Storage Pools.
- Erstellen Sie für das Erasure Coding an drei oder mehr Standorten einen Storage-Pool mit einem Eintrag für jeden Standort. Wenn Sie beispielsweise Objekte aus drei Standorten löschen möchten, erstellen Sie einen Speicherpool.



Schließen Sie den Standort Alle Standorte nicht in einen Speicherpool ein, der in einem Erasure Coding-Profil verwendet wird. Fügen Sie stattdessen für jeden Standort, der Daten mit dem Erasure Coding speichert, einen separaten Eintrag in den Storage-Pool ein. Siehe [Diesem Schritt](#) Beispiel:

- Wenn Sie mehr als eine Storage-Klasse verwenden, sollten Sie an einem einzelnen Standort keinen Storage-Pool erstellen, der verschiedene Storage-Klassen umfasst. Siehe "[Richtlinien zur Erstellung von Speicherpools](#)".

Schritte

1. Wählen Sie **ILM > Storage Pools** aus.

Auf der Registerkarte Speicherpools werden alle definierten Speicherpools aufgeführt.



Bei Neuinstallationen von StorageGRID 11.6 oder früher wird der Speicherpool Alle Speicherknoten automatisch aktualisiert, sobald Sie neue Rechenzentrumsstandorte hinzufügen. Verwenden Sie diesen Pool nicht in ILM-Regeln.

2. Um einen neuen Speicherpool zu erstellen, wählen Sie **Erstellen**.
3. Geben Sie einen eindeutigen Namen für den Speicherpool ein. Verwenden Sie einen Namen, der sich leicht identifizieren lässt, wenn Sie Profile für das Erasure Coding und ILM-Regeln konfigurieren.
4. Wählen Sie aus der Dropdown-Liste **Standort** einen Standort für diesen Speicherpool aus.

Wenn Sie einen Standort auswählen, wird die Anzahl der Speicherknoten und Archivknoten in der Tabelle automatisch aktualisiert.

Im Allgemeinen sollten Sie den Standort „Alle Standorte“ nicht in einem Speicherpool verwenden. ILM-Regeln, die einen Storage-Pool an allen Standorten verwenden, platzieren Objekte an jedem beliebigen verfügbaren Standort, wodurch Sie weniger Kontrolle über die Objektplatzierung haben. Außerdem verwendet ein Speicherpool für alle Standorte sofort die Speicherknoten an einem neuen Standort, was möglicherweise nicht das erwartete Verhalten ist.

5. Wählen Sie aus der Dropdown-Liste **Speichergrad** den Speichertyp aus, der verwendet werden soll, wenn eine ILM-Regel diesen Speicherpool verwendet.

Die Speicherklasse umfasst alle Storage-Klassen und umfasst alle Storage-Nodes am ausgewählten Standort. Die Standard-Speicherklasse Archiv-Knoten umfasst alle Archiv-Knoten am ausgewählten Standort. Wenn Sie zusätzliche Speicherklassen für die Speicherknoten in Ihrem Raster erstellt haben, werden diese im Dropdown-Menü aufgelistet.

6. Wenn Sie den Speicherpool in einem Profil für die Kennzeichnung von Löschvorgängen mit mehreren Standorten verwenden möchten, wählen Sie **Weitere Knoten hinzufügen**, um dem Speicherpool einen Eintrag für jeden Standort hinzuzufügen.



Sie können keine doppelten Einträge erstellen oder einen Speicherpool erstellen, der sowohl die Speicherklasse Archive Nodes als auch jede Speicherklasse mit Speicherknoten umfasst.

Sie werden gewarnt, wenn Sie mehr als einen Eintrag mit unterschiedlichen Speicherqualitäten für einen Standort hinzufügen.

Um einen Eintrag zu entfernen, wählen Sie das Löschsymboll .

7. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie **Speichern**.

Der neue Speicherpool wird der Liste hinzugefügt.

Zeigen Sie Details zum Speicherpool an

Sie können die Details eines Speicherpools anzeigen, um zu bestimmen, wo der Speicherpool verwendet wird, und um zu sehen, welche Nodes und Speicherklassen enthalten sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **ILM > Storage Pools** aus.

Die Tabelle Speicherpools enthält die folgenden Informationen für jeden Speicherpool, der Speicher-Nodes umfasst:

- **Name:** Der eindeutige Anzeigename des Speicherpools.
- **Knotenanzahl:** Die Anzahl der Knoten im Speicherpool.
- **Speichernutzung:** Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten auf diesem Knoten verwendet wurde. Dieser Wert enthält keine Objektmetadaten.
- **Gesamtkapazität:** Die Größe des Speicherpools, die der Gesamtmenge des nutzbaren Speicherplatzes für Objektdaten für alle Knoten im Speicherpool entspricht.
- **ILM-Nutzung:** Wie der Speicherpool derzeit genutzt wird. Ein Storage-Pool wird möglicherweise nicht verwendet oder kann in einem oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beiden verwendet werden.



Ein Speicherpool kann nicht entfernt werden, wenn er verwendet wird.

2. Um Details zu einem bestimmten Speicherpool anzuzeigen, wählen Sie dessen Namen aus.

Die Detailseite für den Speicherpool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Nodes** an, um mehr über die im Speicherpool enthaltenen Speicher-Nodes oder Archiv-Nodes zu erfahren.

Die Tabelle enthält die folgenden Informationen für jeden Node:

- Node-Name
- Standortname
- Storage-Klasse
- Speichernutzung (%): Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der für den Speicher-Node verwendet wurde. Dieses Feld ist für Archive Node Pools nicht sichtbar.



Der gleiche Wert für die Speichernutzung (%) wird auch im Diagramm Speicher verwendet - Objektdaten für jeden Speicherknoten angezeigt (wählen Sie **NODES > Storage Node > Storage**).

4. Wählen Sie die Registerkarte **ILM-Nutzung** aus, um zu ermitteln, ob der Speicherpool derzeit in ILM-Regeln oder Erasure Coding-Profilen verwendet wird.
5. Optional können Sie auf der Seite **ILM-Regeln** weitere Informationen zu den Regeln erhalten, die den Speicherpool verwenden.

Siehe "[Anweisungen zum Arbeiten mit ILM-Regeln](#)".

Speicherpool bearbeiten

Sie können einen Speicherpool bearbeiten, um seinen Namen zu ändern oder Standorte und Speicherklassen zu aktualisieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die geprüft "[Richtlinien für die Erstellung von Speicherpools](#)".
- Wenn Sie einen Speicherpool bearbeiten möchten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, haben Sie überlegt, wie sich Ihre Änderungen auf die Platzierung von Objektdaten auswirken.

Über diese Aufgabe

Wenn Sie einen neuen Standort oder eine Speicherklasse zu einem Speicherpool hinzufügen, der in der aktiven ILM-Richtlinie verwendet wird, beachten Sie, dass die Speicherknoten am neuen Standort oder der Speicherklasse nicht automatisch verwendet werden. Um StorageGRID zu zwingen, einen neuen Standort oder eine neue Speicherklasse zu verwenden, müssen Sie eine neue ILM-Richtlinie aktivieren, nachdem Sie den bearbeiteten Speicherpool gespeichert haben.

Schritte

1. Wählen Sie **ILM > Storage Pools** aus.
2. Aktivieren Sie das Kontrollkästchen für den Speicherpool, den Sie bearbeiten möchten.

Der Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) kann nicht bearbeitet werden.

3. Wählen Sie **Bearbeiten**.
4. Ändern Sie bei Bedarf den Namen des Speicherpools.
5. Wählen Sie bei Bedarf andere Standorte und Lagersorten aus.



Sie können den Standort oder die Storage-Klasse nicht ändern, wenn der Speicherpool in einem Erasure Coding-Profil verwendet wird und die Änderung dazu führen würde, dass das Erasure Coding-Schema ungültig wird. Wenn beispielsweise ein Storage-Pool in einem Profil für Erasure Coding derzeit eine Storage-Klasse mit nur einem Standort umfasst, können Sie eine Storage-Klasse mit zwei Standorten nicht verwenden, da die Änderung das Erasure Coding-Schema ungültig machen würde.

6. Wählen Sie **Speichern**.

Nachdem Sie fertig sind

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, einen neuen Standort oder eine neue Storage-Klasse hinzugefügt haben, aktivieren Sie eine neue ILM-Richtlinie, um StorageGRID zu zwingen, den neuen Standort oder die neue Storage-Klasse zu verwenden. Klonen Sie beispielsweise Ihre vorhandene ILM-Richtlinie und aktivieren Sie dann den Klon. Siehe "[Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien](#)".

Entfernen Sie einen Speicherpool

Sie können einen Speicherpool entfernen, der nicht verwendet wird.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Erforderliche Zugriffsberechtigungen](#)".

Schritte

1. Wählen Sie **ILM > Storage Pools** aus.
2. Überprüfen Sie in der Spalte ILM-Nutzung in der Tabelle, ob Sie den Speicherpool entfernen können.

Sie können einen Storage-Pool nicht entfernen, wenn er in einer ILM-Regel oder in einem Erasure Coding-Profil verwendet wird. Wählen Sie bei Bedarf **Storage Pool Name > ILM usage**, um zu bestimmen, wo der Speicherpool verwendet wird.

3. Wenn der Speicherpool, den Sie entfernen möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen.
4. Wählen Sie **Entfernen**.
5. Wählen Sie **OK**.

Verwendung Von Cloud Storage Pools

Was ist ein Cloud-Storage-Pool?

In einem Cloud Storage Pool können Sie ILM verwenden, um Objektdaten aus Ihrem StorageGRID System zu verschieben. Beispielsweise können Sie selten genutzte Objekte auf kostengünstigeren Cloud-Storage verschieben, wie z. B. Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archiv-Zugriffs-Tier in Microsoft Azure Blob Storage. Alternativ möchten Sie auch ein Cloud-Backup von StorageGRID Objekten beibehalten, um die Disaster Recovery zu verbessern.

Aus einer ILM-Perspektive ähnelt ein Cloud-Storage-Pool einem Storage-Pool. Um Objekte an beiden Standorten zu speichern, wählen Sie den Pool aus, wenn Sie die Anweisungen zur Platzierung einer ILM-Regel erstellen. Während Storage-Pools jedoch aus Storage-Nodes oder Archiv-Nodes innerhalb des StorageGRID-Systems bestehen, besteht ein Cloud Storage Pool aus einem externen Bucket (S3) oder Container (Azure Blob-Storage).



Das Verschieben von Objekten von einem Archive Node über die S3-API in ein externes Archiv-Storage-System ist veraltet und wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten. Wenn Sie derzeit einen Archive Node mit der Option Cloud Tiering – Simple Storage Service (S3) verwenden, "[Migrieren Sie Ihre Objekte in einen Cloud-Storage-Pool](#)" Stattdessen.

Die Tabelle vergleicht Speicherpools mit Cloud-Speicherpools und zeigt die grundlegenden Ähnlichkeiten und Unterschiede.

	Storage-Pool	Cloud-Storage-Pool
Wie wird sie erstellt?	Verwenden der Option ILM > Storage Pools im Grid Manager.	Verwenden der Option ILM > Speicherpools > Cloud-Speicherpools im Grid Manager. Sie müssen den externen Bucket oder Container einrichten, bevor Sie den Cloud Storage-Pool erstellen können.
Wie viele Pools können Sie erstellen?	Unbegrenzt.	Bis zu 10.
Wo werden Objekte gespeichert ?	Auf einem oder mehreren Speicherknoten oder Archivknoten innerhalb von StorageGRID.	In Amazon S3 Bucket, Azure Blob Storage-Container oder Google Cloud, die außerhalb des StorageGRID-Systems sind Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist: <ul style="list-style-type: none">• Optional kann ein Bucket-Lebenszyklus konfiguriert werden, um Objekte auf kostengünstigen Langzeit-Storage wie Amazon S3 Glacier oder S3 Glacier Deep Archive zu verschieben. Das externe Storage-System muss die Glacier Storage-Klasse und die S3 POST Object Restore API unterstützen.• Sie können Cloud-Storage-Pools zur Verwendung mit AWS Commercial Cloud Services (C2S) erstellen, die die AWS Secret Region unterstützen. Wenn der Cloud-Storage-Pool ein Azure Blob-Storage-Container ist, überträgt StorageGRID das Objekt auf die Archiv-Tier. Hinweis: im Allgemeinen sollten Sie Azure Blob Storage-Lifecycle-Management nicht für den Container konfigurieren, der für einen Cloud-Speicherpool verwendet wird. Die Wiederherstellung VON OBJEKTEN NACH DER Objekt-WIEDERHERSTELLUNG im Cloud-Storage-Pool kann vom konfigurierten Lebenszyklus betroffen sein.
Welche Kontrollen steuern die Objektplatzierung?	Eine ILM-Regel in der aktiven ILM-Richtlinie.	Eine ILM-Regel in der aktiven ILM-Richtlinie.

	Storage-Pool	Cloud-Storage-Pool
Welche Datenschutz methode wird verwendet?	Replizierung oder Erasure Coding:	Replizierung:
Wie viele Kopien jedes Objekts sind erlaubt?	Mehrere:	Eine Kopie im Cloud-Storage-Pool und optional eine oder mehrere Kopien in StorageGRID. Hinweis: ein Objekt kann zu keinem Zeitpunkt in mehr als einem Cloud-Speicherpool gespeichert werden.
Worin liegen die Vorteile?	Objekte sind jederzeit schnell abrufbar.	Kostengünstiger Storage:
		Hinweis: FabricPool-Daten können nicht in Cloud-Speicherpools verschoben werden. Objekte mit aktivierter S3-Objektsperre können nicht in Cloud-Storage-Pools platziert werden.

Lebenszyklus eines Cloud-Storage-Pool-Objekts

Überprüfen Sie vor der Implementierung von Cloud-Storage-Pools den Lebenszyklus der Objekte, die in jedem Typ von Cloud-Storage-Pool gespeichert sind.

- [S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts](#)
- [Azure: Lebenszyklus eines Cloud-Storage-Pool-Objekts](#)

S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts

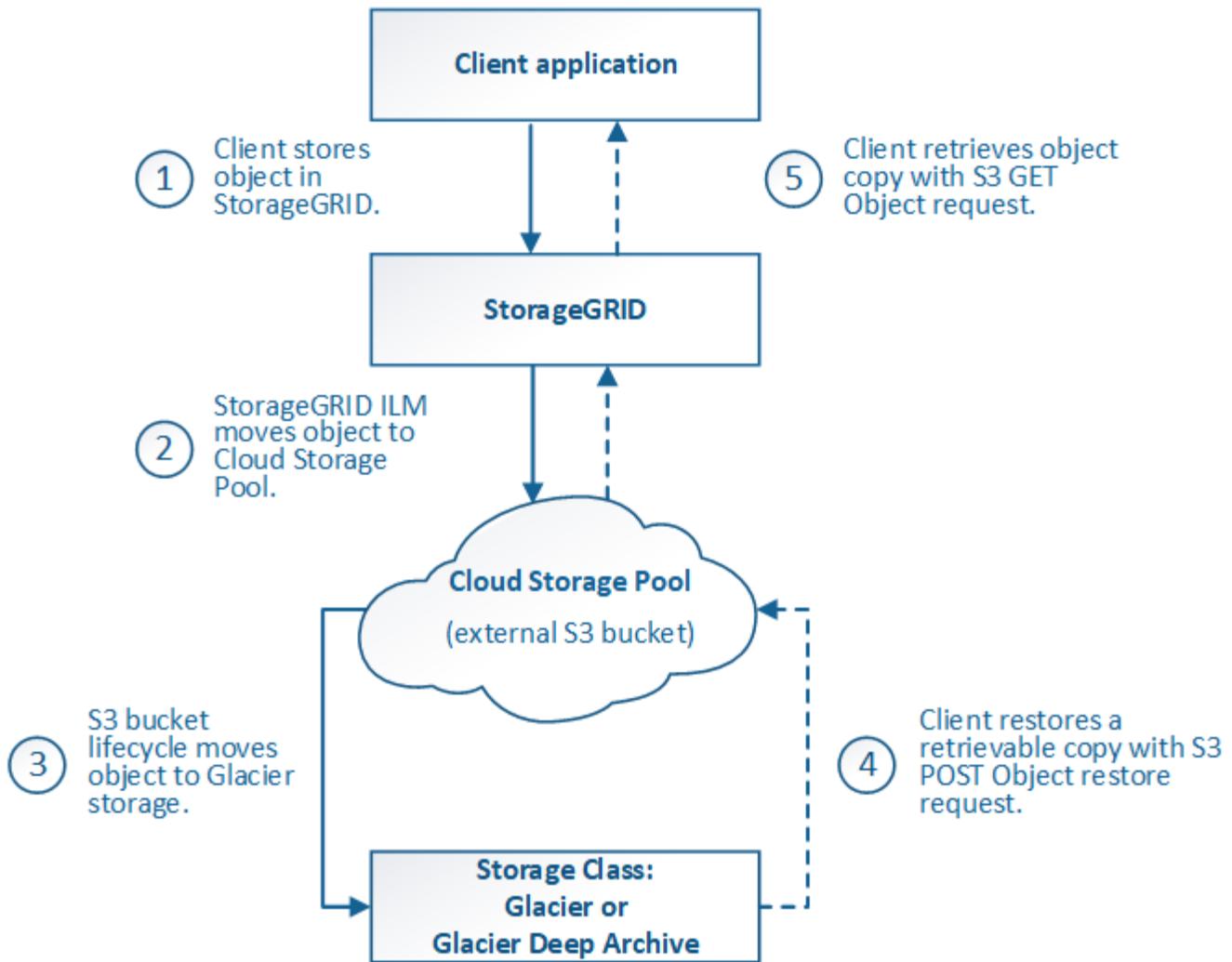
Die Abbildung zeigt die Lebenszyklusphasen eines Objekts, das in einem S3 Cloud-Storage-Pool gespeichert ist.



In der Abbildung und den Erläuterungen bezieht sich „Glacier“ sowohl auf die Glacier Storage-Klasse als auch auf die Glacier Deep Archive Storage-Klasse. Eine Ausnahme bilden die Glacier Deep Archive Storage-Klasse, die Expedited Restore Tier nicht unterstützt. Nur Bulk- oder Standard-Abruf wird unterstützt.



Die Google Cloud Platform (GCP) unterstützt den Abruf von Objekten aus langfristigem Storage ohne EINE WIEDERHERSTELLUNG NACH DER WIEDERHERSTELLUNG.



1. Objekt gespeichert in StorageGRID

Zum Starten des Lebenszyklus speichert eine Client-Applikation ein Objekt in StorageGRID.

2. Objekt in S3 Cloud Storage Pool verschoben

- Wenn das Objekt mit einer ILM-Regel übereinstimmt, die einen S3 Cloud-Storage-Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den vom Cloud-Storage-Pool angegebenen externen S3-Bucket.
- Sobald das Objekt in den S3-Cloud-Storage-Pool verschoben wurde, kann die Client-Applikation es mithilfe einer S3-GET-Objektanforderung von StorageGRID abrufen, es sei denn, das Objekt wurde auf Glacier Storage migriert.

3. Objekt ist auf Glacier umgestiegen (nicht-Retrieable-Zustand)

- Optional kann das Objekt auf Glacier Storage verschoben werden. Der externe S3-Bucket verwendet beispielsweise möglicherweise Lifecycle-Konfigurationen, um ein Objekt sofort oder nach einigen Tagen in Glacier Storage zu verschieben.



Wenn Sie Objekte verschieben möchten, müssen Sie eine Lebenszykluskonfiguration für den externen S3-Bucket erstellen. Außerdem ist eine Storage-Lösung erforderlich, die die Glacier Storage-Klasse implementiert und die S3-API FÜR DIE WIEDERHERSTELLUNG NACH Objekten unterstützt.



Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Wiederherstellungsanforderungen NACH dem Objekt, daher kann StorageGRID keine Swift Objekte abrufen, die auf S3 Glacier Storage verschoben wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

- Während des Übergangs kann die Client-Applikation mithilfe einer S3 HEAD Object-Anfrage den Status des Objekts überwachen.

4. Objekt vom Glacier-Speicher wiederhergestellt

Wenn ein Objekt in den Glacier Storage verschoben wurde, kann die Client-Applikation eine S3-POST-Object-Wiederherstellungsanforderung ausgeben, um eine abrufbare Kopie in den S3 Cloud Storage Pool wiederherzustellen. Die Anfrage gibt an, wie viele Tage die Kopie im Cloud Storage Pool und auf die Datenzugriffsebene für den Wiederherstellungsvorgang (Expedited, Standard oder Bulk) verfügbar sein soll. Wenn das Ablaufdatum der abrufbaren Kopie erreicht ist, wird die Kopie automatisch in einen nicht aufrufbaren Zustand zurückgeführt.



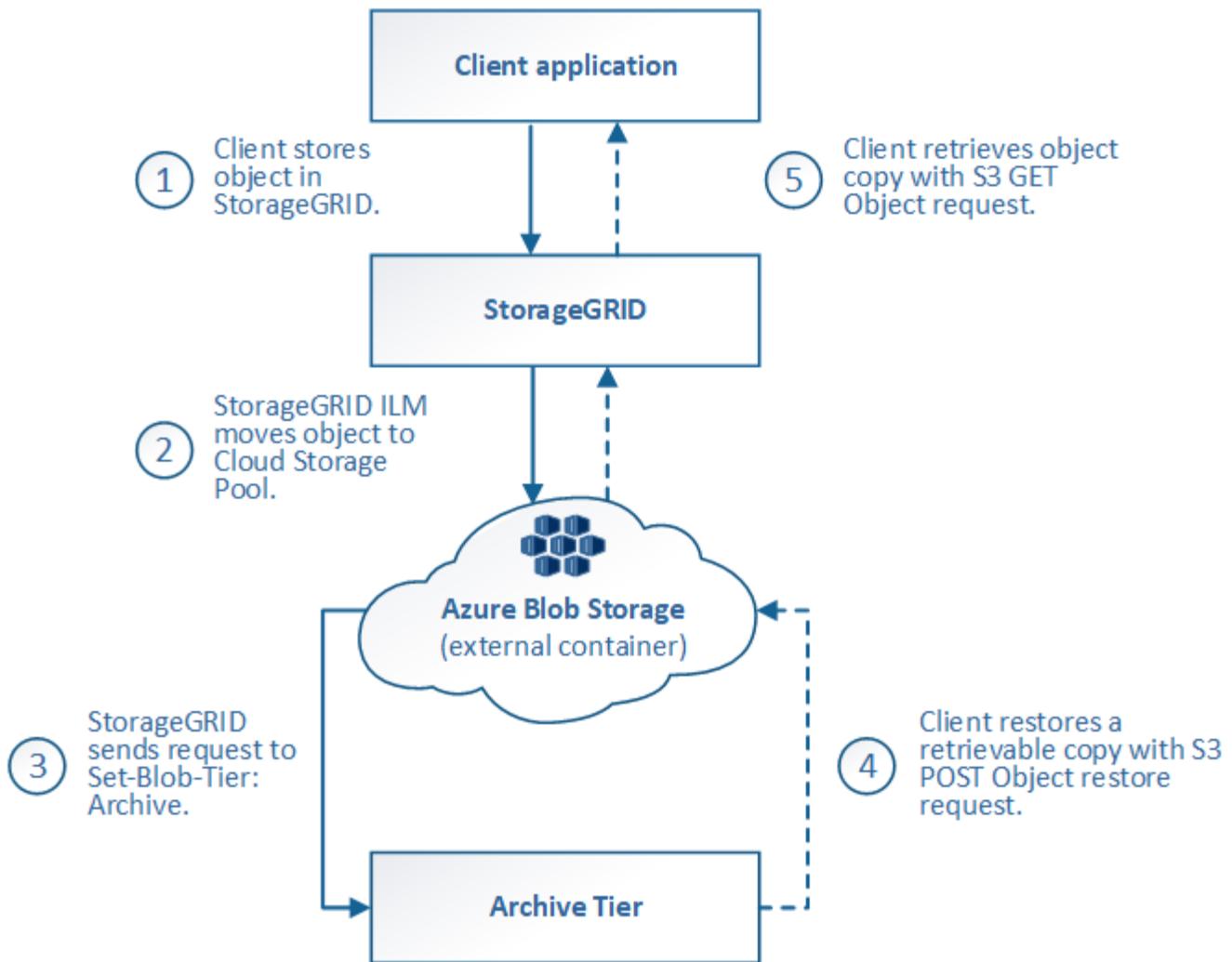
Wenn eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, muss das Objekt nicht von Glacier wiederhergestellt werden, indem eine Anforderung zur Wiederherstellung NACH dem Objekt gestellt wird. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

5. Objekt abgerufen

Sobald ein Objekt wiederhergestellt ist, kann die Client-Applikation eine GET Object-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Azure: Lebenszyklus eines Cloud-Storage-Pool-Objekts

Die Abbildung zeigt die Lebenszyklusphasen eines Objekts, das in einem Azure Cloud-Storage-Pool gespeichert ist.



1. Objekt gespeichert in StorageGRID

Zum Starten des Lebenszyklus speichert eine Client-Applikation ein Objekt in StorageGRID.

2. Objekt in Azure Cloud Storage Pool verschoben

Wird das Objekt mit einer ILM-Regel abgeglichen, die einen Azure Cloud Storage Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den externen Azure Blob-Storage-Container, der vom Cloud-Storage-Pool festgelegt wurde



Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Anfragen zur WIEDERHERSTELLUNG NACH einem Objekt, daher kann StorageGRID keine Swift Objekte abrufen, die auf die Azure Blob Storage-Archivebene übertragen wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

3. Objekt in Archivebene (nicht-Retrieable-Status) umgestiegen

Unmittelbar nach dem Verschieben des Objekts in den Azure Cloud Storage Pool überträgt StorageGRID das Objekt automatisch auf die Azure Blob Storage-Archivebene.

4. Objekt vom Archiv Tier wiederhergestellt

Wenn ein Objekt in die Archivebene migriert wurde, kann die Client-Applikation eine S3-RÜCKSTELLUNGSANFRAGE aus DEM NACHBEARBEITUNGSOBJEKT senden, um eine abrufbare Kopie in den Azure Cloud Storage Pool wiederherzustellen.

Wenn StorageGRID die POST-Objekt-Wiederherstellung empfängt, wird das Objekt vorübergehend in den Azure Blob-Storage Cool-Tier verlagert. Sobald das Ablaufdatum in der Wiederherstellungsanforderung FÜR NACHOBJEKTE erreicht ist, überträgt StorageGRID das Objekt zurück in die Archivebene.



Wenn eine oder mehrere Kopien des Objekts auch auf Storage-Nodes innerhalb von StorageGRID vorhanden sind, muss das Objekt durch Ausgabe einer Anforderung zur WIEDERHERSTELLUNG NACH DEM Objekt nicht aus der Zugriffsebene für Archive wiederhergestellt werden. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

5. Objekt abgerufen

Sobald ein Objekt im Azure Cloud Storage Pool wiederhergestellt ist, kann die Client-Applikation EINE GET Object-Anfrage stellen, um das wiederhergestellte Objekt abzurufen.

Verwandte Informationen

["S3-REST-API VERWENDEN"](#)

Wann sollten Sie Cloud Storage Pools nutzen

Mit Cloud Storage Pools können Sie Daten an einem externen Ort sichern oder per Tiering übertragen. Darüber hinaus können Daten in mehreren Clouds gesichert oder per Tiering verschoben werden.

Backup von StorageGRID Daten an einem externen Speicherort

Sie können einen Cloud-Speicherpool verwenden, um StorageGRID Objekte an einem externen Ort zu sichern.

Wenn der Zugriff auf die Kopien in StorageGRID nicht möglich ist, können die Objektdaten im Cloud-Storage-Pool für Client-Anforderungen verwendet werden. Möglicherweise müssen Sie jedoch eine Anforderung zur Wiederherstellung VON S3-OBJEKTEN NACH DEM Wiederherstellen ausgeben, um auf die Backup-Objektkopie im Cloud-Storage-Pool zuzugreifen.

Die Objektdaten in einem Cloud Storage Pool können auch verwendet werden, um bei einem Ausfall eines Storage-Volumes oder eines Storage-Nodes verlorene Daten von StorageGRID wiederherzustellen. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Storage-Pool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Storage-Node.

So implementieren Sie eine Backup-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Storage-Pool.
2. Konfiguration einer ILM-Regel, die Objektkopien gleichzeitig auf Storage Nodes (als replizierte oder Erasure-codierte Kopien) und einer einzelnen Objektkopie im Cloud Storage Pool speichert
3. Fügen Sie die Regel zur ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Daten-Tiering von StorageGRID auf externen Standort

Sie können einen Cloud-Speicherpool verwenden, um Objekte außerhalb des StorageGRID Systems zu speichern. Angenommen, Sie haben eine große Anzahl von Objekten, die Sie aufbewahren müssen, aber Sie erwarten, dass Sie auf diese Objekte selten zugreifen, wenn überhaupt. Mit einem Cloud-Storage-Pool können Sie die Objekte auf kostengünstigeren Storage verschieben und Speicherplatz in StorageGRID freigeben.

So implementieren Sie eine Tiering-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Storage-Pool.
2. Konfiguration einer ILM-Regel, die selten genutzte Objekte von Storage-Nodes in den Cloud Storage-Pool verschiebt
3. Fügen Sie die Regel zur ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Diverse Cloud-Endpunkte beibehalten

Sie können diverse Cloud-Storage-Pool-Endpunkte konfigurieren, wenn Objektdaten in mehr als einer Cloud verschoben oder gesichert werden sollen. Mit den Filtern Ihrer ILM-Regeln können Sie festlegen, welche Objekte in den einzelnen Cloud Storage-Pools gespeichert werden. Beispielsweise können Sie Objekte von einigen Mandanten oder Buckets in Amazon S3 Glacier und Objekte von anderen Mandanten oder Buckets im Azure Blob Storage speichern. Alternativ können Sie Daten zwischen Amazon S3 Glacier und Azure Blob Storage verschieben.



Bei der Nutzung mehrerer Cloud-Storage-Pool-Endpunkte sollte berücksichtigt werden, dass ein Objekt nur in einem Cloud-Storage-Pool gleichzeitig gespeichert werden kann.

So implementieren Sie diverse Cloud-Endpunkte:

1. Erstellung von bis zu 10 Cloud-Storage-Pools
2. Konfiguration von ILM-Regeln, um die entsprechenden Objektdaten zur entsprechenden Zeit in jedem Cloud-Storage-Pool zu speichern. Speichern Sie beispielsweise Objekte aus Bucket A in Cloud Storage Pool A und speichern Sie Objekte aus Bucket B in Cloud Storage Pool B. Oder speichern Sie Objekte für eine gewisse Zeit im Cloud Storage Pool A und verschieben Sie sie dann in Cloud Storage Pool B.
3. Fügen Sie Regeln zu Ihrer ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Überlegungen zu Cloud-Storage-Pools

Wenn Sie einen Cloud Storage Pool zum Verschieben von Objekten aus dem StorageGRID System verwenden möchten, müssen Sie die Überlegungen für die Konfiguration und Verwendung von Cloud Storage Pools prüfen.

Allgemeine Überlegungen

- Im Allgemeinen ist Cloud-Archiv-Storage, wie Amazon S3 Glacier oder Azure Blob Storage, ein kostengünstiger Ort für die Speicherung von Objektdaten. Die Kosten für den Abruf von Daten aus dem Cloud-Archiv-Storage sind jedoch relativ hoch. Um die niedrigsten Gesamtkosten zu erreichen, müssen Sie berücksichtigen, wann und wie oft Sie auf die Objekte im Cloud Storage Pool zugreifen. Die Verwendung eines Cloud-Storage-Pools wird nur für Inhalte empfohlen, auf die Sie voraussichtlich nur selten zugreifen.
- Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Anforderungen für DIE WIEDERHERSTELLUNG NACH dem Objekt, sodass StorageGRID keine Swift Objekte abrufen kann, die auf S3 Glacier Storage oder in die Azure Blob

Storage-Archivebene verschoben wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

- Die Verwendung von Cloud Storage Pools mit FabricPool wird nicht unterstützt, weil die zusätzliche Latenz zum Abrufen eines Objekts aus dem Cloud-Storage-Pool-Ziel hinzugefügt wird.
- Objekte mit aktivierter S3-Objektsperre können nicht in Cloud-Storage-Pools platziert werden.
- Wenn für den Ziel-S3-Bucket für einen Cloud-Storage-Pool die S3-Objektsperre aktiviert ist, schlägt der Versuch, die Bucket-Replizierung (PutBucketReplication) zu konfigurieren, mit einem Fehler bei AccessDenied fehl.

Überlegungen zu den Ports, die für Cloud-Storage-Pools verwendet werden

Um sicherzustellen, dass die ILM-Regeln Objekte in den und aus dem angegebenen Cloud Storage-Pool verschieben können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die Storage-Nodes Ihres Systems enthalten. Sie müssen sicherstellen, dass die folgenden Ports mit dem Cloud-Speicherpool kommunizieren können.

Standardmäßig verwenden Cloud-Speicherpools die folgenden Ports:

- **80**: Für Endpunkt-URLs, die mit http beginnen
- **443**: Für Endpunkt-URLs, die mit https beginnen

Sie können einen anderen Port angeben, wenn Sie einen Cloud-Speicherpool erstellen oder bearbeiten.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch ["Konfigurieren Sie einen Speicher-Proxy"](#) Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

Überlegungen zu Kosten

Der Zugriff auf den Storage in der Cloud mit einem Cloud Storage Pool erfordert Netzwerkkonnektivität zur Cloud. Dabei müssen die Kosten der Netzwerkinfrastruktur berücksichtigt werden, die für den Zugriff auf die Cloud und die entsprechende Bereitstellung gemäß der Datenmenge verwendet werden, die Sie voraussichtlich zwischen StorageGRID und der Cloud mithilfe des Cloud-Storage-Pools verschieben möchten.

Wenn sich StorageGRID mit dem Endpunkt eines externen Cloud-Storage-Pools verbinden, werden diverse Anfragen zur Überwachung der Konnektivität bearbeitet, um sicherzustellen, dass die IT die erforderlichen Operationen ausführen kann. Während mit diesen Anforderungen einige zusätzliche Kosten verbunden sind, dürfen die Kosten für die Überwachung eines Cloud Storage Pools nur einen kleinen Bruchteil der Gesamtkosten für das Speichern von Objekten in S3 oder Azure ausmachen.

Es können jedoch weitere erhebliche Kosten entstehen, wenn Sie Objekte von einem externen Endpunkt eines Cloud-Storage-Pools zurück auf StorageGRID verschieben müssen. Objekte können in einem der folgenden Fälle zurück auf StorageGRID verschoben werden:

- Die einzige Kopie des Objekts befindet sich in einem Cloud-Storage-Pool, und Sie entscheiden, das Objekt stattdessen in StorageGRID zu speichern. In diesem Fall konfigurieren Sie Ihre ILM-Regeln und -Richtlinien neu. Wenn eine ILM-Bewertung erfolgt, gibt StorageGRID mehrere Anforderungen aus, um das Objekt aus dem Cloud Storage Pool abzurufen. StorageGRID erstellt dann lokal die angegebene Anzahl von replizierten oder mit Erasure Coding verschlüsselten Kopien. Nachdem das Objekt zurück in den StorageGRID verschoben wurde, wird die Kopie im Cloud-Speicherpool gelöscht.
- Objekte sind aufgrund eines Ausfalls des Storage-Nodes verloren. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Storage-Pool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Storage-Node.



Wenn Objekte von einem Cloud-Storage-Pool aus zurück zu StorageGRID verschoben werden, gibt StorageGRID diverse Anfragen an den Cloud-Storage-Pool-Endpunkt für jedes Objekt aus. Bevor Sie eine große Anzahl von Objekten verschieben, wenden Sie sich an den technischen Support, um den Zeitrahmen und die damit verbundenen Kosten zu schätzen.

S3: Für den Cloud Storage Pool Bucket sind Berechtigungen erforderlich

Die Bucket-Richtlinie für den externen S3-Bucket, der für Cloud Storage Pool verwendet wird, muss StorageGRID-Berechtigung erteilen, ein Objekt in den Bucket zu verschieben, den Status eines Objekts zu erhalten, bei Bedarf ein Objekt aus dem Glacier Storage wiederherzustellen usw. Idealerweise sollte StorageGRID über vollständigen Kontrollzugriff auf den Bucket verfügen (`s3:*`). Ist dies jedoch nicht möglich, muss die Bucket-Richtlinie StorageGRID die folgenden S3-Berechtigungen erteilen:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Überlegungen für den Lebenszyklus externer Buckets

Das Verschieben von Objekten zwischen StorageGRID und dem im Cloud Storage Pool angegebenen externen S3-Bucket wird durch ILM-Regeln und die aktive ILM-Richtlinie in StorageGRID gesteuert. Im Gegensatz dazu wird die Transition von Objekten vom im Cloud Storage Pool angegebenen externen S3-Bucket auf Amazon S3 Glacier oder S3 Glacier Deep Archive (oder auf eine Storage-Lösung, die die Glacier Storage-Klasse implementiert) über die Lifecycle-Konfiguration dieses Buckets gesteuert.

Wenn Sie Objekte aus dem Cloud Storage Pool verschieben möchten, müssen Sie eine entsprechende Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen. Außerdem muss eine Storage-Lösung verwendet werden, die die Glacier Storage-Klasse implementiert und die S3-API FÜR DIE WIEDERHERSTELLUNG NACH Objekten unterstützt.

Wenn Sie beispielsweise möchten, dass alle Objekte, die von StorageGRID in den Cloud-Storage-Pool verschoben werden, sofort in Amazon S3 Glacier Storage migriert werden. Sie würden eine Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen, die eine einzelne Aktion (**Transition**) wie folgt festlegt:

```

<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>

```

Diese Regel würde alle Bucket-Objekte an dem Tag der Erstellung auf Amazon S3 Glacier übertragen (d. h. an dem Tag, an dem sie von StorageGRID in den Cloud-Storage-Pool verschoben wurden).



Wenn Sie den Lebenszyklus des externen Buckets konfigurieren, verwenden Sie niemals **Expiration**-Aktionen, um zu definieren, wann Objekte ablaufen. Durch Ablaufaktionen wird das Löschen abgelaufener Objekte im externen Speichersystem verursacht. Wenn Sie später versuchen, von StorageGRID auf ein abgelaufenes Objekt zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Wenn Sie Objekte im Cloud Storage Pool zum S3 Glacier Deep Archive verschieben möchten (statt zu Amazon S3 Glacier), geben Sie an `<StorageClass>DEEP_ARCHIVE</StorageClass>` Im Bucket-Lebenszyklus: Beachten Sie jedoch, dass Sie die nicht verwenden können Expedited Tier zur Wiederherstellung von Objekten aus S3 Glacier Deep Archive.

Azure: Überlegungen für Zugriffsebene

Wenn Sie ein Azure-Speicherkonto konfigurieren, können Sie die Standard-Zugriffsebene auf „Hot“ oder „Cool“ festlegen. Wenn Sie ein Speicherkonto für die Verwendung mit einem Cloud-Speicherpool erstellen, sollten Sie den Hot-Tier als Standardebene verwenden. Auch wenn StorageGRID beim Verschieben von Objekten in den Cloud-Speicherpool sofort den Tier auf Archivierung setzt, stellt mit einer Standardeinstellung von Hot sicher, dass für Objekte, die vor dem 30-Tage-Minimum aus dem Cool Tier entfernt wurden, keine Gebühr für vorzeitiges Löschen berechnet wird.

Azure: Lifecycle-Management nicht unterstützt

Verwenden Sie das Azure Blob Storage-Lifecycle-Management nicht für den Container, der mit einem Cloud-Storage-Pool verwendet wird. Lifecycle-Operationen beeinträchtigen möglicherweise Cloud-Storage-Pool-Vorgänge.

Verwandte Informationen

- ["Erstellen Sie einen Cloud-Storage-Pool"](#)

Vergleich der Replizierung von Cloud-Storage-Pools und CloudMirror

Wenn Sie mit Cloud-Speicherpools beginnen, wäre es möglicherweise hilfreich, die

Ähnlichkeiten und Unterschiede zwischen Cloud-Speicherpools und dem Replizierungsservice für StorageGRID CloudMirror zu verstehen.

	Cloud-Storage-Pool	CloudMirror Replikationsservice
Was ist der primäre Zweck?	Fungiert als Archivziel. Die Objektkopie im Cloud-Storage-Pool kann die einzige Kopie des Objekts sein oder es kann eine zusätzliche Kopie sein. Das heißt, statt zwei Kopien vor Ort zu behalten, kann eine Kopie im StorageGRID behalten und eine Kopie an den Cloud-Storage-Pool senden.	Ermöglicht einem Mandanten, automatisch Objekte aus einem Bucket in StorageGRID (Quelle) in einen externen S3-Bucket (Ziel) zu replizieren. Erstellt eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur.
Wie ist es eingerichtet?	Definiert auf dieselbe Weise wie Speicherpools, mit dem Grid Manager oder der Grid-Management-API. Kann als Speicherort in einer ILM-Regel ausgewählt werden. Während ein Storage-Pool aus einer Gruppe von Storage-Nodes besteht, wird ein Cloud-Storage-Pool mit einem Remote-S3- oder Azure-Endpunkt (IP-Adresse, Zugangsdaten usw.) definiert.	Ein Mandantenbenutzer " Konfiguration der CloudMirror-Replizierung " CloudMirror-Endpunkt (IP-Adresse, Anmeldeinformationen usw.) werden mithilfe des Tenant Manager oder der S3-API definiert. Nachdem der CloudMirror Endpunkt eingerichtet wurde, können alle Buckets dieses Mandantenkontos so konfiguriert werden, dass sie auf den CloudMirror Endpunkt verweisen.
Wer ist für die Einrichtung zuständig?	In der Regel ist ein Grid-Administrator erforderlich.	In der Regel ein Mandantenbenutzer.
Was ist das Ziel?	<ul style="list-style-type: none"> • Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3) • Azure Blob Archiveebene • Google Cloud Platform (GCP) 	<ul style="list-style-type: none"> • Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Ein oder mehrere ILM-Regeln in der aktiven ILM-Richtlinie. Die ILM-Regeln legen fest, welche Objekte die StorageGRID in den Cloud-Storage-Pool verschoben und wann sie verschoben werden.	Aufnahme eines neuen Objekts in einen Quell-Bucket, der mit einem CloudMirror-Endpunkt konfiguriert wurde. Objekte, die sich im Quell-Bucket befanden, bevor der Bucket mit dem CloudMirror-Endpunkt konfiguriert wurde, werden nur repliziert, wenn sie geändert wurden.

	Cloud-Storage-Pool	CloudMirror Replikationsservice
Wie werden Objekte abgerufen?	Applikationen müssen Anfragen an StorageGRID stellen, um Objekte abzurufen, die in einen Cloud-Speicherpool verschoben wurden. Wenn die einzige Kopie eines Objekts in den Archiv-Storage verschoben wurde, managt StorageGRID den Prozess der Wiederherstellung des Objekts, um es abgerufen werden zu können.	Da die gespiegelte Kopie im Ziel-Bucket eine unabhängige Kopie ist, können Applikationen das Objekt abrufen. Dazu müssen sie Anfragen entweder an StorageGRID oder an das S3-Ziel stellen. Angenommen, Sie verwenden CloudMirror Replizierung, um Objekte auf eine Partnerorganisation zu spiegeln. Der Partner kann mithilfe eigener Applikationen Objekte direkt vom S3-Ziel lesen oder aktualisieren. Die Verwendung von StorageGRID ist nicht erforderlich.
Können Sie direkt vom Ziel lesen?	Nein Objekte, die in einen Cloud-Storage-Pool verschoben werden, werden von StorageGRID gemanagt. Leseanforderungen müssen an StorageGRID gerichtet sein (und StorageGRID ist für den Abruf aus Cloud Storage Pool verantwortlich).	Ja, da die gespiegelte Kopie eine unabhängige Kopie ist.
Was geschieht, wenn ein Objekt aus der Quelle gelöscht wird?	Das Objekt wird auch aus dem Cloud-Speicher-Pool gelöscht.	Die Löschkaktion wird nicht repliziert. Ein gelöscht Objekt ist nicht mehr im StorageGRID-Bucket vorhanden, ist jedoch weiterhin im Ziel-Bucket vorhanden. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass die Quelle beeinträchtigt wird.
Wie greifen Sie nach einem Ausfall auf Objekte zu (StorageGRID System nicht betriebsbereit)?	Fehlerhafte StorageGRID-Knoten müssen wiederhergestellt werden. Während dieses Prozesses können Kopien replizierter Objekte mithilfe der Kopien im Cloud Storage Pool wiederhergestellt werden.	Die Objektkopien im CloudMirror Zielsystem sind unabhängig von StorageGRID, sodass sie direkt vor dem Recovery der StorageGRID-Nodes zugänglich sind.

Erstellen Sie einen Cloud-Storage-Pool

Ein Cloud-Storage-Pool gibt einen einzelnen externen Amazon S3-Bucket oder einen anderen S3-kompatiblen Provider oder Azure Blob-Storage-Container an.

Wenn Sie einen Cloud-Storage-Pool erstellen, geben Sie den Namen und den Speicherort des externen Buckets oder Containers an, den StorageGRID zum Speichern von Objekten verwendet, den Cloud-Provider-Typ (Amazon S3/GCP oder Azure Blob Storage) und die Informationen, die StorageGRID für den Zugriff auf den externen Bucket oder Container benötigt.

StorageGRID validiert den Cloud-Storage-Pool, sobald Sie ihn speichern. Sie müssen also sicherstellen, dass der im Cloud-Speicherpool angegebene Bucket oder Container vorhanden ist und erreichbar ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Erforderliche Zugriffsberechtigungen](#)".
- Sie haben die geprüft "[Überlegungen zu Cloud-Storage-Pools](#)".
- Der externe Bucket oder Container, auf den der Cloud-Storage-Pool verweist, ist bereits vorhanden, und Sie kennen seinen Namen und seinen Speicherort.
- Für den Zugriff auf den Bucket oder Container stehen Ihnen die folgenden Informationen für den von Ihnen gewählten Authentifizierungstyp zur Verfügung:

S3 Zugriffsschlüssel

Für den externen S3-Bucket

- Die Zugriffsschlüssel-ID für das Konto, dem der externe Bucket gehört.
- Der zugehörige geheime Zugriffsschlüssel.

Alternativ können Sie Anonymous für den Authentifizierungstyp angeben.

C2S-Zugangsportal

Für Commercial Cloud Services (C2S) S3 Service

Sie haben Folgendes:

- Vollständige URL, die StorageGRID verwendet, um temporäre Anmeldeinformationen vom C2S-Zugriffsportal (CAP)-Server zu erhalten, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
- Zertifikat der Server-Zertifizierungsstelle, ausgestellt von einer entsprechenden Zertifizierungsstelle (Government Certificate Authority, CA). StorageGRID verwendet dieses Zertifikat, um die Identität des CAP-Servers zu überprüfen. Das Server-CA-Zertifikat muss die PEM-Kodierung verwenden.
- Kundenzertifikat, ausgestellt von einer entsprechenden Zertifizierungsstelle (Government Certificate Authority, CA). StorageGRID verwendet dieses Zertifikat zur Identität des CAP-Servers. Das Clientzertifikat muss PEM-Kodierung verwenden und Zugriff auf Ihr C2S-Konto haben.
- PEM-codierter privater Schlüssel für das Clientzertifikat.
- Passphrase zur Entschlüsselung des privaten Schlüssels für das Clientzertifikat, sofern es verschlüsselt ist.



Wenn das Clientzertifikat verschlüsselt wird, verwenden Sie das herkömmliche Format für die Verschlüsselung. Das verschlüsselte PKCS #8-Format wird nicht unterstützt.

Azure Blob Storage

Für den externen Container

- Uniform Resource Identifier (URI), der für den Zugriff auf den Blob-Speicher-Container verwendet wird.
- Name des Speicherkontos und des Kontoschlüssels. Im Azure-Portal finden Sie diese Werte.

Schritte

1. Wählen Sie **ILM > Speicherpools > Cloud-Speicherpools**.
2. Wählen Sie **Create**, und geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Name des Cloud-Storage-Pools	Ein Name, der kurz den Cloud Storage Pool und dessen Zweck beschreibt. Verwenden Sie einen Namen, der leicht zu erkennen ist, wenn Sie ILM-Regeln konfigurieren.
Anbietertyp	Welcher Cloud-Provider nutzen Sie für diesen Cloud-Storage-Pool? <ul style="list-style-type: none">• Amazon S3/GCP: Wählen Sie diese Option für einen Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) oder einen anderen S3-kompatiblen Anbieter.• * Azure Blob Storage*
Eimer oder Container	Der Name des externen S3-Buckets oder Azure-Containers. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

3. Geben Sie je nach Auswahl des Anbietertyps die Informationen zum Service-Endpunkt ein.

Amazon S3/GCP

- a. Wählen Sie für das Protokoll entweder HTTPS oder HTTP aus.



Verwenden Sie keine HTTP-Verbindungen für sensible Daten.

- b. Geben Sie den Hostnamen ein. Beispiel:

`s3-aws-region.amazonaws.com`

- c. URL-Stil auswählen:

Option	Beschreibung
Automatische Erkennung	Versuchen Sie, basierend auf den bereitgestellten Informationen automatisch zu erkennen, welchen URL-Stil verwendet werden soll. Wenn Sie beispielsweise eine IP-Adresse angeben, verwendet StorageGRID eine URL im Pfadstil. Wählen Sie diese Option nur aus, wenn Sie nicht wissen, welcher Stil verwendet werden soll.
Virtual-Hosted-Style	Verwenden Sie eine URL im virtuellen Hosted-Stil, um auf den Bucket zuzugreifen. Virtuelle gehostete URLs enthalten den Bucket-Namen als Teil des Domain-Namens. Beispiel: <code>https://bucket-name.s3.company.com/key-name</code>
Pfadstil	Verwenden Sie eine URL im Pfadstil, um auf den Bucket zuzugreifen. URLs im Pfadstil enthalten am Ende den Bucket-Namen Beispiel: <code>https://s3.company.com/bucket-name/key-name</code> Hinweis: die URL-Option im Pfadstil wird nicht empfohlen und wird in einer zukünftigen Version von StorageGRID veraltet sein.

- d. Geben Sie optional die Portnummer ein, oder verwenden Sie den Standardport: 443 für HTTPS oder 80 für HTTP.

Azure Blob Storage

- a. Geben Sie unter Verwendung eines der folgenden Formate den URI für den Service-Endpunkt ein.

- `https://host:port`
- `http://host:port`

Beispiel: `https://myaccount.blob.core.windows.net:443`

Wenn Sie keinen Port angeben, wird standardmäßig Port 443 für HTTPS und Port 80 für HTTP verwendet.

4. Wählen Sie **Weiter**. Wählen Sie dann den Authentifizierungstyp aus und geben Sie die erforderlichen Informationen für den Endpunkt des Cloud-Storage-Pools ein:

Zugriffsschlüssel

Nur für Amazon S3/GCP Provider type

- Geben Sie für **Zugriffsschlüssel-ID** die Zugriffsschlüssel-ID für das Konto ein, dem der externe Bucket gehört.
- Geben Sie für **Secret Access key** den geheimen Zugriffsschlüssel ein.

KAPPE (C2S-Zugangsportale)

Für Commercial Cloud Services (C2S) S3 Service

- Geben Sie für die URL der temporären Anmeldeinformationen * die vollständige URL ein, die StorageGRID zum Abrufen temporärer Anmeldeinformationen vom CAP-Server verwendet, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
- Wählen Sie für **Server-CA-Zertifikat Durchsuchen** aus, und laden Sie das PEM-kodierte CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwendet.
- Wählen Sie für **Clientzertifikat Durchsuchen** aus, und laden Sie das PEM-kodierte Zertifikat hoch, das StorageGRID verwendet, um sich auf dem CAP-Server zu identifizieren.
- Wählen Sie für **Client private key Browse** aus, und laden Sie den PEM-kodierten privaten Schlüssel für das Clientzertifikat hoch.
- Wenn der private Clientschlüssel verschlüsselt ist, geben Sie die Passphrase zum Entschlüsseln des privaten Clientschlüssels ein. Andernfalls lassen Sie das Feld **Client Private Key Passphrase** leer.

Azure Blob Storage

- Geben Sie für **Kontoname** den Namen des Blob-Speicherkontos ein, dem der externe Service-Container gehört.
- Geben Sie für **Account key** den geheimen Schlüssel für das Blob-Speicherkonto ein.

Anonym

Es sind keine zusätzlichen Informationen erforderlich.

- Wählen Sie **Weiter**. Wählen Sie dann die Art der Serverüberprüfung aus, die Sie verwenden möchten:

Option	Beschreibung
Verwenden Sie Stammzertifizierungsstellen-Zertifikate in Storage Node OS	Verwenden Sie zum Sichern der Verbindungen die auf dem Betriebssystem installierten Grid CA-Zertifikate.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Wählen Sie Browse , und laden Sie das PEM-kodierte Zertifikat hoch.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

- Wählen Sie **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Bucket oder Container und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Anmeldedaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Bucket oder Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie niemals diese Datei, die benannt ist `x-ntap-sgws-cloud-pool-uuid`.

Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatfehler vorliegt oder der Bucket oder Container, den Sie angegeben haben, nicht bereits vorhanden ist.

7. Wenn ein Fehler auftritt, lesen Sie die ["Anweisungen zur Fehlerbehebung bei Cloud Storage Pools"](#) Beheben Sie alle Probleme, und versuchen Sie dann erneut, den Cloud-Speicherpool zu speichern.

Bearbeiten eines Cloud-Speicherpools

Sie können einen Cloud-Storage-Pool bearbeiten, um dessen Namen, Service-Endpunkt oder andere Details zu ändern. Sie können jedoch nicht den S3-Bucket oder Azure-Container für einen Cloud-Storage-Pool ändern.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die geprüft ["Überlegungen zu Cloud-Storage-Pools"](#).

Schritte

1. Wählen Sie **ILM > Speicherpools > Cloud-Speicherpools**.

In der Tabelle Cloud-Storage-Pools werden die vorhandenen Cloud-Storage-Pools aufgeführt.

2. Aktivieren Sie das Kontrollkästchen für den Cloud-Storage-Pool, den Sie bearbeiten möchten.
3. Wählen Sie **Actions > Edit**.
4. Ändern Sie bei Bedarf den Anzeigenamen, den Dienstendpunkt, die Authentifizierungsdaten oder die Methode zur Zertifikatvalidierung.



Sie können den Provider-Typ oder den S3-Bucket oder Azure-Container für einen Cloud-Storage-Pool nicht ändern.

Wenn Sie zuvor ein Server- oder Client-Zertifikat hochgeladen haben, können Sie **Zertifikatdetails** auswählen, um das derzeit verwendete Zertifikat zu überprüfen.

5. Wählen Sie **Speichern**.

Wenn Sie einen Cloud-Storage-Pool speichern, überprüft StorageGRID, ob der Bucket oder Container und der Service-Endpunkt vorhanden sind. Ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.

Wenn die Validierung des Cloud-Speicherpools fehlschlägt, wird eine Fehlermeldung angezeigt. Ein Fehler kann z. B. gemeldet werden, wenn ein Zertifikatfehler vorliegt.

Siehe Anweisungen für ["Fehlerbehebung bei Cloud Storage Pools"](#), Beheben Sie das Problem, und versuchen Sie dann erneut, den Cloud-Speicher-Pool zu speichern.

Entfernen Sie einen Cloud-Speicherpool

Sie können einen Cloud-Speicherpool entfernen, wenn er nicht in einer ILM-Regel verwendet wird und keine Objektdaten enthält.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Erforderliche Zugriffsberechtigungen](#)".

Verwenden Sie bei Bedarf ILM, um Objektdaten zu verschieben

Wenn der Cloud Storage Pool, den Sie entfernen möchten, Objektdaten enthält, müssen Sie ILM verwenden, um die Daten an einen anderen Speicherort zu verschieben. Sie können die Daten beispielsweise in Storage Nodes in Ihrem Grid oder in einen anderen Cloud-Storage-Pool verschieben.

Schritte

1. Wählen Sie **ILM > Speicherpools > Cloud-Speicherpools**.
2. Prüfen Sie in der Spalte „ILM-Nutzung“ der Tabelle, ob Sie den Cloud Storage-Pool entfernen können.

Sie können einen Cloud Storage-Pool nicht entfernen, wenn er in einer ILM-Regel oder in einem Profil für Erasure Coding verwendet wird.
3. Wenn der Cloud Storage Pool verwendet wird, wählen Sie **Cloud Storage Pool Name > ILM usage** aus.
4. "[Klonen jeder ILM-Regel](#)" Damit werden Objekte im Cloud-Storage-Pool platziert, den Sie entfernen möchten.
5. Legen Sie fest, wo die vorhandenen Objekte, die von den einzelnen von Ihnen geklonten Regeln verwaltet werden, verschoben werden sollen.

Sie können einen oder mehrere Speicherpools oder einen anderen Cloud-Speicherpool verwenden.

6. Bearbeiten Sie jede der von Ihnen geklonten Regeln.

Wählen Sie für Schritt 2 des Assistenten zum Erstellen von ILM-Regeln den neuen Speicherort aus dem Feld **copies at** aus.
7. "[Erstellen einer neuen vorgeschlagenen ILM-Richtlinie](#)" Und ersetzen Sie jede der alten Regeln durch eine geklonte Regel.
8. Aktivieren Sie die neue Richtlinie.
9. Warten Sie, bis ILM Objekte aus dem Cloud Storage-Pool entfernt und an dem neuen Speicherort platziert hat.

Cloud Storage-Pool Löschen

Wenn der Cloud Storage Pool leer ist und in keiner ILM-Regel verwendet wird, können Sie ihn löschen.

Bevor Sie beginnen

- Sie haben alle ILM-Regeln entfernt, die den Pool möglicherweise verwendet haben.
- Sie haben bestätigt, dass der S3-Bucket oder der Azure-Container keine Objekte enthält.

Ein Fehler tritt auf, wenn Sie versuchen, einen Cloud-Speicherpool zu entfernen, wenn er Objekte enthält. Siehe "[Fehlerbehebung Bei Cloud Storage Pools](#)".



Beim Erstellen eines Cloud Storage-Pools schreibt StorageGRID eine Markierungsdatei in den Bucket oder Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie diese Datei, die den Namen hat, nicht `x-ntap-sgws-cloud-pool-uuid`.

Schritte

1. Wählen Sie **ILM > Speicherpools > Cloud-Speicherpools**.
2. Wenn in der Spalte „ILM-Nutzung“ angezeigt wird, dass Cloud Storage Pool nicht verwendet wird, aktivieren Sie das Kontrollkästchen.
3. Wählen Sie **Aktionen > Entfernen**.
4. Wählen Sie **OK**.

Fehlerbehebung Bei Cloud Storage Pools

Verwenden Sie diese Fehlerbehebungsschritte, um Fehler zu beheben, die beim Erstellen, Bearbeiten oder Löschen eines Cloud-Speicherpools auftreten können.

Ermitteln Sie, ob ein Fehler aufgetreten ist

StorageGRID führt einmal pro Minute eine einfache Zustandsprüfung für jeden Cloud Storage Pool durch, um sicherzustellen, dass auf den Cloud Storage Pool zugegriffen werden kann und dass er ordnungsgemäß funktioniert. Wenn durch die Integritätsprüfung ein Problem erkannt wird, wird auf der Seite Speicherpools in der Spalte Letzter Fehler der Tabelle Cloud-Speicherpools eine Meldung angezeigt.

In der Tabelle ist der aktuellste Fehler aufgeführt, der bei den einzelnen Cloud-Storage-Pools erkannt wurde. Der Fehler ist vor langer Zeit aufgetreten.

Zusätzlich wird eine Meldung mit * Cloud Storage Pool Verbindungsfehler* ausgelöst, wenn die Systemprüfung feststellt, dass innerhalb der letzten 5 Minuten ein oder mehrere neue Cloud Storage Pool-Fehler aufgetreten sind. Wenn Sie eine E-Mail-Benachrichtigung für diese Warnung erhalten, gehen Sie zur Seite Speicherpools (wählen Sie **ILM > Speicherpools**), überprüfen Sie die Fehlermeldungen in der Spalte Letzter Fehler und lesen Sie die unten stehenden Richtlinien zur Fehlerbehebung.

Überprüfen Sie, ob ein Fehler behoben wurde

Nach der Behebung von Problemen können Sie feststellen, ob der Fehler behoben ist. Wählen Sie auf der Seite Cloud Storage Pool den Endpunkt aus, und wählen Sie **Fehler löschen** aus. Eine Bestätigungsmeldung gibt an, dass StorageGRID den Fehler für den Cloud-Speicherpool gelöscht hat.

Wenn das zugrunde liegende Problem behoben wurde, wird die Fehlermeldung nicht mehr angezeigt. Wenn das zugrunde liegende Problem jedoch nicht behoben wurde (oder ein anderer Fehler auftritt), wird die Fehlermeldung innerhalb weniger Minuten in der Spalte Letzter Fehler angezeigt.

Fehler: Dieser Cloud-Speicherpool enthält unerwartete Inhalte

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen, zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Bucket oder Container den enthält `x-ntap-sgws-cloud-pool-uuid` Markierungsdatei, aber diese Datei verfügt nicht über die erwartete UUID.

In der Regel wird dieser Fehler nur angezeigt, wenn Sie einen neuen Cloud Storage-Pool erstellen, und eine andere Instanz von StorageGRID verwendet bereits den gleichen Cloud Storage-Pool.

Versuchen Sie mit diesen Schritten das Problem zu beheben:

- Vergewissern Sie sich, dass niemand in Ihrem Unternehmen diesen Cloud-Speicherpool verwendet.
- Löschen Sie die `x-ntap-sgws-cloud-pool-uuid` Datei und versuchen Sie erneut, den Cloud-Speicherpool zu konfigurieren.

Fehler: Cloud-Speicherpool konnte nicht erstellt oder aktualisiert werden. Fehler vom Endpunkt

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Dieser Fehler zeigt an, dass eine Art von Verbindungs- oder Konfigurationsproblem darin besteht, dass StorageGRID das Schreiben in den Cloud Storage Pool verhindert.

Überprüfen Sie die Fehlermeldung vom Endpunkt, um das Problem zu beheben.

- Wenn die Fehlermeldung enthält ``Get url: EOF`` Überprüfen Sie, ob der für den Cloud-Speicher-Pool verwendete Service-Endpunkt HTTP nicht für einen Container oder Bucket verwendet, der HTTPS erfordert.
- Wenn die Fehlermeldung enthält `Get url: net/http: request canceled while waiting for connection`, Überprüfen Sie, ob die Netzwerkkonfiguration Storage-Knoten Zugriff auf den Service-Endpunkt erlaubt, der für den Cloud Storage Pool verwendet wird.
- Versuchen Sie bei allen anderen Fehlermeldungen am Endpunkt eine oder mehrere der folgenden Optionen:
 - Erstellen Sie einen externen Container oder Bucket mit demselben Namen, den Sie für den Cloud-Storage-Pool eingegeben haben, und versuchen Sie, den neuen Cloud-Storage-Pool erneut zu speichern.
 - Korrigieren Sie den für den Cloud Storage Pool angegebenen Container- oder Bucket-Namen und versuchen Sie, den neuen Cloud Storage-Pool erneut zu speichern.

Fehler: Fehler beim Parsen des CA-Zertifikats

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Der Fehler tritt auf, wenn StorageGRID das bei der Konfiguration des Cloud-Speicherpools eingegebene Zertifikat nicht analysieren konnte.

Überprüfen Sie zum Beheben des Problems das von Ihnen bereitgestellte CA-Zertifikat auf Probleme.

Fehler: Ein Cloud-Speicherpool mit dieser ID wurde nicht gefunden

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Endpunkt eine 404-Antwort zurückgibt. Dies kann eine der folgenden Optionen bedeuten:

- Die für den Cloud-Storage-Pool verwendeten Anmeldeinformationen haben keine Leseberechtigung für den Bucket.
- Der für den Cloud-Storage-Pool verwendete Bucket enthält nicht den `x-ntap-sgws-cloud-pool-uuid` Markierungsdatei.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Stellen Sie sicher, dass der dem konfigurierten Zugriffsschlüssel zugeordnete Benutzer über die erforderlichen Berechtigungen verfügt.
- Bearbeiten Sie den Cloud Storage Pool mit Zugangsdaten, die über die entsprechenden Berechtigungen verfügen.

- Wenn die Berechtigungen korrekt sind, wenden Sie sich an den Support.

Fehler: Der Inhalt des Cloud-Speicherpools konnte nicht überprüft werden. Fehler vom Endpunkt

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Dieser Fehler zeigt an, dass eine Art von Verbindungs- oder Konfigurationsproblem darin besteht, dass StorageGRID den Inhalt des Cloud Storage Pool Buckets liest.

Überprüfen Sie die Fehlermeldung vom Endpunkt, um das Problem zu beheben.

Fehler: Objekte wurden bereits in diesen Bucket platziert

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Sie können einen Cloud-Storage-Pool nicht löschen, wenn er Daten enthält, die durch ILM dorthin verschoben wurden, Daten, die sich vor dem Konfigurieren des Cloud-Storage-Pools im Bucket befinden, oder Daten, die nach der Erstellung des Cloud-Storage-Pools von einer anderen Quelle in den Bucket verschoben wurden.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Folgen Sie den Anweisungen, um Objekte in „Lifecycle eines Cloud-Storage-Pool-Objekts zurück in StorageGRID zu verschieben.“
- Wenn Sie sicher sind, dass die verbleibenden Objekte nicht durch ILM im Cloud-Storage-Pool platziert wurden, löschen Sie die Objekte manuell aus dem Bucket.



Löschen Sie nie Objekte manuell aus einem Cloud-Storage-Pool, der eventuell durch ILM gespeichert wurde. Wenn Sie später versuchen, auf ein manuell gelöscht Objekt aus StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Fehler: Beim Versuch, den Cloud-Speicherpool zu erreichen, ist ein externer Fehler aufgetreten

Dieser Fehler kann auftreten, wenn Sie zwischen Storage-Nodes einen nicht transparenten Storage Proxy und den externen S3-Endpunkt konfiguriert haben, der für den Cloud Storage-Pool verwendet wird. Dieser Fehler tritt auf, wenn der externe Proxyserver den Endpunkt des Cloud-Speicherpools nicht erreichen kann. Beispielsweise kann der DNS-Server den Hostnamen möglicherweise nicht lösen, oder es könnte ein externes Netzwerkproblem geben.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Überprüfen Sie die Einstellungen für den Cloud Storage Pool (**ILM > Storage Pools**).
- Überprüfen Sie die Netzwerkkonfiguration des Storage Proxy-Servers.

Verwandte Informationen

["Lebenszyklus eines Cloud-Storage-Pool-Objekts"](#)

Profile für das Erasure Coding managen

Sie können bei Bedarf ein Profil für die Erasure Coding umbenennen. Sie können ein Profil für Erasure Coding deaktivieren, wenn es derzeit nicht in ILM-Regeln verwendet wird.

Umbenennen eines Profils für die Erasure Coding

Möglicherweise möchten Sie ein Erasure Coding-Profil umbenennen, um es deutlicher zu machen, was das Profil tut.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Erforderliche Zugriffsberechtigungen](#)".

Schritte

1. Wählen Sie **ILM > Erasure Coding** aus.
2. Wählen Sie das Profil aus, das Sie umbenennen möchten.
3. Wählen Sie **Umbenennen**.
4. Geben Sie einen eindeutigen Namen für das Erasure Coding-Profil ein.

Der Name des Erasure Coding-Profiles wird in der Platzierungsanweisung für eine ILM-Regel an den Namen des Speicherpools angehängt.



Profilnamen für das Erasure Coding müssen eindeutig sein. Ein Validierungsfehler tritt auf, wenn Sie den Namen eines vorhandenen Profils verwenden, auch wenn dieses Profil deaktiviert wurde.

5. Wählen Sie **Speichern**.

Deaktivieren Sie ein Erasure Coding-Profil

Sie können ein Profil für Erasure Coding deaktivieren, wenn Sie es nicht mehr verwenden möchten und das Profil derzeit in keiner ILM-Regel verwendet wird.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Erforderliche Zugriffsberechtigungen](#)".
- Sie haben bestätigt, dass derzeit keine Reparatur- oder Deaktivierung von Daten mithilfe von Erasure Coding ausgeführt wird. Wenn Sie versuchen, ein Erasure Coding-Profil zu deaktivieren, während eines dieser Vorgänge ausgeführt wird, wird eine Fehlermeldung ausgegeben.

Über diese Aufgabe

Wenn Sie ein Erasure Coding-Profil deaktivieren, wird das Profil weiterhin auf der Seite Erasure Coding Profiles angezeigt, sein Status ist jedoch **deactivated**.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input type="radio"/> 2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
<input checked="" type="radio"/> New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

Sie können kein deaktiviertes Erasure Coding-Profil mehr verwenden. Ein deaktiviertes Profil wird nicht angezeigt, wenn Sie die Platzierungsanweisungen für eine ILM-Regel erstellen. Ein deaktiviertes Profil kann nicht reaktiviert werden.

StorageGRID verhindert, dass Sie ein Erasure Coding-Profil deaktivieren, wenn eine der folgenden Optionen zutrifft:

- Das Erasure Coding-Profil wird derzeit in einer ILM-Regel verwendet.
- Das Erasure Coding-Profil wird in keiner ILM-Regel mehr verwendet, es existieren jedoch noch Objektdaten und Paritätsfragmente für das Profil.

Schritte

1. Wählen Sie **ILM > Erasure Coding** aus.
2. Überprüfen Sie die Spalte **Status**, um zu bestätigen, dass das Erasure Coding-Profil, das Sie deaktivieren möchten, in keiner ILM-Regel verwendet wird.

Sie können ein Profil für Erasure Coding nicht deaktivieren, wenn es in einer ILM-Regel verwendet wird. Im Beispiel wird das Profil **2+1 Data Center 1** in mindestens einer ILM-Regel verwendet.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input checked="" type="radio"/> 2+1 Data Center 1	Used in ILM Rule	Data Center 1	3	1	2+1	50	1	No
<input type="radio"/> New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

3. Wenn das Profil in einer ILM-Regel verwendet wird, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie **ILM > Regeln**.
 - b. Wählen Sie jede Regel aus, und prüfen Sie das Aufbewahrungsdiagramm, um festzustellen, ob die Regel das zu deaktivierende Erasure Coding-Profil verwendet.
 - c. Wenn die ILM-Regel das Profil für die Erasure Coding verwendet, das Sie deaktivieren möchten, bestimmen Sie, ob die Regel in der aktiven ILM-Richtlinie oder in einer vorgeschlagenen Richtlinie verwendet wird.
 - d. Führen Sie die zusätzlichen Schritte in der Tabelle aus, je nachdem, wo das Erasure Coding-Profil verwendet wird.

Wo wurde das Profil verwendet?	Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen	Beachten Sie diese zusätzlichen Anweisungen
Nie in einer ILM-Regel verwendet	Weitere Schritte sind nicht erforderlich. Fahren Sie mit diesem Verfahren fort.	<i>Keine</i>
In einer ILM-Regel, die noch nie in einer ILM-Richtlinie verwendet wurde	<ol style="list-style-type: none"> i. Alle betroffenen ILM-Regeln bearbeiten oder löschen. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. ii. Fahren Sie mit diesem Verfahren fort. 	"Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"

Wo wurde das Profil verwendet?	Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen	Beachten Sie diese zusätzlichen Anweisungen
In einer ILM-Regel, die sich derzeit in der aktiven ILM-Richtlinie befindet	<ul style="list-style-type: none"> i. Klonen der aktiven Richtlinie ii. Entfernen Sie die ILM-Regel, die das Profil für das Erasure Coding verwendet. iii. Fügen Sie mindestens eine neue ILM-Regel hinzu, um die Sicherheit von Objekten zu gewährleisten. iv. Speichern, simulieren und aktivieren Sie die neue Richtlinie. v. Warten Sie, bis die neue Richtlinie angewendet wird und vorhandene Objekte basierend auf den neuen Regeln, die Sie hinzugefügt haben, an neue Orte verschoben werden. <p>Hinweis: abhängig von der Anzahl der Objekte und der Größe Ihres StorageGRID-Systems kann es Wochen oder sogar Monate dauern, bis ILM-Vorgänge die Objekte auf der Grundlage der neuen ILM-Regeln an neue Orte verschieben.</p> <p>Obwohl Sie sicher versuchen können, ein Erasure Coding-Profil zu deaktivieren, während es noch mit Daten verknüpft ist, schlägt die Deaktivierung fehl. Eine Fehlermeldung informiert Sie darüber, ob das Profil noch nicht deaktiviert werden kann.</p> <ul style="list-style-type: none"> 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. 	<p>"ILM-Richtlinie erstellen"</p> <p>"Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"</p>
In einer ILM-Regel, die sich derzeit in einer vorgeschlagenen ILM-Richtlinie befindet	<ul style="list-style-type: none"> i. Bearbeiten Sie die vorgeschlagene Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Profil für das Erasure Coding verwendet. iii. Fügen Sie ein oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass alle Objekte geschützt sind. iv. Speichern Sie die vorgeschlagene Richtlinie. v. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. vi. Fahren Sie mit diesem Verfahren fort. 	<p>"ILM-Richtlinie erstellen"</p> <p>"Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"</p>

Wo wurde das Profil verwendet?	Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen	Beachten Sie diese zusätzlichen Anweisungen
In einer ILM-Regel, die sich in einer historischen ILM-Richtlinie befindet	i. Bearbeiten oder löschen Sie die Regel. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. (Die Regel wird nun als historische Regel in der historischen Richtlinie angezeigt.) ii. Fahren Sie mit diesem Verfahren fort.	"Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"

e. Aktualisieren Sie die Seite Erasure Coding Profiles, um sicherzustellen, dass das Profil nicht in einer ILM-Regel verwendet wird.

4. Wenn das Profil nicht in einer ILM-Regel verwendet wird, aktivieren Sie das Optionsfeld und wählen Sie **Deaktivieren**.

Das Dialogfeld EC-Profil deaktivieren wird angezeigt.

5. Wenn Sie sicher sind, dass Sie das Profil deaktivieren möchten, wählen Sie **Deactivate**.
 - Wenn StorageGRID das Erasure Coding-Profil deaktivieren kann, ist sein Status **deactivated**. Sie können dieses Profil nicht mehr für eine ILM-Regel auswählen.
 - Wenn StorageGRID das Profil nicht deaktivieren kann, wird eine Fehlermeldung angezeigt. Wenn Objektdaten weiterhin mit diesem Profil verknüpft sind, wird beispielsweise eine Fehlermeldung angezeigt. Sie müssen möglicherweise mehrere Wochen warten, bevor Sie den Deaktivierungsprozess erneut versuchen.

Regionen konfigurieren (nur optional und S3)

ILM-Regeln können Objekte auf Basis der Bereiche filtern, in denen S3-Buckets erstellt werden, und so Objekte aus verschiedenen Regionen an unterschiedlichen Storage-Standorten speichern.

Wenn Sie einen S3-Bucket-Bereich als Filter in einer Regel verwenden möchten, müssen Sie zuerst die Regionen erstellen, die von den Buckets in Ihrem System verwendet werden können.



Sie können den Bereich für einen Bucket nicht ändern, nachdem der Bucket erstellt wurde.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Beim Erstellen eines S3-Buckets können Sie angeben, dass er in einer bestimmten Region erstellt wird. Wenn Sie eine Region angeben, kann der Bucket sich in geografischer Nähe zu seinen Benutzern befinden, um die Latenz zu optimieren, Kosten zu minimieren und gesetzliche Anforderungen zu erfüllen.

Wenn Sie eine ILM-Regel erstellen, möchten Sie die Region, die einem S3-Bucket zugeordnet ist, möglicherweise als erweiterten Filter verwenden. Sie können zum Beispiel eine Regel entwerfen, die sich nur

auf Objekte bezieht, die in den in us-West-2 erstellten S3-Buckets gelten. Sie können dann angeben, die Kopien dieser Objekte an Storage-Nodes an einem Datacenter-Standort innerhalb dieser Region platziert werden, um die Latenz zu optimieren.

Befolgen Sie bei der Konfiguration von Regionen die folgenden Richtlinien:

- Standardmäßig gehören alle Buckets zu US-East-1-Region.
- Sie müssen die Regionen mit dem Grid Manager erstellen, bevor Sie beim Erstellen von Buckets mithilfe der Mandanten-Manager- oder Mandantenmanagement-API oder mit dem LocationConstraint-Anforderungselement für S3 PUT-Bucket-API-Anforderungen eine nicht standardmäßige Region angeben können. Ein Fehler tritt auf, wenn eine PUT-Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.
- Sie müssen beim Erstellen des S3-Buckets den genauen Regionalnamen verwenden. Bei Regionalnamen wird zwischen Groß- und Kleinschreibung unterschieden. Gültige Zeichen sind Zahlen, Buchstaben und Bindestriche.



Die EU gilt nicht als ein Alias für eu-West-1. Wenn Sie die Region EU oder eu-West-1 nutzen möchten, müssen Sie den genauen Namen verwenden.

- Sie können eine Region nicht löschen oder ändern, wenn sie derzeit innerhalb der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.
- Wenn die Region, die als erweiterter Filter in einer ILM-Regel verwendet wird, ungültig ist, kann diese Regel noch zur vorgeschlagenen Richtlinie hinzugefügt werden. Es tritt jedoch ein Fehler auf, wenn Sie versuchen, die vorgeschlagene Richtlinie zu speichern oder zu aktivieren.

Eine ungültige Region kann sich ergeben, wenn Sie eine Region als erweiterten Filter in einer ILM-Regel verwenden, diese Region jedoch später löschen oder wenn Sie die Grid-Management-API zum Erstellen einer Regel und zum Festlegen einer Region verwenden, die Sie nicht definiert haben.

- Wenn Sie eine Region löschen, nachdem Sie sie zum Erstellen eines S3-Buckets verwendet haben, müssen Sie die Region erneut hinzufügen, wenn Sie den erweiterten Filter Speicherungsbedingung verwenden möchten, um Objekte in diesem Bucket zu finden.

Schritte

1. Wählen Sie **ILM > Regionen**.

Die Seite Regionen wird angezeigt, wobei die derzeit definierten Regionen aufgelistet sind. **Region 1** zeigt die Standardregion, `us-east-1`, die nicht geändert oder entfernt werden können.

2. So fügen Sie eine Region hinzu:

- a. Wählen Sie das Einfügesymbol aus **+** Rechts neben dem letzten Eintrag.
- b. Geben Sie den Namen einer Region ein, die Sie beim Erstellen von S3-Buckets verwenden möchten.

Sie müssen diesen genauen Regionalnamen als LocationConstraint Request Element verwenden, wenn Sie den entsprechenden S3-Bucket erstellen.

3. Um eine nicht verwendete Region zu entfernen, wählen Sie das Löschsymbolsymbol aus **X**.

Wenn Sie versuchen, eine Region zu entfernen, die derzeit in der aktiven Richtlinie oder der vorgeschlagenen Richtlinie verwendet wird, wird eine Fehlermeldung angezeigt.

4. Wenn Sie Änderungen vorgenommen haben, wählen Sie **Speichern**.

Sie können diese Bereiche nun im Abschnitt Erweiterte Filter in Schritt 1 des Assistenten zum Erstellen von ILM-Regeln auswählen. Siehe "[Verwenden Sie erweiterte Filter in ILM-Regeln](#)".

ILM-Regel erstellen

Erstellen Sie eine ILM-Regel: Überblick

Zum Managen von Objekten erstellen Sie eine Reihe von Regeln für das Information Lifecycle Management (ILM) und organisieren diese in eine ILM-Richtlinie.

Jedes im System aufgenommene Objekt wird anhand der aktiven Richtlinie ausgewertet. Wenn eine Regel in der Richtlinie mit den Metadaten eines Objekts übereinstimmt, bestimmen die Anweisungen in der Regel, welche Aktionen StorageGRID zum Kopieren und Speichern des Objekts ergreift.



Objektmetadaten werden nicht durch ILM-Regeln gemanagt. Stattdessen werden Objekt-Metadaten in einer Cassandra-Datenbank in einem sogenannten Metadaten-Speicher gespeichert. Drei Kopien von Objekt-Metadaten werden automatisch an jedem Standort aufbewahrt, um die Daten vor Verlust zu schützen.

Elemente einer ILM-Regel

Eine ILM-Regel besteht aus drei Elementen:

- **Filterkriterien:** Die Basis- und erweiterten Filter einer Regel definieren, für welche Objekte die Regel gilt. Wenn ein Objekt allen Filtern entspricht, wendet StorageGRID die Regel an und erstellt die Objektkopien, die in den Platzierungsanweisungen der Regel angegeben sind.
- **Platzierungsanweisungen:** Die Platzierungsanweisungen einer Regel definieren die Zahl, den Typ und den Ort von Objektkopien. Jede Regel kann eine Reihe von Anweisungen zur Platzierung enthalten, um die Anzahl, den Typ und den Standort der Objektkopien im Laufe der Zeit zu ändern. Wenn der Zeitraum für eine Platzierung abgelaufen ist, werden die Anweisungen in der nächsten Platzierung automatisch bei der nächsten ILM-Bewertung angewendet.
- **Ingest Behavior:** Das Ingest Behavior einer Regel erlaubt Ihnen zu wählen, wie die Objekte, die durch die Regel gefiltert werden, geschützt werden, wenn sie aufgenommen werden (wenn ein S3- oder Swift-Client ein Objekt im Grid speichert).

ILM-Regelfilterung

Wenn Sie eine ILM-Regel erstellen, geben Sie Filter an, um zu identifizieren, für welche Objekte die Regel gilt.

Im einfachsten Fall verwendet eine Regel möglicherweise keine Filter. Alle Regeln, die keine Filter verwenden, gelten für alle Objekte. Daher muss es sich um die letzte (standardmäßige) Regel in einer ILM-Richtlinie handeln. Die Standardregel enthält Speicheranweisungen für Objekte, die nicht mit den Filtern einer anderen Regel übereinstimmen.

- Grundlegende Filter ermöglichen es Ihnen, unterschiedliche Regeln auf große, unterschiedliche Objektgruppen anzuwenden. Mit diesen Filtern können Sie eine Regel auf bestimmte Mandantenkonten, bestimmte S3-Buckets oder Swift-Container oder beides anwenden.

Grundlegende Filter geben Ihnen eine einfache Möglichkeit, verschiedene Regeln auf eine große Anzahl von Objekten anzuwenden. So müssen beispielsweise die Finanzdaten Ihres Unternehmens möglicherweise gespeichert werden, um gesetzliche Vorgaben einzuhalten. Daten aus der Marketing-Abteilung müssen möglicherweise gespeichert werden, um den täglichen Betrieb zu erleichtern. Nach der

Erstellung separater Mandantenkonten für jede Abteilung oder nach Trennung von Daten aus den verschiedenen Abteilungen in separate S3 Buckets können Sie problemlos eine Regel erstellen, die für alle Finanzdaten und eine zweite Regel gilt für alle Marketingdaten.

- Erweiterte Filter geben Ihnen eine präzise Kontrolle. Sie können Filter erstellen, um Objekte anhand der folgenden Objekteigenschaften auszuwählen:
 - Aufnahmezeit
 - Zeitpunkt des letzten Zugriffs
 - Der Objektname (Schlüssel) ganz oder teilweise
 - Speicherortbeschränkung (nur S3)
 - Objektgröße
 - Benutzer-Metadaten
 - Objekt-Tag (nur S3)

Sie können Objekte nach sehr spezifischen Kriterien filtern. So können beispielsweise Objekte, die von der Bildgebungsabteilung eines Krankenhauses gespeichert sind, häufig verwendet werden, wenn sie weniger als 30 Tage alt und selten danach sind, während Objekte, die Angaben zu Patientenbesuchen enthalten, möglicherweise in die Rechnungsabteilung des Gesundheitsnetzwerks kopiert werden müssen. Sie können Filter erstellen, die jeden Objekttyp anhand von Objektname, -Größe, S3-Objekt-Tags oder anderen relevanten Kriterien identifizieren. Anschließend können separate Regeln erstellt werden, um jeden Objektsatz entsprechend zu speichern.

Sie können Filter nach Bedarf in einer einzigen Regel kombinieren. Beispielsweise möchte die Marketingabteilung große Bilddateien anders speichern als die Lieferantendaten, während die Personalabteilung Personaldatensätze in einer bestimmten Region und in einer bestimmten Richtlinie zentral speichern muss. In diesem Fall können Sie Regeln erstellen, die nach Mandantenkonto filtern, um die Datensätze von jeder Abteilung zu trennen, während Sie in jeder Regel Filter verwenden, um den spezifischen Objekttyp zu identifizieren, auf den die Regel angewendet wird.

Anweisungen zur Platzierung von ILM-Regeln

Eine Anleitung zur Platzierung bestimmt, wo, wann und wie Objektdaten gespeichert werden. Eine ILM-Regel kann eine oder mehrere Anweisungen zur Platzierung enthalten. Jede Einstufungsanweisung gilt für einen einzelnen Zeitraum.

Wenn Sie Anweisungen zur Platzierung erstellen:

- Sie beginnen mit der Angabe der Referenzzeit, die bestimmt, wann die Platzierungsanweisungen beginnen. Die Referenzzeit kann sein, wenn ein Objekt aufgenommen wird, wenn auf ein Objekt zugegriffen wird, wenn ein versioniertes Objekt nicht mehr aktuell wird oder eine benutzerdefinierte Zeit.
- Als Nächstes geben Sie an, wann die Platzierung in Bezug auf die Referenzzeit gelten soll. Beispielsweise kann eine Platzierung am Tag 0 beginnen und 365 Tage lang fortgesetzt werden, relativ zu dem Zeitpunkt, zu dem das Objekt aufgenommen wurde.
- Schließlich geben Sie die Art der Kopien (Replizierung oder Erasure Coding) und den Speicherort der Kopien an. So können Sie beispielsweise zwei replizierte Kopien an zwei unterschiedlichen Standorten speichern.

Jede Regel kann mehrere Platzierungen für einen einzigen Zeitraum und verschiedene Platzierungen für unterschiedliche Zeiträume definieren.

- Um Objekte in einem Zeitraum an mehreren Orten zu platzieren, wählen Sie **anderen Typ oder Standort**

hinzufügen, um mehr als eine Zeile für diesen Zeitraum hinzuzufügen.

- Um Objekte an verschiedenen Orten in verschiedenen Zeiträumen zu platzieren, wählen Sie **weiteren Zeitraum hinzufügen**, um den nächsten Zeitraum hinzuzufügen. Geben Sie dann eine oder mehrere Zeilen innerhalb des Zeitraums an.

Das Beispiel zeigt zwei Platzierungsanweisungen auf der Seite Platzierungen definieren des Assistenten zum Erstellen einer ILM-Regel.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 store for 365 days

Store objects by replicating 2 copies at Data Center 1, Data Center 2

and store objects by erasure coding using 6+3 EC scheme at All 3 sites (6 plus 3)

Add other type or location

Time period 2 From Day 365 store forever

Store objects by replicating 2 copies at Archive

Add other type or location

Die erste Platzierungsanweisung **1** Hat zwei Linien für das erste Jahr:

- In der ersten Zeile werden zwei replizierte Objektkopien an zwei Datacenter-Standorten erstellt.
- Die zweite Zeile erstellt eine Kopie mit 6 und 3 zur Fehlerkorrektur codierten Kopien unter Verwendung von drei Datacenter-Standorten.

Die zweite Platzierungsanweisung **2** Erstellt zwei archivierte Kopien nach einem Jahr und speichert diese Kopien für immer.

Wenn Sie den Satz von Anweisungen zur Platzierung für eine Regel definieren, müssen Sie sicherstellen, dass mindestens eine Platzierungsanweisung an Tag 0 beginnt, dass zwischen den von Ihnen definierten Zeiträumen keine Lücken bestehen. Und dass die abschließende Anweisung zum Platzieren entweder für immer oder bis Sie keine Objektkopien mehr benötigen.

Da jeder Zeitraum in der Regel abläuft, werden die Anweisungen zur Inhaltsplatzierung für den nächsten Zeitraum angewendet. Neue Objektkopien werden erstellt und nicht benötigte Kopien werden gelöscht.

ILM-Regel Aufnahme-Verhalten

Das Aufnahmeverhalten steuert, ob Objektkopien sofort nach den Anweisungen in der Regel platziert werden oder ob zwischenzeitliche Kopien erstellt und die Speicheranweisungen später angewendet werden. Die folgenden Aufnahmeverhalten stehen für ILM-Regeln zur Verfügung:

- **Ausgewogen:** StorageGRID versucht bei der Aufnahme alle in der ILM-Regel festgelegten Kopien zu erstellen; wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg an den Client zurückgesendet. Die Kopien, die in der ILM-Regel angegeben sind, werden, wenn möglich gemacht.
- **Streng:** Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor der Erfolg an den Client zurückgesendet wird.
- **Dual Commit:** StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Client zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

Verwandte Informationen

- ["Aufnahmeoptionen"](#)
- ["Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen"](#)
- ["Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung zu beeinträchtigen"](#)

Beispiel für eine ILM-Regel

Eine ILM-Regel könnte beispielsweise Folgendes angeben:

- Nur auf die Objekte anwenden, die zu Mandant A gehören
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Standort.
- Behalten Sie die beiden Kopien „Forever,“ bei, was bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte so lange bei, bis sie von einer Löschanfrage eines Clients oder nach Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die ausgewogene Option für das Aufnahmeverhalten: Die Anweisung zur Platzierung von zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, sofort beide erforderlichen Kopien zu erstellen.

Wenn z. B. Standort 2 nicht erreichbar ist, wenn Mandant A ein Objekt speichert, erstellt StorageGRID zwei Zwischenkopien auf Storage-Nodes an Standort 1. Sobald Standort 2 verfügbar wird, erstellt StorageGRID die erforderliche Kopie an diesem Standort.

Verwandte Informationen

- ["Was ist ein Speicherpool?"](#)
- ["Was ist ein Cloud-Storage-Pool?"](#)

Greifen Sie auf den Assistenten zum Erstellen einer ILM-Regel zu

ILM-Regeln ermöglichen es Ihnen, die Platzierung von Objektdaten im Laufe der Zeit zu managen. Zum Erstellen einer ILM-Regel verwenden Sie den Assistenten zum Erstellen einer ILM-Regel.

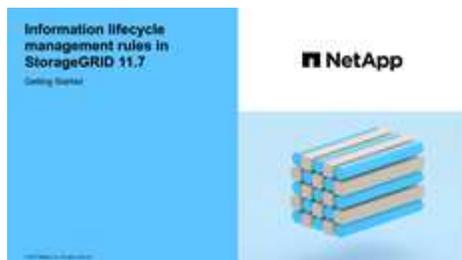


Wenn Sie die Standard-ILM-Regel für eine Richtlinie erstellen möchten, befolgen Sie die Anweisungen unter ["Anweisungen zum Erstellen einer standardmäßigen ILM-Regel"](#) Stattdessen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.

- Wenn Sie angeben möchten, für welche Mandantenkonten diese Regel gilt, verfügen Sie über die Berechtigung für die Mandantenkonten oder Sie kennen die Konto-ID für jedes Konto.
- Wenn die Regel Objekte nach Metadaten der Uhrzeit des letzten Zugriffs filtern soll, müssen die Updates der Uhrzeit des letzten Zugriffs für Bucket für S3 oder für Container für Swift aktiviert werden.
- Sie haben alle Cloud-Storage-Pools konfiguriert, die Sie verwenden möchten. Siehe "[Cloud Storage Pool Erstellen](#)".
- Sie kennen das "[Aufnahmeoptionen](#)".
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, kennen Sie die "[Anforderungen für die S3-Objektsperre](#)".
- Optional haben Sie sich das Video angesehen: "[Video: Information Lifecycle Management Regeln in StorageGRID 11.7](#)".



Über diese Aufgabe

Wenn ILM-Regeln erstellt werden:

- Dabei sind die Topologie und Storage-Konfigurationen des StorageGRID Systems zu berücksichtigen.
- Es sollte berücksichtigt werden, welche Arten von Objektkopien Sie erstellen möchten (replizierte oder Erasure Coding) und wie viele Kopien der einzelnen Objekte erforderlich sind.
- Legen Sie fest, welche Typen von Objekt-Metadaten in den Applikationen verwendet werden, die sich mit dem StorageGRID System verbinden. ILM-Regeln filtern Objekte auf Basis ihrer Metadaten.
- Dabei sollten Sie berücksichtigen, wo Sie Objektkopien über einen längeren Zeitraum ablegen möchten.
- Entscheiden Sie, welche Aufnahmeoption verwendet werden soll (ausgeglichen, streng oder doppelte Übertragung).

Schritte

1. Wählen Sie **ILM > Regeln**.

Basierend auf der Anzahl der Standorte in der Tabelle wird die Regel 2 Kopien erstellen oder die Regel 1 Kopie pro Standort in der Regelliste angezeigt.



Wenn die globale S3-Objektsperre für das StorageGRID-System aktiviert wurde, enthält die Übersichtstabelle eine Spalte **konform**, und die Details für die ausgewählte Regel enthalten ein Feld **konform**.

2. Wählen Sie **Erstellen**. "[Schritt 1 \(Details eingeben\)](#)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Schritt 1 von 3: Details eingeben

Im Schritt **Details eingeben** des Assistenten zum Erstellen einer ILM-Regel können Sie

einen Namen und eine Beschreibung für die Regel eingeben und Filter für die Regel definieren.

Die Eingabe einer Beschreibung und das Definieren von Filtern für die Regel sind optional.

Über diese Aufgabe

Bei der Auswertung eines Objekts mit einem "ILM-Regel", StorageGRID vergleicht die Objektmetadaten mit den Filtern der Regel. Wenn die Objektmetadaten mit allen Filtern übereinstimmen, verwendet StorageGRID die Regel, um das Objekt abzulegen. Sie können eine Regel für alle Objekte entwerfen oder grundlegende Filter angeben, z. B. ein oder mehrere Mandantenkonten und Bucket-Namen oder erweiterte Filter, wie z. B. Größe des Objekts oder Benutzermetadaten.

Schritte

1. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.
2. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.

Sie sollten den Zweck oder die Funktion der Regel beschreiben, damit Sie die Regel später erkennen können.

3. Wählen Sie optional ein oder mehrere S3- oder Swift-Mandantenkonten aus, für die diese Regel gilt. Wenn diese Regel für alle Mandanten gilt, lassen Sie dieses Feld leer.

Wenn Sie weder über die Berechtigung für den Root-Zugriff noch über die Berechtigung für die Mandantenkonten verfügen, können Sie keine Mandanten aus der Liste auswählen. Geben Sie stattdessen die Mandanten-ID ein, oder geben Sie mehrere IDs als durch Komma getrennte Zeichenfolge ein.

4. Geben Sie optional die S3-Buckets oder Swift-Container an, für die diese Regel gilt.

Wenn **entspricht allen** ausgewählt ist (Standard), gilt die Regel für alle S3-Buckets oder Swift-Container.

5. Wählen Sie für S3-Mandanten optional **Yes** aus, um die Regel nur auf ältere Objektversionen in S3-Buckets anzuwenden, für die die Versionierung aktiviert ist.

Wenn Sie **Ja** auswählen, wird automatisch „nicht aktuelle Zeit“ für die Referenzzeit in ausgewählt "[Schritt 2 des Assistenten zum Erstellen einer ILM-Regel](#)".



Die nicht aktuelle Zeit gilt nur für S3 Objekte in versionierungsfähigen Buckets. Siehe "[Operationen für Buckets, PUT Bucket-Versionierung](#)" Und "[Objekte managen mit S3 Object Lock](#)".

Mit dieser Option können Sie die Auswirkungen versionierter Objekte auf den Speicher reduzieren, indem Sie nach nicht aktuellen Objektversionen filtern. Siehe "[Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3](#)".

6. Wählen Sie optional **Erweiterten Filter hinzufügen**, um weitere Filter festzulegen.

Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den Grundfiltern entsprechen. Weitere Informationen zum erweiterten Filtern finden Sie unter [Verwenden Sie erweiterte Filter in ILM-Regeln](#) Und [Geben Sie mehrere Metadaten und -Werte an](#).

7. Wählen Sie **Weiter**. "[Schritt 2 \(Platzierungen definieren\)](#)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Verwenden Sie erweiterte Filter in ILM-Regeln

Mit der erweiterten Filterung können Sie ILM-Regeln erstellen, die sich nur auf bestimmte Objekte anwenden lassen, basierend auf ihren Metadaten. Wenn Sie die erweiterte Filterung für eine Regel einrichten, wählen Sie den Metadatentyp aus, der übereinstimmen soll, wählen Sie einen Operator aus und geben einen Metadatenwert an. Wenn Objekte ausgewertet werden, wird die ILM-Regel nur auf Objekte angewendet, die Metadaten enthalten, die dem erweiterten Filter entsprechen.

Die Tabelle zeigt die Metadatentypen, die Sie in den erweiterten Filtern angeben können, die Operatoren, die Sie für jeden Metadatentyp verwenden können, und die erwarteten Metadaten.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Aufnahmezeit	<ul style="list-style-type: none">• Ist• Ist es nicht• Ist vorher• Ist ein oder vorher• Ist nachher• Ist ein oder nach	<p>Uhrzeit und Datum, an dem das Objekt aufgenommen wurde.</p> <p>Hinweis: um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter für die Einspielzeit in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie für die Aufnahme-Zeit den Wert fest, der ungefähr der Zeit entspricht, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.</p>
Taste	<ul style="list-style-type: none">• Gleich• Ist nicht gleich• Enthält• Enthält nicht• Beginnt mit• Startet nicht mit• Endet mit• Endet nicht mit	<p>Der gesamte Objektschlüssel oder Teil eines eindeutigen S3- oder Swift-Objektschlüssels.</p> <p>Beispielsweise können Sie Objekte, die mit enden, aufeinander abstimmen <code>.txt</code> Oder beginnen Sie mit <code>test-object/</code>.</p>
Zeitpunkt des letzten Zugriffs	<ul style="list-style-type: none">• Ist• Ist es nicht• Ist vorher• Ist ein oder vorher• Ist nachher• Ist ein oder nach	<p>Uhrzeit und Datum, an dem das Objekt zuletzt abgerufen wurde (gelesen oder angezeigt).</p> <p>Hinweis: Wenn Sie Vorhaben "Letzte Zugriffszeit verwenden" Als erweiterter Filter müssen die Updates der Uhrzeit des letzten Zugriffs für den S3-Bucket oder Swift-Container aktiviert sein.</p>

Metadattentyp	Unterstützte Operatoren	Metadatenwert
Speicherortbeschränkung (nur S3)	<ul style="list-style-type: none"> • Gleich • Ist nicht gleich 	<p>Die Region, in der ein S3-Bucket erstellt wurde. Verwenden Sie ILM > Regionen, um die angezeigten Regionen zu definieren.</p> <p>Hinweis: Ein Wert von US-East-1 entspricht Objekten in Eimern, die in der Region US-East-1 erstellt wurden, sowie Objekten in Buckets, die keine Region angegeben haben. Siehe "Regionen konfigurieren (nur optional und S3)".</p>
Objektgröße	<ul style="list-style-type: none"> • Gleich • Ist nicht gleich • Kleiner als • Kleiner als oder gleich • Größer als • Größer als oder gleich 	<p>Die Größe des Objekts.</p> <p>Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.</p> <p>Hinweis: um nach Objektgrößen kleiner als 1 MB zu filtern, geben Sie einen Dezimalwert ein. Der Browsertyp und die Ländereinstellungen steuern, ob Sie einen Punkt oder ein Komma als Dezimaltrennzeichen verwenden müssen.</p>
Benutzer-Metadaten	<ul style="list-style-type: none"> • Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit 	<p>Schlüssel-Wert-Paar, wobei Benutzer-Metadaten-Name der Schlüssel und Metadaten-Wert der Wert ist.</p> <p>Zum Beispiel nach Objekten mit Benutzer-Metadaten von filtern <code>color=blue</code>, Spezifizieren <code>color</code> Für Name der Metadaten des Benutzers, <code>equals</code> Für den Bediener, und <code>blue</code> Für Metadatenwert.</p> <p>Hinweis: Benutzer-Metadaten-Namen sind nicht zwischen Groß- und Kleinschreibung zu beachten; Benutzer-Metadaten-Werte sind Groß- und Kleinschreibung zu beachten.</p>

Metadattentyp	Unterstützte Operatoren	Metadatenwert
Objekt-Tag (nur S3)	<ul style="list-style-type: none"> • Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit 	<p>Schlüssel-Wert-Paar, wobei Objekt-Tag-Name der Schlüssel und Objekt-Tag-Wert der Wert ist.</p> <p>Zum Beispiel, um nach Objekten zu filtern, die ein Objekt-Tag von haben <code>Image=True</code>, Spezifizieren <code>Image</code> Für Objekt-Tag-Name, <code>equals</code> Für den Bediener, und <code>True</code> Für Objekt Tag Wert.</p> <p>Hinweis: Objekt-Tag-Namen und Objekt-Tag-Werte sind Groß- und Kleinschreibung. Sie müssen diese Elemente genau so eingeben, wie sie für das Objekt definiert wurden.</p>

Geben Sie mehrere Metadattentypen und -Werte an

Wenn Sie die erweiterte Filterung definieren, können Sie mehrere Metadattentypen und mehrere Metadatenwerte angeben. Wenn Sie beispielsweise eine Regel mit Objekten zwischen 10 MB und 100 MB Größe vergleichen möchten, wählen Sie den Metadattentyp **Objektgröße** aus und geben zwei Metadatenwerte an.

- Der erste Metadatenwert gibt Objekte an, die größer oder gleich 10 MB sind.
- Der zweite Metadatenwert gibt Objekte an, die kleiner als oder gleich 100 MB sind.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼

greater than or equal to ▼

10 ⬆️

MB ▼

✕

and

Object size ▼

less than or equal to ▼

100 ⬆️

MB ▼

✕

Durch die Verwendung mehrerer Einträge können Sie genau steuern, welche Objekte abgeglichen werden. Im folgenden Beispiel gilt die Regel für Objekte, die einen Brand A oder eine Marke B als Wert der `Camera_type`-Benutzermetadaten haben. Die Regel gilt jedoch nur für Objekte der Marke B, die kleiner als 10 MB sind.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

User metadata camera_type equals Brand A ✕

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

User metadata camera_type equals Brand B ✕
and Object size less than or equal to 10 MB ✕

[Add another advanced filter](#)

Schritt 2 von 3: Definieren von Platzierungen

Im Schritt **Platzierungen definieren** des Assistenten zum Erstellen von ILM-Regeln können Sie die Platzierungsanweisungen definieren, die festlegen, wie lange Objekte gespeichert werden, welche Art von Kopien (repliziert oder Erasure codiert), den Speicherort und die Anzahl der Kopien.

Über diese Aufgabe

Eine ILM-Regel kann eine oder mehrere Anweisungen zur Platzierung enthalten. Jede Einstufungsanweisung gilt für einen einzelnen Zeitraum. Wenn Sie mehrere Befehle verwenden, müssen die Zeiträume zusammenhängend sein, und mindestens eine Anweisung muss am Tag 0 beginnen. Die Anweisungen können entweder für immer fortgesetzt werden oder bis Sie keine Objektkopien mehr benötigen.

Jede Anweisung für die Platzierung kann mehrere Zeilen haben, wenn Sie verschiedene Arten von Kopien erstellen oder verschiedene Standorte während dieses Zeitraums verwenden möchten.

In diesem Beispiel speichert die ILM-Regel eine replizierte Kopie an Standort 1 und eine replizierte Kopie am Standort 2 im ersten Jahr. Nach einem Jahr wird eine 2+1-Kopie mit Erasure-Coding-Verfahren an nur einem Standort erstellt und gespeichert.

Schritte

1. Wählen Sie unter **Referenzzeit** den Zeittyp aus, der bei der Berechnung der Startzeit für eine Platzierungsanweisung verwendet werden soll.

Option	Beschreibung
Aufnahmezeit	Die Zeit, zu der das Objekt aufgenommen wurde.
Zeitpunkt des letzten Zugriffs	Die Zeit, zu der das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde. Hinweis: um diese Option nutzen zu können, müssen die Updates für die Uhrzeit des letzten Zugriffs für den S3-Bucket oder Swift-Container aktiviert sein. Siehe " Verwenden Sie die letzte Zugriffszeit in ILM-Regeln ".

Option	Beschreibung
Benutzerdefinierte Erstellungszeit	Eine in benutzerdefinierten Metadaten angegebene Zeit.
Nicht aktuelle Zeit	„nicht aktuelle Zeit“ wird automatisch ausgewählt, wenn Sie für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ ausgewählt haben. Zoll "Schritt 1 des Assistenten zum Erstellen einer ILM-Regel" .



Wenn Sie eine konforme Regel erstellen möchten, müssen Sie **Ingest Time** auswählen. Siehe ["Objekte managen mit S3 Object Lock"](#).

2. Geben Sie im Abschnitt **Zeitraum und Platzierungen** eine Startzeit und eine Dauer für den ersten Zeitraum ein.

Sie können beispielsweise festlegen, wo Objekte für das erste Jahr gespeichert werden sollen (*von Tag 0 für 365 Tage*). Mindestens eine Anweisung muss am Tag 0 beginnen.

3. So erstellen Sie replizierte Kopien:

- a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Replizieren** aus.
- b. Wählen Sie die Anzahl der Kopien aus, die Sie erstellen möchten.

Wenn Sie die Anzahl der Kopien in 1 ändern, wird eine Warnung angezeigt. Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Siehe ["Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden"](#).

Um dieses Risiko zu vermeiden, führen Sie einen oder mehrere der folgenden Schritte aus:

- Erhöhen Sie die Anzahl der Kopien für den Zeitraum.
- Fügen Sie Kopien zu anderen Speicherpools oder zu einem Cloud-Speicherpool hinzu.
- Wählen Sie **Erasure Coding** anstelle von **replizierung**.

Sie können diese Warnung ohne Bedenken ignorieren, wenn diese Regel bereits mehrere Kopien für alle Zeiträume erstellt.

- c. Wählen Sie im Feld **copies at** die Speicherpools aus, die Sie hinzufügen möchten.

Wenn Sie nur einen Speicherpool angeben, beachten Sie, dass StorageGRID nur eine replizierte Kopie eines Objekts auf einem beliebigen Speicherknoten speichern kann. Wenn Ihr Raster drei Storage-Nodes enthält und Sie 4 als Anzahl der Kopien auswählen, werden nur drei Kopien erstellt—eine Kopie für jeden Storage-Node.



Die Warnung **ILM-Platzierung unerreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Wenn Sie mehr als einen Speicherpool angeben, beachten Sie folgende Regeln:

- Die Anzahl der Kopien darf nicht größer sein als die Anzahl der Speicherpools.
- Wenn die Anzahl der Kopien der Anzahl der Storage-Pools entspricht, wird in jedem Storage-Pool

eine Kopie des Objekts gespeichert.

- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Storage-Pools, wird eine Kopie am Aufnahmeort gespeichert, und das System verteilt die restlichen Kopien, um die Festplattennutzung unter den Pools gleichmäßig zu halten. Dabei wird sichergestellt, dass kein Standort mehr als eine Kopie eines Objekts erhält.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Geben Sie daher nicht den Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) und einen anderen Speicherpool an.

4. Wenn Sie eine Kopie mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) erstellen möchten:

- a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Erasure Coding** aus.



Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

- b. Wenn Sie keinen Filter für die Objektgröße für einen Wert größer als 0.2 MB hinzugefügt haben, wählen Sie **Zurück**, um zu Schritt 1 zurückzukehren. Wählen Sie dann **Erweiterten Filter hinzufügen** und setzen Sie einen **Objektgröße**-Filter auf einen Wert größer als 0.2 MB.
- c. Wählen Sie den Speicherpool aus, den Sie hinzufügen möchten, und das Erasure-Coding-Schema, das Sie verwenden möchten.

Der Speicherort für eine Kopie, die nach der Fehlerkorrektur codiert wurde, enthält den Namen des Erasure Coding-Schemas und den Namen des Storage-Pools.

5. Optional:

- a. Wählen Sie **anderen Typ oder Speicherort hinzufügen**, um weitere Kopien an verschiedenen Standorten zu erstellen.
- b. Wählen Sie **weiteren Zeitraum hinzufügen**, um verschiedene Zeiträume hinzuzufügen.



Objekte werden am Ende des Endzeitraums automatisch gelöscht, es sei denn, der Endzeitraum endet mit **forever**.

6. Wenn Sie Objekte in einem Cloud-Speicherpool speichern möchten:

- a. Wählen Sie in der Dropdown-Liste **Objekte speichern nach Replizieren** aus.
- b. Wählen Sie das Feld **copies at** aus, und wählen Sie dann einen Cloud-Speicherpool aus.

Beachten Sie bei der Verwendung von Cloud-Storage-Pools folgende Regeln:

- Sie können nicht mehr als einen Cloud Storage-Pool in einer einzelnen Anweisung auswählen. Ebenso können Sie keinen Cloud-Storage-Pool und keinen Storage-Pool in derselben Anweisung auswählen.
- Sie können nur eine Kopie eines Objekts in einem beliebigen Cloud Storage Pool speichern. Wenn Sie **Copies** auf 2 oder mehr setzen, wird eine Fehlermeldung angezeigt.
- Es können nicht mehr als eine Objektkopie gleichzeitig in einem Cloud-Storage-Pool gespeichert werden. Eine Fehlermeldung wird angezeigt, wenn mehrere Platzierungen, die einen Cloud-Speicher-Pool verwenden, sich überschneidende Daten aufweisen oder wenn mehrere Zeilen

derselben Platzierung einen Cloud-Storage-Pool verwenden.

- Ein Objekt kann in einem Cloud-Storage-Pool gleichzeitig gespeichert werden, als replizierte oder als Erasure Coding-Kopie in StorageGRID. Sie müssen jedoch für den Zeitraum mehr als eine Zeile in die Platzierungsanweisung aufnehmen, damit Sie die Anzahl und die Typen der Kopien für jeden Speicherort angeben können.

7. Bestätigen Sie im Aufbewahrungsdiagramm Ihre Platzierungsanweisungen.

Jede Zeile im Diagramm zeigt an, wo und wann Objektkopien platziert werden. Die Farbe einer Linie steht für den Kopiertyp:

	Replizierte Kopie
	Kopie mit Erasure Coding – eine Kopie
	Cloud-Storage-Pool-Kopie

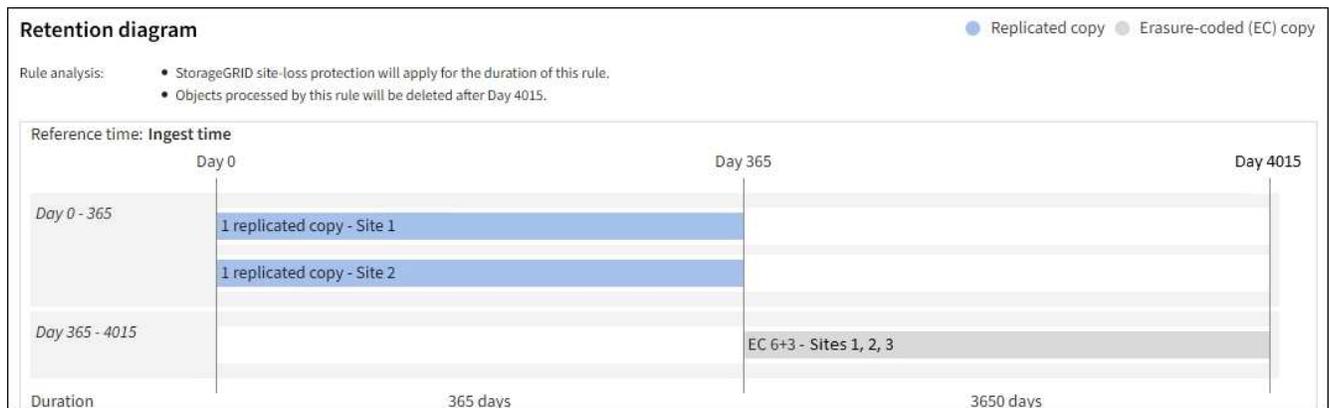
In diesem Beispiel speichert die ILM-Regel eine replizierte Kopie an Standort 1 und eine replizierte Kopie am Standort 2 im ersten Jahr. Nach einem Jahr und für weitere 10 Jahre wird eine 6+3 Erasure-coded Kopie an drei Standorten gespeichert. Nach insgesamt 11 Jahren werden die Objekte aus StorageGRID gelöscht.

Im Abschnitt Regelanalyse des Aufbewahrungsdiagramms steht Folgendes:

- Für die Dauer dieser Regel gilt eine StorageGRID-Sicherung gegen vor-Ort-Verlust.
- Durch diese Regel verarbeitete Objekte werden nach Tag 4015 gelöscht.



Siehe "[Schutz vor Standortausfällen](#)"



8. Wählen Sie **Weiter**. "[Schritt 3 \(Aufnahmeverhalten auswählen\)](#)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Verwenden Sie die letzte Zugriffszeit in ILM-Regeln

Sie können die Uhrzeit des letzten Zugriffs als Referenzzeit in einer ILM-Regel verwenden. Sie möchten beispielsweise Objekte, die in den letzten drei Monaten auf lokalen Speicherknoten angezeigt wurden, während Sie Objekte verschieben, die noch nicht in letzter Zeit an einen externen Standort betrachtet wurden. Sie können die Uhrzeit

des letzten Zugriffs auch als erweiterten Filter verwenden, wenn eine ILM-Regel nur auf Objekte angewendet werden soll, auf die an einem bestimmten Datum zuletzt zugegriffen wurde.

Über diese Aufgabe

Bevor Sie die letzte Zugriffszeit in einer ILM-Regel verwenden, sollten Sie die folgenden Überlegungen durchgehen:

- Wenn Sie die Uhrzeit des letzten Zugriffs als Referenzzeit verwenden, beachten Sie, dass die Änderung der Uhrzeit des letzten Zugriffs für ein Objekt keine sofortige ILM-Bewertung auslöst. Stattdessen werden die Platzierungen des Objekts bewertet und das Objekt nach Bedarf verschoben, wenn im Hintergrund ILM das Objekt bewertet wird. Dies kann zwei Wochen oder länger dauern, nachdem auf das Objekt zugegriffen wurde.

Berücksichtigen Sie diese Latenz bei der Erstellung von ILM-Regeln auf der Grundlage der letzten Zugriffszeit und vermeiden Sie Platzierungen, die kurze Zeiträume (weniger als einen Monat) verwenden.

- Wenn Sie die letzte Zugriffszeit als erweiterten Filter oder als Referenzzeit verwenden, müssen Sie die Updates der letzten Zugriffszeit für S3-Buckets aktivieren. Sie können das verwenden "[Mandanten-Manager](#)" Oder im "[Mandantenmanagement-API](#)".



Updates der letzten Zugriffszeit sind immer für Swift Container aktiviert. Für S3 Buckets sind sie jedoch standardmäßig deaktiviert.



Beachten Sie, dass eine Aktualisierung der letzten Zugriffszeit die Performance beeinträchtigen kann, insbesondere bei Systemen mit kleinen Objekten. Die Auswirkungen auf die Performance werden dadurch erzielt, dass StorageGRID die Objekte bei jedem Abruf mit neuen Zeitstempel aktualisieren muss.

In der folgenden Tabelle wird zusammengefasst, ob die Uhrzeit des letzten Zugriffs für alle Objekte im Bucket für verschiedene Arten von Anforderungen aktualisiert wird.

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit deaktiviert sind	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit aktiviert sind
Anforderung zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Ja.
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	<ul style="list-style-type: none"> • Nein, für die Quellkopie • Ja, für die Zielkopie 	<ul style="list-style-type: none"> • Ja, für die Quellkopie • Ja, für die Zielkopie

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit deaktiviert sind	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit aktiviert sind
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritt 3 von 3: Wählen Sie Ingest Behavior

Im Schritt **Einspielverhalten auswählen** des Assistenten zum Erstellen von ILM-Regeln können Sie festlegen, wie die von dieser Regel gefilterten Objekte bei der Aufnahme geschützt werden.

Über diese Aufgabe

StorageGRID erstellt Zwischenkopien und stellt die Objekte später zur ILM-Evaluierung in einen Warteschleife. Außerdem kann es Kopien erstellen, um sofort die Anweisungen zur Platzierung der Regel zu erfüllen.

Schritte

1. Wählen Sie die aus **"Aufnahmeverhalten"** Zu verwenden.

Weitere Informationen finden Sie unter **"Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen"**.



Sie können die Option „ausgeglichen“ oder „streng“ nicht verwenden, wenn die Regel eine dieser Platzierungen verwendet:

- Ein Cloud-Storage-Pool am Tag 0
- Ein Archiv-Node am Tag 0
- Ein Cloud-Speicherpool oder ein Archivknoten, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit verwendet

Siehe **"Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"**.

2. Wählen Sie **Erstellen**.

Die ILM-Regel wird erstellt. Die Regel wird erst aktiv, wenn sie zu einem hinzugefügt wird **"ILM-Richtlinie"** Und diese Richtlinie ist aktiviert.

Um die Details der Regel anzuzeigen, wählen Sie den Namen der Regel auf der Seite ILM-Regeln aus.

Erstellen einer Standard-ILM-Regel

Bevor Sie eine ILM-Richtlinie erstellen, müssen Sie eine Standardregel erstellen, um Objekte zu platzieren, die nicht mit einer anderen Regel in der Richtlinie übereinstimmt. Die Standardregel kann keine Filter verwenden. Die Lösung muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet **"Unterstützter Webbrowser"**.

- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die Standardregel ist die letzte Regel, die in einer ILM-Richtlinie evaluiert werden muss, sodass keine Filter verwendet werden können. Die Platzierungsanweisungen für die Standardregel werden auf alle Objekte angewendet, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen.

In diesem Beispiel gilt die erste Regel nur für Objekte, die zu Test-Tenant-1 gehören. Die letzte Standardregel gilt für Objekte, die zu allen anderen Mandantenkonten gehören.

Proposed policy name

Reason for change

Manage rules

1. Select the rules you want to add to the policy.
 2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	EC for test-tenant-1 	Tenant is test-tenant-1
Default	Default rule	—

Beachten Sie beim Erstellen der Standardregel die folgenden Anforderungen:

- Die Standardregel wird automatisch als letzte Regel in der Richtlinie gesetzt.
- Die Standardregel kann keine einfachen oder erweiterten Filter verwenden.
- Die Standardregel muss auf alle Objektversionen angewendet werden.
- Die Standardregel sollte replizierte Kopien erstellen.



Verwenden Sie keine Regel, die Kopien, die nach der Löschung codiert wurden, als Standardregel für eine Richtlinie erstellt. Für Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) sollte ein erweiterter Filter verwendet werden, um zu verhindern, dass bei kleineren Objekten die Codierung von Datenkonsistenz erfolgt.

- Im Allgemeinen sollte die Standardregel Objekte für immer aufbewahren.
- Wenn Sie die globale S3-Objektsperre verwenden (oder diese aktivieren möchten), muss die Standardregel für die aktive oder vorgeschlagene Richtlinie konform sein.

Schritte

1. Wählen Sie **ILM > Regeln**.

2. Wählen Sie **Erstellen**.

Schritt 1 (Details eingeben) des Assistenten zum Erstellen von ILM-Regeln wird angezeigt.

3. Geben Sie einen eindeutigen Namen für die Regel in das Feld **Regelname** ein.
4. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.
5. Lassen Sie das Feld **Tenant Accounts** leer.

Die Standardregel muss auf alle Mandantenkonten angewendet werden.

6. Lassen Sie die Dropdown-Liste „Bucket Name“ als **Matches all** ausgewählt.

Die Standardregel muss auf alle S3-Buckets und Swift-Container angewendet werden.

7. Behalten Sie die Standardantwort **Nein** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ bei.
8. Fügen Sie keine erweiterten Filter hinzu.

Die Standardregel kann keine Filter angeben.

9. Wählen Sie **Weiter**.

Schritt 2 (Platzierungen definieren) wird angezeigt.

10. Wählen Sie für Referenzzeit eine beliebige Option aus.

Wenn Sie die Standardantwort **Nein** für die Frage beibehalten haben, „Diese Regel nur auf ältere Objektversionen anwenden?“ Nicht aktuelle Zeit wird nicht in die Pulldown-Liste aufgenommen. Die Standardregel muss alle Objektversionen anwenden.

11. Legen Sie die Anweisungen für die Platzierung der Standardregel fest.

- Die Standardregel sollte Objekte für immer aufbewahren. Wenn die Standardregel Objekte nicht dauerhaft enthält, wird eine Warnung angezeigt, wenn Sie eine neue Richtlinie aktivieren. Sie müssen bestätigen, dass dies das Verhalten ist, das Sie erwarten.
- Die Standardregel sollte replizierte Kopien erstellen.



Verwenden Sie keine Regel, die Kopien, die nach der Löschung codiert wurden, als Standardregel für eine Richtlinie erstellt. Die Regeln für das Erasure Coding sollten den erweiterten Filter **Object size (MB) größer als 0.2** enthalten, um zu verhindern, dass kleinere Objekte Erasure Coded werden.

- Wenn Sie die globale S3-Objektsperre verwenden (oder diese aktivieren möchten), muss die Standardregel konform sein:
 - Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
 - Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Platzierung vorhanden sein.
 - Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
 - Objektkopien können nicht auf Archivknoten gespeichert werden.
 - Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei die

Einspielzeit als Referenzzeit verwendet wird.

- Mindestens eine Zeile der Platzierungsanweisungen muss „Forever“ sein.

12. Sehen Sie sich das Aufbewahrungsdiagramm an, um Ihre Platzierungsanweisungen zu bestätigen.

13. Wählen Sie **Weiter**.

Schritt 3 (Aufnahmeverhalten auswählen) wird angezeigt.

14. Wählen Sie die zu verwendende Ingest-Option und dann **Create**.

ILM-Richtlinie erstellen

Erstellen Sie eine ILM-Richtlinie: Überblick

Eine Information Lifecycle Management-Richtlinie (ILM) ist ein bestellter Satz von ILM-Regeln, die bestimmen, wie das StorageGRID System Objektdaten über einen längeren Zeitraum managt.

Bei der Erstellung einer ILM-Richtlinie wählen Sie zunächst die ILM-Regeln aus und ordnen sie an. Anschließend überprüfen Sie das Verhalten Ihrer vorgeschlagenen Richtlinie, indem Sie sie mit zuvor aufgenommenen Objekten simulieren. Wenn Sie damit zufrieden sind, dass die vorgeschlagene Richtlinie wie vorgesehen funktioniert, können Sie sie aktivieren, um die aktive Richtlinie zu erstellen.



Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Standardmäßige ILM-Richtlinie

Wenn Sie StorageGRID installieren und Standorte hinzufügen, wird automatisch eine standardmäßige ILM-Richtlinie erstellt. Wenn Ihr Raster einen Standort enthält, enthält die Standardrichtlinie eine Standardregel, die zwei Kopien jedes Objekts an diesem Standort repliziert. Wenn Ihr Raster mehr als einen Standort enthält, repliziert die Standardregel eine Kopie jedes Objekts an jedem Standort.

Entspricht die Standardrichtlinie nicht Ihren Storage-Anforderungen, können Sie eigene Regeln und Richtlinien erstellen. Siehe ["Was ist eine ILM-Regel"](#) und ["Erstellen einer vorgeschlagenen ILM-Richtlinie"](#).

Wie evaluiert eine ILM-Richtlinie Objekte?

Die aktive ILM-Richtlinie für Ihr StorageGRID System steuert die Platzierung, Dauer und Datensicherung aller Objekte.

Wenn Clients Objekte in StorageGRID speichern, werden die Objekte anhand der bestellten ILM-Regeln in der aktiven Richtlinie bewertet:

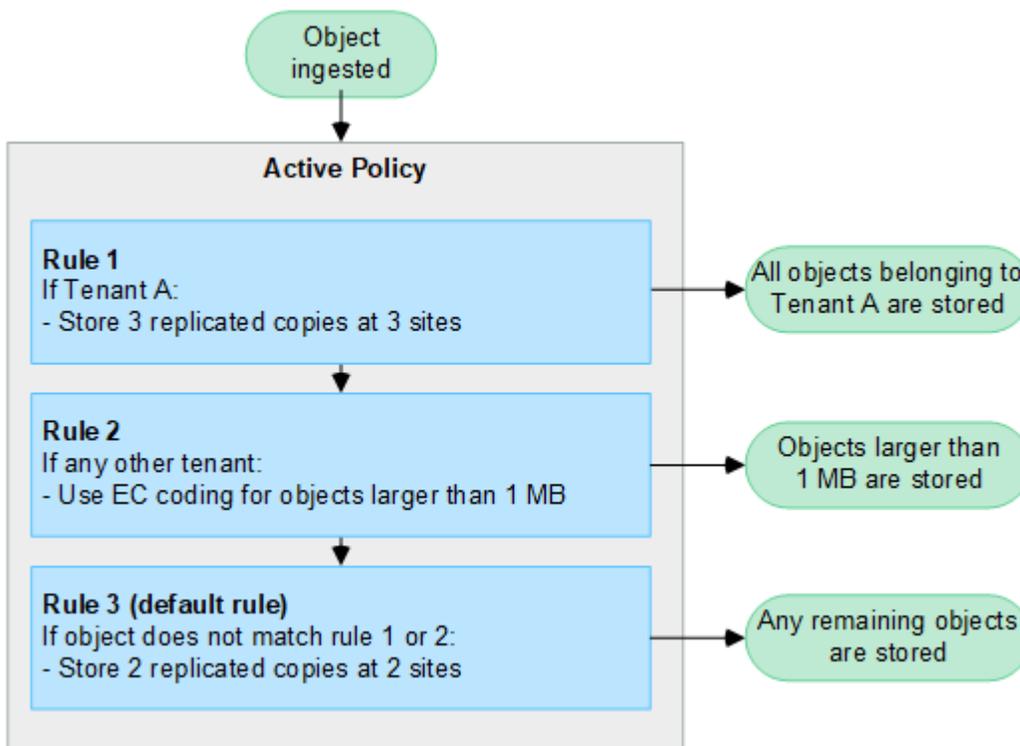
1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten der Regel aufgenommen und gemäß den Anweisungen zur Platzierung dieser Regel gespeichert.
2. Wenn die Filter für die erste Regel nicht mit dem Objekt übereinstimmen, wird das Objekt anhand jeder nachfolgenden Regel in der Richtlinie bewertet, bis eine Übereinstimmung vorgenommen wird.
3. Stimmen keine Regeln mit einem Objekt überein, werden das Aufnahmeverhalten und die Anweisungen

zur Platzierung der Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie. Die Standardregel muss für alle Mandanten, alle Buckets und alle Objektversionen gelten und kann keine erweiterten Filter verwenden.

Beispiel für eine ILM-Richtlinie

Eine ILM-Richtlinie könnte beispielsweise drei ILM-Regeln enthalten, die Folgendes angeben:

- **Regel 1: Replizierte Kopien für Mandant A**
 - Alle Objekte, die zu Mandant A gehören, abgleichen
 - Speichern Sie diese Objekte als drei replizierte Kopien an drei Standorten.
 - Objekte, die zu anderen Mandanten gehören, werden nicht mit Regel 1 abgeglichen, daher werden sie mit Regel 2 verglichen.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
 - Alle Objekte von anderen Mandanten abgleichen, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert.
 - Entspricht nicht Objekten mit einer Größe von 1 MB oder weniger, daher werden diese Objekte mit Regel 3 verglichen.
- **Regel 3: 2 Exemplare 2 Rechenzentren (Standard)**
 - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
 - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und mindestens 1 MB groß sind).



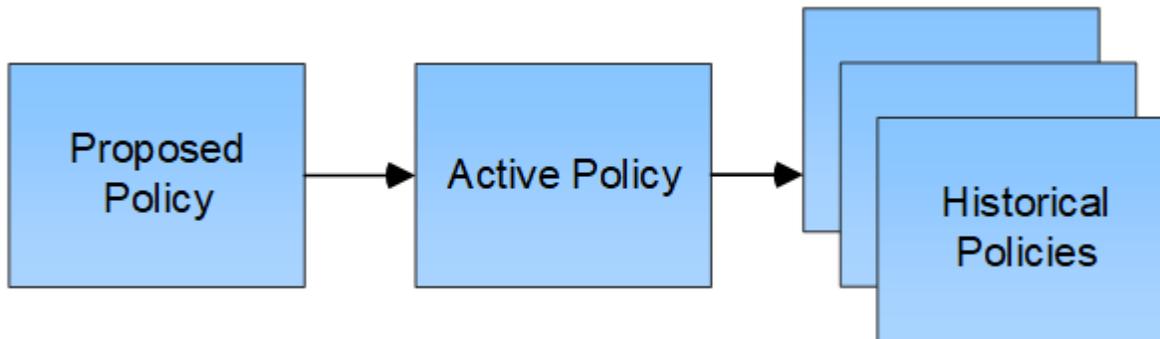
Was sind vorgeschlagene, aktive und historische Politiken?

Jedes StorageGRID System muss über eine aktive ILM-Richtlinie verfügen. Ein StorageGRID System kann auch über eine vorgeschlagene ILM-Richtlinie und eine beliebige Anzahl an historischen Richtlinien verfügen.

Beim ersten Erstellen einer ILM-Richtlinie erstellen Sie eine vorgeschlagene Richtlinie, indem Sie eine oder mehrere ILM-Regeln auswählen und in einer bestimmten Reihenfolge anordnen. Nachdem Sie die vorgeschlagene Richtlinie simuliert haben, um ihr Verhalten zu bestätigen, aktivieren Sie sie, um die aktive Richtlinie zu erstellen.

Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID diese Richtlinie, um alle Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte, zu managen. Vorhandene Objekte können an neue Standorte verschoben werden, wenn die ILM-Regeln der neuen Richtlinie implementiert werden.

Die Aktivierung der vorgeschlagenen Richtlinie führt dazu, dass die zuvor aktive Richtlinie zu einer historischen Politik wird. Historische ILM-Richtlinien können nicht gelöscht werden.



Überlegungen bei der Erstellung einer ILM-Richtlinie

- Verwenden Sie die vom System bereitgestellte Richtlinie, Richtlinie für Baseline 2 Kopien, nur in Testsystemen. Für StorageGRID 11.6 und frühere Versionen verwendet die Regel 2 Kopien erstellen in dieser Richtlinie den Speicherpool Alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.



Der Speicherpool Alle Speicherknoten wird automatisch während der Installation von StorageGRID 11.6 und früher erstellt. Wenn Sie ein Upgrade auf eine höhere Version von StorageGRID durchführen, ist der Pool Alle Storage-Nodes weiterhin vorhanden. Wenn Sie StorageGRID 11.7 oder höher als neue Installation installieren, wird der Pool Alle Speicherknoten nicht erstellt.

- Berücksichtigen Sie beim Entwurf einer neuen Richtlinie alle unterschiedlichen Objekttypen, die in das Grid aufgenommen werden können. Stellen Sie sicher, dass die Richtlinie Regeln enthält, die mit diesen Objekten übereinstimmen und sie nach Bedarf platziert werden können.
- Halten Sie die ILM-Richtlinie so einfach wie möglich. Dadurch werden potenziell gefährliche Situationen vermieden, in denen Objektdaten nicht wie vorgesehen geschützt werden, wenn im Laufe der Zeit Änderungen am StorageGRID System vorgenommen werden.
- Stellen Sie sicher, dass die Regeln in der Richtlinie in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen. Wenn z. B. die erste Regel in einer Richtlinie mit einem Objekt übereinstimmt, wird dieses Objekt nicht von einer anderen Regel bewertet.
- Die letzte Regel in jeder ILM-Richtlinie ist die standardmäßige ILM-Regel, die keine Filter verwenden kann. Wenn ein Objekt nicht mit einer anderen Regel übereinstimmt, steuert die Standardregel, wo das Objekt platziert wird und wie lange es aufbewahrt wird.
- Überprüfen Sie vor der Aktivierung einer neuen Richtlinie alle Änderungen, die die Richtlinie an der Platzierung vorhandener Objekte vornimmt. Das Ändern des Speicherorts eines vorhandenen Objekts

kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Erstellen einer vorgeschlagenen ILM-Richtlinie

Sie können eine vorgeschlagene ILM-Richtlinie von Grund auf erstellen oder die aktuelle aktive Richtlinie klonen, wenn Sie mit demselben Regelsatz beginnen möchten.

Bevor Sie eine eigene Richtlinie erstellen, überprüfen Sie, ob die ["Standardmäßige ILM-Richtlinie"](#) Erfüllt Ihre Storage-Anforderungen nicht.



Wenn der ["Die Einstellung für die globale S3-Objektsperre wurde aktiviert"](#), Sie müssen sicherstellen, dass die ILM-Richtlinie den Anforderungen von Buckets entspricht, für die S3 Object Lock aktiviert ist. Befolgen Sie in diesem Abschnitt die Anweisungen, die erwähnen, dass S3 Object Lock aktiviert ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Erforderliche Zugriffsberechtigungen"](#).
- Das ist schon ["ILM-Regeln wurden erstellt"](#) Basierend darauf, ob S3 Object Lock aktiviert ist.

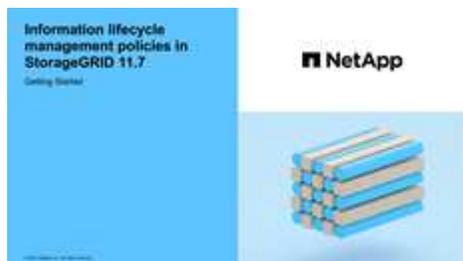
S3 Objektsperre nicht aktiviert

- Das ist schon ["ILM-Regeln erstellt"](#) Sie möchten der vorgeschlagenen Richtlinie hinzufügen. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
- Das ist schon ["Eine Standard-ILM-Regel wurde erstellt"](#) Das keine Filter enthält.

S3-Objektsperre aktiviert

- Der ["Die Einstellung für die globale S3-Objektsperre ist bereits aktiviert"](#) Für das StorageGRID-System.
- Das ist schon ["Erstellung der konformen und nicht konformen ILM-Regeln"](#) Sie möchten der vorgeschlagenen Richtlinie hinzufügen. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
- Das ist schon ["Eine Standard-ILM-Regel wurde erstellt"](#) Für die Richtlinie, die konform ist.

- Optional haben Sie sich das Video angesehen: ["Video: Information Lifecycle Management Policies in StorageGRID 11.7"](#)



Siehe auch ["Erstellen Sie eine ILM-Richtlinie: Überblick"](#).

Über diese Aufgabe

Typische Gründe für die Erstellung einer vorgeschlagenen ILM-Richtlinie sind:

- Sie haben einen neuen Standort hinzugefügt und müssen neue ILM-Regeln verwenden, um Objekte an diesem Standort zu platzieren.
- Sie müssen einen Standort stilllegen und alle ILM-Regeln entfernen, die sich auf den Standort beziehen.
- Sie haben einen neuen Mandanten mit besonderen Anforderungen an die Datensicherheit hinzugefügt.
- Sie haben damit begonnen, einen Cloud-Storage-Pool zu verwenden.



Verwenden Sie die vom System bereitgestellte Richtlinie, Richtlinie für Baseline 2 Kopien, nur in Testsystemen. Für StorageGRID 11.6 und früher verwendet die Standardregel in dieser Richtlinie den Speicherpool Alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

Schritte

1. Wählen Sie **ILM > Richtlinien**.

Wenn die globale S3 Object Lock-Einstellung aktiviert ist, gibt die Seite ILM-Richtlinien an, welche ILM-Regeln konform sind.

2. Legen Sie fest, wie Sie die vorgeschlagene ILM-Richtlinie erstellen möchten. +

Beginnen Sie von vorne

1. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie **vorgeschlagene Richtlinie > Aktionen > Entfernen** aus.

Sie können keine neue vorgeschlagene Richtlinie erstellen, wenn bereits eine vorgeschlagene Richtlinie vorhanden ist.

2. Wählen Sie **vorgeschlagene Richtlinie erstellen > Neue Richtlinie erstellen**.

Beginnen Sie mit Regeln aus der aktiven Richtlinie

1. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie **vorgeschlagene Richtlinie > Aktionen > Entfernen** aus.

Sie können die aktive Richtlinie nicht klonen, wenn bereits eine vorgeschlagene Richtlinie vorhanden ist.

2. Wählen Sie **vorgeschlagene Richtlinie erstellen > aktive Richtlinie klonen**.

Vorhandene vorgeschlagene Richtlinie bearbeiten

1. Wählen Sie **vorgeschlagene Richtlinie > Aktionen > Bearbeiten**.

1. Geben Sie im Feld **vorgeschlagener Richtlinienname** einen eindeutigen Namen für die vorgeschlagene Richtlinie ein.
2. Geben Sie im Feld **Grund für Änderung** den Grund ein, aus dem Sie eine neue vorgeschlagene Richtlinie erstellen.
3. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**. Wählen Sie einen Regelnamen

aus, um die Einstellungen für diese Regel anzuzeigen.



In regelmäßigen Abständen wird die Liste der Regeln automatisch aktualisiert, um Hinzufügungen oder Entnahmen zu berücksichtigen. Wenn eine Regel entfernt wird, nachdem Sie sie ausgewählt haben, wird eine Fehlermeldung angezeigt.

Beim Klonen einer Richtlinie:

- Die von der Richtlinie, die Sie klonen, verwendeten Regeln sind ausgewählt.
- Wenn die Richtlinie, die Sie klonen, Regeln ohne Filter verwendet hat, die nicht die Standardregel waren, werden Sie aufgefordert, alle Regeln außer einer dieser Regeln zu entfernen.
- Wenn die Standardregel einen Filter verwendet hat, werden Sie aufgefordert, eine neue Standardregel auszuwählen.
- Wenn die Standardregel nicht die letzte Regel war, können Sie die Regel an das Ende der neuen Richtlinie verschieben.

S3 Objektsperre nicht aktiviert

1. Wählen Sie eine Standardregel für die vorgeschlagene Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite** aus .

Die Standardregel gilt für alle Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen. Die Standardregel kann keine Filter verwenden und wird immer zuletzt ausgewertet.



Verwenden Sie nicht die Regel 2 Kopien erstellen als Standardregel für eine Richtlinie. Die Regel 2 Kopien erstellen verwendet einen einzelnen Speicherpool, alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

S3-Objektsperre aktiviert

1. Wählen Sie eine Standardregel für die vorgeschlagene Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite** aus .

Die Liste der Regeln enthält nur die Regeln, die konform sind und keine Filter verwenden.



Verwenden Sie nicht die Regel 2 Kopien erstellen als Standardregel für eine Richtlinie. Die Regel 2 Kopien erstellen verwendet einen einzelnen Speicherpool, alle Speicherknoten, der alle Standorte enthält. Wenn Sie diese Regel verwenden, können mehrere Kopien eines Objekts auf demselben Standort platziert werden.

2. Wenn Sie eine andere "default"-Regel für Objekte in nicht konformen S3-Buckets benötigen, wählen Sie **eine Regel ohne Filter für nicht konforme S3-Buckets** aus und wählen Sie eine nicht konforme Regel aus, die keinen Filter verwendet.

Sie können beispielsweise einen Cloud-Storage-Pool verwenden, um Objekte in Buckets zu speichern, für die die S3-Objektsperre nicht aktiviert ist.



Sie können nur eine nicht kompatible Regel auswählen, die keinen Filter verwendet.

Siehe auch "[Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock](#)".

1. Wenn Sie mit der Auswahl der Standardregel fertig sind, wählen Sie **Weiter**.
2. Wählen Sie für den Schritt andere Regeln alle anderen Regeln aus, die Sie der Richtlinie hinzufügen möchten. Diese Regeln verwenden mindestens einen Filter (Mandantenkonto, Bucket-Name, erweiterter Filter oder nicht aktuelle Referenzzeit). Wählen Sie dann **Select**.

Im Fenster vorgeschlagene Richtlinie erstellen werden nun die ausgewählten Regeln aufgelistet. Die Standardregel ist am Ende, mit den anderen Regeln darüber.

Wenn S3 Object Lock aktiviert ist und Sie außerdem eine nicht konforme Regel „default“ ausgewählt haben, wird diese Regel als die zweitrangige Regel in der Richtlinie hinzugefügt.



Eine Warnung wird angezeigt, wenn eine Regel Objekte nicht für immer behält. Wenn Sie diese Richtlinie aktivieren, müssen Sie bestätigen, dass StorageGRID Objekte löschen soll, wenn die Platzierungsanweisungen für die Standardregel abgelaufen sind (es sei denn, ein Bucket-Lebenszyklus hält die Objekte für einen längeren Zeitraum).

3. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

Sie können die Standardregel nicht verschieben. Wenn S3 Object Lock aktiviert ist, können Sie die nicht konforme Regel „default“ auch nicht verschieben, wenn eine ausgewählt wurde.



Sie müssen sich vergewissern, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen.

4. Wählen Sie bei Bedarf **Regeln auswählen**, um Regeln hinzuzufügen oder zu entfernen.
5. Wenn Sie fertig sind, wählen Sie **Speichern**.
6. Gehen Sie zu "[Simulation einer ILM-Richtlinie](#)". Sie sollten eine vorgeschlagene Richtlinie immer simulieren, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie erwartet funktioniert.

Simulation einer ILM-Richtlinie

Simulieren Sie eine vorgeschlagene Richtlinie für Testobjekte, bevor Sie die Richtlinie aktivieren und auf Ihre Produktionsdaten anwenden. Das Simulationsfenster bietet eine eigenständige Umgebung, die zum Testen von Richtlinien sicher ist, bevor sie aktiviert und auf Daten in der Produktionsumgebung angewendet werden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Erforderliche Zugriffsberechtigungen](#)".
- Für jedes zu testende Objekt ist der S3-Bucket/Objektschlüssel oder der Swift-Container-/Objektname bekannt.

Über diese Aufgabe

Wählen Sie sorgfältig die Objekte aus, die die vorgeschlagene Richtlinie testen soll. Um eine Richtlinie gründlich zu simulieren, sollten Sie mindestens ein Objekt für jeden Filter in jeder Regel testen.

Wenn eine Richtlinie beispielsweise eine Regel enthält, mit der Objekte in Bucket A und eine andere Regel übereinstimmen, um Objekte in Bucket B zu entsprechen, müssen Sie mindestens ein Objekt aus Bucket A und ein Objekt aus Bucket B auswählen, um die Richtlinie gründlich zu testen. Sie müssen außerdem mindestens ein Objekt aus einem anderen Bucket auswählen, um die Standardregel zu testen.

Bei der Simulation einer Richtlinie gelten folgende Überlegungen:

- Nachdem Sie Änderungen an einer Richtlinie vorgenommen haben, speichern Sie die vorgeschlagene Richtlinie. Dann simulieren Sie das Verhalten der gespeicherten vorgeschlagenen Richtlinie.
- Wenn Sie eine Richtlinie simulieren, filtern die ILM-Regeln in der Richtlinie die Testobjekte ab, sodass Sie sehen können, welche Regel auf jedes Objekt angewendet wurde. Es werden jedoch keine Objektkopien erstellt und keine Objekte abgelegt. Wenn Sie eine Simulation ausführen, ändern Sie Ihre Daten, Regeln oder Richtlinien in keiner Weise.

- Das Fenster vorgeschlagene Richtlinie simulieren behält die getesteten Objekte bei, bis Sie entweder **Alle löschen** oder das Symbol entfernen auswählen ✕ Für jedes Objekt in der Liste Simulationsergebnisse.
- Simulation gibt den Namen der übereinstimmenden Regel zurück. Um zu ermitteln, welches Profil für den Speicherpool oder die Erasure Coding-Funktion verwendet wird, wählen Sie den Namen der Regel aus, um auf die Seite mit den Regeldetails zu gelangen. Dort können Sie das Aufbewahrungsdigramm sowie weitere Details zur Regel anzeigen.
- Wenn die S3-Versionierung aktiviert ist, können Sie die Versions-ID für die Version des Objekts eingeben, das Sie für die Simulation verwenden möchten.

Schritte

1. "Erstellen Sie eine vorgeschlagene Richtlinie".
2. Verwenden eines S3- oder Swift-Clients oder des "Experimentelle S3 Konsole", Die im Tenant Manager für jeden Mandanten verfügbar ist, geben Sie die Objekte ein, die zum Testen jeder Regel erforderlich sind.
3. Wählen Sie auf der ILM-Richtlinienseite, Registerkarte vorgeschlagene Richtlinie, **Simulate** aus.
4. Geben Sie im Feld **Objekt** das S3 ein `bucket/object-key` Oder den Swift `container/object-name` Für ein Testobjekt. Beispiel: `bucket-01/filename.png`.
5. Geben Sie optional eine Versions-ID für das Objekt in das Feld **Versions-ID** ein.
6. Wählen Sie **Simulieren**.
7. Bestätigen Sie im Abschnitt Simulationsergebnisse, dass jedes Objekt mit der richtigen Regel abgeglichen wurde.

Beispiel 1: Überprüfung der Regeln bei der Simulation einer vorgeschlagenen ILM-Richtlinie

In diesem Beispiel wird beschrieben, wie Regeln bei der Simulation einer vorgeschlagenen Richtlinie überprüft werden.

In diesem Beispiel wird die **Beispiel ILM-Richtlinie** für die aufgenommene Objekte in zwei Buckets simuliert. Die Richtlinie umfasst drei Regeln:

- Die erste Regel, **zwei Kopien, zwei Jahre für Eimer-A**, gilt nur für Objekte in Eimer-a.
- Die zweite Regel, **EC-Objekte > 1 MB**, gilt für alle Buckets, aber für Filter auf Objekten größer als 1 MB.
- Die dritte Regel, **zwei Kopien, zwei Rechenzentren**, ist die Standardregel. Er enthält keine Filter und verwendet keine nicht aktuelle Referenzzeit.

Bestätigen Sie nach der Simulation der Richtlinie, dass jedes Objekt mit der richtigen Regel abgeglichen wurde.

Simulation results

Use this table to confirm the results of applying this policy to the selected objects.

Clear all ?

Object	Version ID	Rule matched	Previous match	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	X
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	X
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	X

In diesem Beispiel:

- `bucket-a/bucket-a object.pdf` Die erste Regel, die nach Objekten in filtert, wurde richtig zugeordnet `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` Ist in `bucket-b`, So dass es nicht mit der ersten Regel. Stattdessen wurde sie durch die zweite Regel korrekt abgeglichen, die nach Objekten mit einer Größe von mehr als 1 MB filtert.
- `bucket-b/test object less than 1 MB.pdf` Stimmt nicht mit den Filtern in den ersten beiden Regeln überein, so wird sie durch die Standardregel platziert, die keine Filter enthält.

Beispiel 2: Neuordnung von Regeln bei der Simulation einer vorgeschlagenen ILM-Richtlinie

Dieses Beispiel zeigt, wie Sie Regeln neu anordnen können, um die Ergebnisse bei der Simulation einer Richtlinie zu ändern.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie, die zum Auffinden von Objekten mit Metadaten für Benutzer der Serie=`x-men` bestimmt ist, enthält drei Regeln:

- Die erste Regel, **PNGs**, filtert nach Schlüsselnamen, die enden `.png`.
- Die zweite Regel, **X-Men**, gilt nur für Objekte für Mieter A und Filter für `series=x-men` Benutzer-Metadaten:
- Die letzte Regel, **two copies two Data Centers**, ist die Standardregel, die allen Objekten entspricht, die nicht den ersten beiden Regeln entsprechen.

Schritte

1. Nachdem Sie die Regeln hinzugefügt und die Richtlinie gespeichert haben, wählen Sie **Simulieren**.
2. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und wählen Sie **Simulate** aus.

Die Simulationsergebnisse werden angezeigt und zeigen an, dass der `Havok.png` Das Objekt wurde durch die **PNGs**-Regel abgeglichen.

Simulation results
Use this table to confirm the results of applying this policy to the selected objects.

Clear all ?

Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

Jedoch `Havok.png` Sollte die **X-Men**-Regel testen.

3. Um das Problem zu lösen, ordnen Sie die Regeln neu an.
 - a. Wählen Sie **Finish**, um das Fenster ILM-Richtlinie simulieren zu schließen.
 - b. Wählen Sie **actions > Edit**, um die Richtlinie zu bearbeiten.
 - c. Ziehen Sie die **X-Men**-Regel an den Anfang der Liste.
 - d. Wählen Sie **Speichern**.
4. Wählen Sie **Simulieren**.

Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie neu bewertet und die neuen Simulationsergebnisse angezeigt. In dem Beispiel zeigt die Spalte „Regelabgleich“, dass der `Havok.png` Das Objekt entspricht jetzt wie erwartet der X-Men-Metadatenregel. In der Spalte Vorheriger Abgleich wird angezeigt, dass die PNGs-Regel mit dem Objekt in der vorherigen Simulation übereinstimmt.

Simulation results
Use this table to confirm the results of applying this policy to the selected objects.

Clear all ?

Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	X



Wenn Sie auf der Registerkarte vorgeschlagene Richtlinie bleiben, können Sie eine Richtlinie neu simulieren, nachdem Sie Änderungen vorgenommen haben, ohne die Namen der Testobjekte erneut eingeben zu müssen.

Beispiel 3: Korrigieren Sie eine Regel bei der Simulation einer vorgeschlagenen ILM-Richtlinie

Dieses Beispiel zeigt, wie eine Richtlinie simuliert, eine Regel in der Richtlinie korrigiert und die Simulation fortgesetzt wird.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie dient zum Suchen von Objekten, die über solche verfügen `series=x-men` Benutzer-Metadaten: Bei der Simulation dieser Richtlinie gegen die `traten` jedoch unerwartete Ergebnisse auf `Beast.jpg` Objekt: Anstatt die X-Men-Metadatenregel zu entsprechen, kopiert das Objekt die Standardregel. Zwei Rechenzentren werden kopiert.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
<input type="button" value="Clear all"/> 				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	

Wenn ein Testobjekt nicht mit der erwarteten Regel in der Richtlinie übereinstimmt, müssen Sie jede Regel in der Richtlinie überprüfen und eventuelle Fehler korrigieren.

Schritte

1. Wählen Sie **Fertig**, um das Dialogfeld Richtlinie simulieren zu schließen. Wählen Sie auf der Registerkarte vorgeschlagene Richtlinie **Aufbewahrungsdiagramm** aus. Wählen Sie dann **Alle erweitern** oder **Details anzeigen** für jede Regel nach Bedarf aus.
2. Prüfen Sie das Mandantenkonto der Regel, die Referenzzeit und die Filterkriterien.

Angenommen, die Metadaten für die X-men-Regel wurden als „x-men01“ anstelle von „x-men“ eingegeben.“

3. Um den Fehler zu beheben, korrigieren Sie die Regel wie folgt:
 - Wenn die Regel Teil der vorgeschlagenen Richtlinie ist, können Sie entweder die Regel klonen oder die Regel aus der Richtlinie entfernen und sie dann bearbeiten.
 - Wenn die Regel Teil der aktiven Richtlinie ist, müssen Sie die Regel klonen. Sie können keine Regel aus der aktiven Richtlinie bearbeiten oder entfernen.

Option	Schritte
Die Regel klonen	<ol style="list-style-type: none"> i. Wählen Sie ILM > Regeln. ii. Wählen Sie die falsche Regel aus, und wählen Sie Clone. iii. Geben Sie einen Namen für die neue Regel ein, ändern Sie dann die falschen Informationen und wählen Sie Create. iv. Wählen Sie ILM > Richtlinien > vorgeschlagene Richtlinie aus. v. Wählen Sie Actions > Edit. vi. Wählen Sie Regeln auswählen, und wählen Sie dann Weiter, um dieselbe Standardregel zu akzeptieren. vii. Aktivieren Sie im Schritt andere Regeln auswählen das Kontrollkästchen für die neue Regel, deaktivieren Sie das Kontrollkästchen für die ursprüngliche Regel und wählen Sie Auswählen. viii. Ordnen Sie die Regeln bei Bedarf neu an, indem Sie die neue Regel an die richtige Stelle ziehen. ix. Wählen Sie Speichern.

Option	Schritte
Bearbeiten Sie die Regel	<ol style="list-style-type: none"> i. Wählen Sie ILM > Richtlinien > vorgeschlagene Richtlinie und entfernen Sie die Regel, die Sie bearbeiten möchten. ii. Wählen Sie ILM > Regeln. iii. Wählen Sie die Regel aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten. Oder aktivieren Sie das Kontrollkästchen für die Regel und wählen Sie Aktionen > Bearbeiten. iv. Ändern Sie die falschen Informationen für jeden Teil des Assistenten, und wählen Sie dann Update. v. Wählen Sie ILM > Richtlinien > vorgeschlagene Richtlinie aus. vi. Wählen Sie Actions > Edit. vii. Wählen Sie Regeln auswählen, und wählen Sie dann Weiter, um dieselbe Standardregel zu akzeptieren. viii. Aktivieren Sie im Dialogfeld andere Regeln auswählen das Kontrollkästchen für die korrigierte Regel, wählen Sie Auswählen und dann Speichern. ix. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

4. Führen Sie die Simulation erneut aus.

In diesem Beispiel entspricht die korrigierte X-Men-Regel nun dem `Beast.jpg` Objekt auf Grundlage des `series=x-men` Benutzer-Metadaten, wie erwartet.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
<input type="button" value="Clear all"/>				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	

Aktivieren Sie die ILM-Richtlinie

Wenn Sie einer vorgeschlagenen ILM-Richtlinie ILM-Regeln hinzufügen, die Richtlinie simulieren und bestätigen, dass es sich wie erwartet verhält, sind Sie bereit, die vorgeschlagene Richtlinie zu aktivieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".
- Sie haben die vorgeschlagene ILM-Richtlinie gespeichert und simuliert.



Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen. Prüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert. + Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID sie für die Verwaltung aller Objekte, einschließlich vorhandener und neu aufgenommenen Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Über diese Aufgabe

Wenn Sie eine ILM-Richtlinie aktivieren, verteilt das System die neue Richtlinie auf alle Nodes. Die neue aktive Richtlinie tritt jedoch möglicherweise erst in Kraft, wenn alle Grid-Nodes zur Verfügung stehen, um die neue Richtlinie zu erhalten. In einigen Fällen wartet das System auf die Implementierung einer neuen aktiven Richtlinie, um sicherzustellen, dass Grid-Objekte nicht versehentlich entfernt werden.

- Nehmen Richtlinienänderungen vor, die die Datenredundanz oder Aufbewahrungszeit verbessern, werden diese Änderungen sofort implementiert. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Regel mit drei Kopien anstelle einer Regel mit zwei Kopien enthält, wird diese Richtlinie sofort implementiert, da sie die Datenredundanz erhöht.
- Bei Richtlinienänderungen, die Datenredundanz oder -Langlebigkeit verringern könnten, werden diese Änderungen erst implementiert, wenn alle Grid-Nodes verfügbar sind. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Regel mit zwei Kopien anstelle einer Regel mit drei Kopien verwendet, wird die neue Richtlinie auf der Registerkarte „Aktive Richtlinie“ angezeigt. Sie wird jedoch erst wirksam, wenn alle Nodes online und verfügbar sind.

Schritte

1. Wenn Sie bereit sind, eine vorgeschlagene Richtlinie zu aktivieren, wählen Sie **ILM-Richtlinien > vorgeschlagene Richtlinie** aus, und wählen Sie dann **Aktivieren** aus.

Es wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, zu bestätigen, dass Sie die vorgeschlagene Richtlinie aktivieren möchten.

In der Warnmeldung wird eine Eingabeaufforderung angezeigt, wenn die Standardregel Objekte nicht für immer behält. In diesem Beispiel zeigt das Aufbewahrungsdigramm, dass die Standardregel Objekte nach 730 Tagen (2 Jahre) löscht. Sie müssen **730** in das Textfeld eingeben, um zu bestätigen, dass alle Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen, nach 730 Tagen aus StorageGRID entfernt werden.

⚠️ Activate the proposed policy ✕

Errors in an ILM policy can cause irreparable data loss. Review and test the policy carefully before activating.

⚠️ The following rules do not store objects forever. When the last time period ends, objects will be automatically purged.

- Rule 1 (730 days)

The default rule in the policy does not retain objects forever. Confirm this is the behavior you want by referring to the retention diagram for the default rule:

Reference time: **Ingest time** Ingest behavior: **Balanced**

The diagram shows a horizontal timeline from Day 0 to Day 730. Two blue bars represent '2 replicated copies - Data Center 2' and '2 replicated copies - Data Center 1'. A grey box on the left is labeled 'Day 0 - 730'. Below the timeline, 'Duration' is indicated as '730 days'.

Now, complete the following prompt:

Any objects that are not matched by another rule in this policy will be deleted after days.

Are you sure you want to activate the proposed policy?

Cancel
OK

2. Wählen Sie **OK**.

Ergebnis

Wenn eine neue ILM-Richtlinie aktiviert wurde:

- Die Richtlinie wird auf der Registerkarte Aktive Richtlinie angezeigt. Der Eintrag Startdatum zeigt das Datum und die Uhrzeit an, zu der die Richtlinie aktiviert wurde.
- Die zuvor aktive Richtlinie wird auf der Registerkarte Richtlinienverlauf angezeigt. Die Einträge für das Start- und Enddatum geben an, wann die Richtlinie aktiv wurde und wann sie nicht mehr in Kraft war.

Verwandte Informationen

["Beispiel 6: Ändern einer ILM-Richtlinie"](#)

Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup

Sobald Sie eine ILM-Richtlinie aktiviert haben, sollten Sie repräsentative Testobjekte in das StorageGRID System aufnehmen. Anschließend sollten Sie eine Objektmetadaten abfragen durchführen, um zu bestätigen, ob Kopien wie vorgesehen erstellt und an den richtigen Orten platziert werden.

Bevor Sie beginnen

- Sie haben eine Objektkennung, die einer der folgenden sein kann:
 - **UUID**: Der Universally Unique Identifier des Objekts. Geben Sie die UUID in allen Großbuchstaben ein.
 - **CBID**: Die eindeutige Kennung des Objekts in StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in allen Großbuchstaben ein.

- **S3-Bucket und Objektschlüssel:** Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren. Wenn der S3-Bucket versioniert ist und Sie eine bestimmte Version eines S3-Objekts mithilfe des Bucket und Objektschlüssels nachsehen möchten, steht Ihnen die **Version-ID** zur Verfügung.
- **Swift Container und Objektname:** Wenn ein Objekt über die Swift-Schnittstelle aufgenommen wird, verwendet die Client-Anwendung eine Container- und Objektname-Kombination, um das Objekt zu speichern und zu identifizieren.

Schritte

1. Aufnahme des Objekts.
2. Wählen Sie **ILM > Object Metadata Lookup**.
3. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein. Sie können eine UUID, CBID, S3 Bucket/Objektschlüssel oder Swift Container/Objektname eingeben.
4. Optional können Sie eine Version-ID für das Objekt eingeben (nur S3).

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier: source/testobject

Version ID (optional): MEJGMkMyQzgtNEY5OC0xMUU3LTkzMEYtRDkyNTAwQkY5N0Mx

Look Up

5. Wählen Sie **Look Up**.

Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

- Systemmetadaten, einschließlich Objekt-ID (UUID), Objektname, Name des Containers, Mandantenkontenname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36056",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

6. Vergewissern Sie sich, dass das Objekt am richtigen Ort und an den richtigen Stellen gespeichert ist und dass es sich um den richtigen Kopiertyp handelt.



Wenn die Option „Audit“ aktiviert ist, können Sie auch das Audit-Protokoll für die Meldung „ORLM-Objektregeln erfüllt“ überwachen. Die ORLM-Audit-Meldung kann Ihnen weitere Informationen über den Status des ILM-Evaluierungsprozesses liefern, kann Ihnen jedoch keine Informationen über die Richtigkeit der Platzierung der Objektdaten oder die Vollständigkeit der ILM-Richtlinie geben. Das müssen Sie selbst beurteilen. Weitere Informationen finden Sie unter ["Prüfung von Audit-Protokollen"](#).

Verwandte Informationen

- ["S3-REST-API VERWENDEN"](#)
- ["Nutzen Sie die Swift REST API"](#)

Arbeiten mit ILM-Richtlinien und ILM-Regeln

Wenn sich Ihre Speicheranforderungen ändern, müssen Sie möglicherweise eine andere Richtlinie implementieren oder die mit dieser Richtlinie verbundenen ILM-Regeln ändern. Sie können ILM-Metriken anzeigen, um die Systemperformance zu ermitteln.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

ILM-Richtlinien anzeigen

So zeigen Sie aktive, vorgeschlagene und historische ILM-Richtlinien an:

1. Wählen Sie **ILM > Richtlinien**.
2. Wählen Sie je nach Bedarf **Aktive Richtlinie**, **vorgeschlagene Richtlinie** oder **Richtlinienverlauf** aus, um die Details zu den einzelnen Richtlinien anzuzeigen. Auf jeder Registerkarte können Sie **Policy rules** und **Retention diagram** auswählen.

The screenshot displays the 'Active policy' tab in the ILM configuration interface. At the top, there are three tabs: 'Active policy' (selected), 'Proposed policy', and 'Policy history'. A notification banner indicates: 'You have a proposed policy. Review details on the Proposed policy tab.' Below this, the policy details are shown: 'Policy name: Policy 1', 'Reason for change: test', and 'Start date: 2022-09-28 15:04:48 MDT'. A 'Simulate' button is present. Underneath, there are two sub-tabs: 'Policy rules' (selected) and 'Retention diagram'. The 'Policy rules' section contains a table with the following data:

Rule order	Rule name	Filters
1	Project A	Ingest time is 2022-10-01 00:00:00 MDT
Default	Project B	—

Klonen einer historischen ILM-Richtlinie

So klonen Sie eine historische ILM-Richtlinie:

1. Wählen Sie **ILM > Richtlinien > Richtlinienverlauf** aus.
2. Entfernen Sie die vorgeschlagene Richtlinie, falls vorhanden.
3. Aktivieren Sie das Optionsfeld für die Richtlinie, die Sie klonen möchten, und wählen Sie dann **historische Richtlinie klonen** aus.
4. Füllen Sie die erforderlichen Angaben aus, indem Sie den Anweisungen unter folgen "[Vorgeschlagene ILM-Richtlinie erstellen](#)".



Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Entfernen Sie die vorgeschlagene ILM-Richtlinie

So entfernen Sie die vorgeschlagene Richtlinie:

1. Wählen Sie **ILM > Richtlinien > vorgeschlagene Richtlinie** aus.
2. Wählen Sie **Aktionen > Entfernen**.

Die vorgeschlagene Richtlinie und die vorgeschlagene Policy-Registerkarte werden entfernt.

Zeigen Sie Einzelheiten zur ILM-Regel an

So zeigen Sie die Details für eine ILM-Regel an, einschließlich des Aufbewahrungsdiagramms und der Anweisungen zur Platzierung der Regel:

1. Wählen Sie **ILM > Regeln**.
2. Wählen Sie die Regel aus, deren Details Sie anzeigen möchten. Beispiel:

2 copies 2 data centers

Compliant:	Yes	Ingest behavior:	Strict
Used in active policy:	No	Reference time:	Ingest time
Used in proposed policy:	No		
Description:	test		

[Clone](#) [Edit](#) [Remove](#)

Time period and placements

Retention diagram [Placement instructions](#)

Sort placements by **Time period** [Storage pool](#) ● Replicated copy ● Erasure-coded (EC) copy

Reference time: **Ingest time** Ingest behavior: **Strict**

Day 0 Day 365

Day 0 - forever

Day 0 - 365

Duration 365 days Forever

Darüber hinaus können Sie auf der Detailseite eine Regel klonen, bearbeiten oder entfernen.

Klonen einer ILM-Regel

Sie können eine Regel nicht bearbeiten, wenn sie in der vorgeschlagenen ILM-Richtlinie oder der aktiven ILM-Richtlinie verwendet wird. Stattdessen können Sie eine Regel klonen und alle erforderlichen Änderungen an der geklonten Kopie vornehmen. Anschließend können Sie die ursprüngliche Regel bei Bedarf aus der

vorgeschlagenen Richtlinie entfernen und durch die geänderte Version ersetzen. Sie können eine ILM-Regel nicht klonen, wenn sie mit StorageGRID Version 10.2 oder früher erstellt wurde.

Bevor Sie einer aktiven ILM-Richtlinie eine geklonte Regel hinzufügen, sollten Sie beachten, dass eine Änderung der Anweisungen zur Platzierung eines Objekts zu einer erhöhten Systemauslastung führen kann.

Schritte

1. Wählen Sie **ILM > Regeln**.
2. Aktivieren Sie das Kontrollkästchen für die Regel, die Sie klonen möchten, und wählen Sie dann **Clone** aus. Alternativ wählen Sie den Regelnamen aus, und wählen Sie dann auf der Seite mit den Regeldetails **Clone** aus.
3. Aktualisieren Sie die geklonte Regel, indem Sie die Schritte für befolgen [Bearbeiten einer ILM-Regel](#) Und ["Verwenden erweiterter Filter in ILM-Regeln"](#).

Beim Klonen einer ILM-Regel müssen Sie einen neuen Namen eingeben.

Bearbeiten einer ILM-Regel

Möglicherweise müssen Sie eine ILM-Regel bearbeiten, um einen Filter oder eine Platzierungsanweisung zu ändern.

Sie können eine Regel nicht bearbeiten, wenn sie in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird. Stattdessen können Sie diese Regeln klonen und erforderliche Änderungen an der geklonten Kopie vornehmen. Sie können auch die vom System bereitgestellte Regel nicht bearbeiten, erstellen Sie 2 Kopien.



Bevor Sie einer aktiven ILM-Richtlinie eine bearbeitete Regel hinzufügen, müssen Sie beachten, dass eine Änderung der Anweisungen zur Platzierung eines Objekts zu einer erhöhten Systemauslastung führen kann.

Schritte

1. Wählen Sie **ILM > Regeln**.
2. Bestätigen Sie, dass die zu bearbeitende Regel nicht in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.
3. Wenn die Regel, die Sie bearbeiten möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen für die Regel und wählen Sie **Aktionen > Bearbeiten**. Alternativ wählen Sie den Namen der Regel aus, und wählen Sie dann auf der Seite mit den Regeldetails **Bearbeiten** aus.
4. Füllen Sie die Seiten des Assistenten zum Bearbeiten von ILM-Regeln aus. Befolgen Sie bei Bedarf die Schritte für ["Erstellen einer ILM-Regel"](#) Und ["Verwenden erweiterter Filter in ILM-Regeln"](#).

Beim Bearbeiten einer ILM-Regel können Sie ihren Namen nicht ändern.



Wenn Sie eine Regel bearbeiten, die in einer historischen Richtlinie verwendet wird, wird die Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.

Entfernen einer ILM-Regel

Um die Liste der aktuellen ILM-Regeln kontrollierbar zu halten, entfernen Sie alle ILM-Regeln, die Sie wahrscheinlich nicht verwenden werden.

Schritte

So entfernen Sie eine ILM-Regel, die derzeit in der aktiven Richtlinie oder in der vorgeschlagenen Richtlinie verwendet wird:

1. Klonen Sie die aktive Richtlinie, oder bearbeiten Sie die vorgeschlagene Richtlinie.
2. Entfernen Sie die ILM-Regel aus der Richtlinie.
3. Speichern, simulieren und aktivieren Sie die neue Richtlinie, um sicherzustellen, dass Objekte wie erwartet geschützt sind.

So entfernen Sie eine derzeit nicht verwendete ILM-Regel:

1. Wählen Sie **ILM > Regeln**.
2. Bestätigen Sie, dass die Regel, die Sie entfernen möchten, nicht in der aktiven Richtlinie oder der vorgeschlagenen Richtlinie verwendet wird.
3. Wenn die Regel, die Sie entfernen möchten, nicht verwendet wird, wählen Sie die Regel aus und wählen Sie **Entfernen**. Sie können mehrere Regeln auswählen und alle gleichzeitig entfernen.
4. Wählen Sie **Yes**, um zu bestätigen, dass Sie die ILM-Regel entfernen möchten.

Die ILM-Regel wird entfernt.



Wenn Sie eine Regel entfernen, die in einer historischen Richtlinie verwendet wird, wird die Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.

Anzeigen von ILM-Metriken

Sie können Metriken für ILM anzeigen, z. B. die Anzahl der Objekte in der Warteschlange und die Evaluierungsrate. Sie können diese Kennzahlen überwachen, um die Systemperformance zu ermitteln. Eine große Warteschlange oder Evaluierungsrate zeigt möglicherweise an, dass das System nicht mit der Aufnahmezeit Schritt halten kann, die Auslastung der Client-Applikationen zu hoch ist oder dass ein ungewöhnlicher Zustand vorliegt.

Schritte

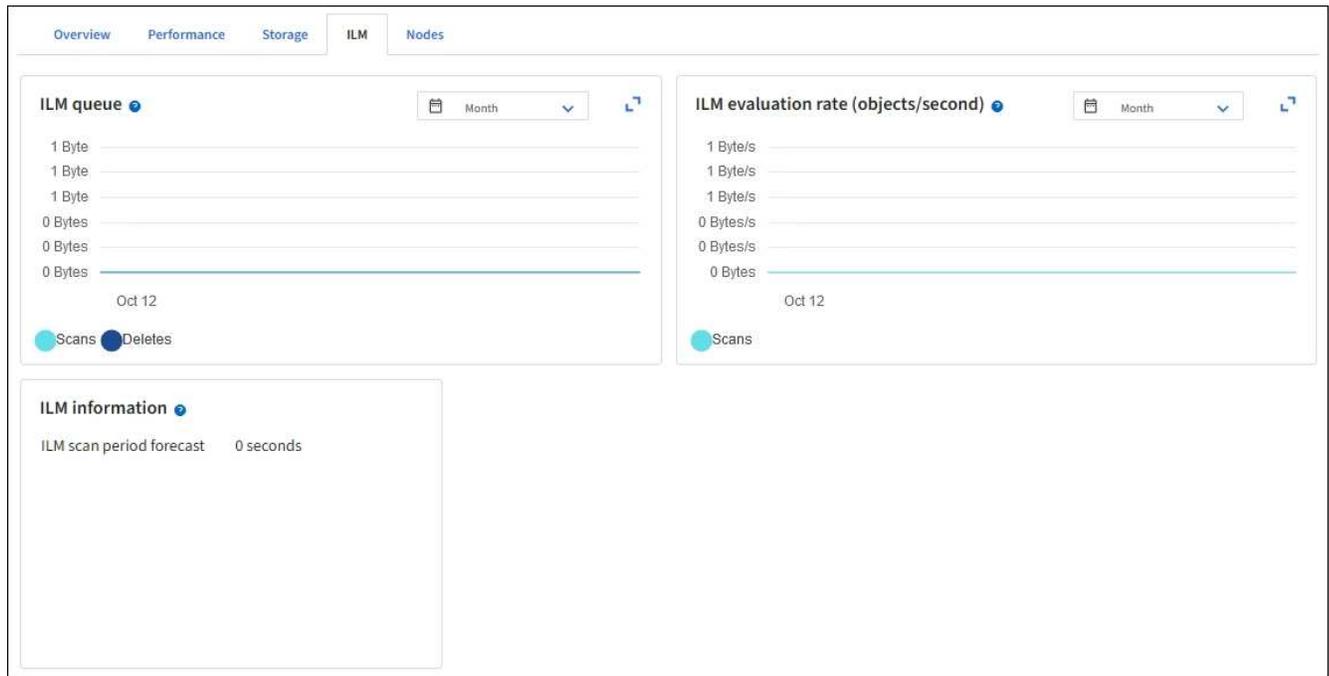
1. Wählen Sie **Dashboard > ILM**.



Da das Dashboard angepasst werden kann, ist die Registerkarte ILM möglicherweise nicht verfügbar.

2. Überwachen Sie die Kennzahlen auf der Registerkarte ILM.

Sie können das Fragezeichen auswählen Um eine Beschreibung der Elemente auf der Registerkarte ILM anzuzeigen.



Verwenden Sie die S3-Objektsperre

Objekte managen mit S3 Object Lock

Als Grid-Administrator können Sie S3 Object Lock für Ihr StorageGRID System aktivieren und eine konforme ILM-Richtlinie implementieren. So können Sie sicherstellen, dass Objekte in bestimmten S3 Buckets nicht für einen bestimmten Zeitraum gelöscht oder überschrieben werden.

Was ist S3 Object Lock?

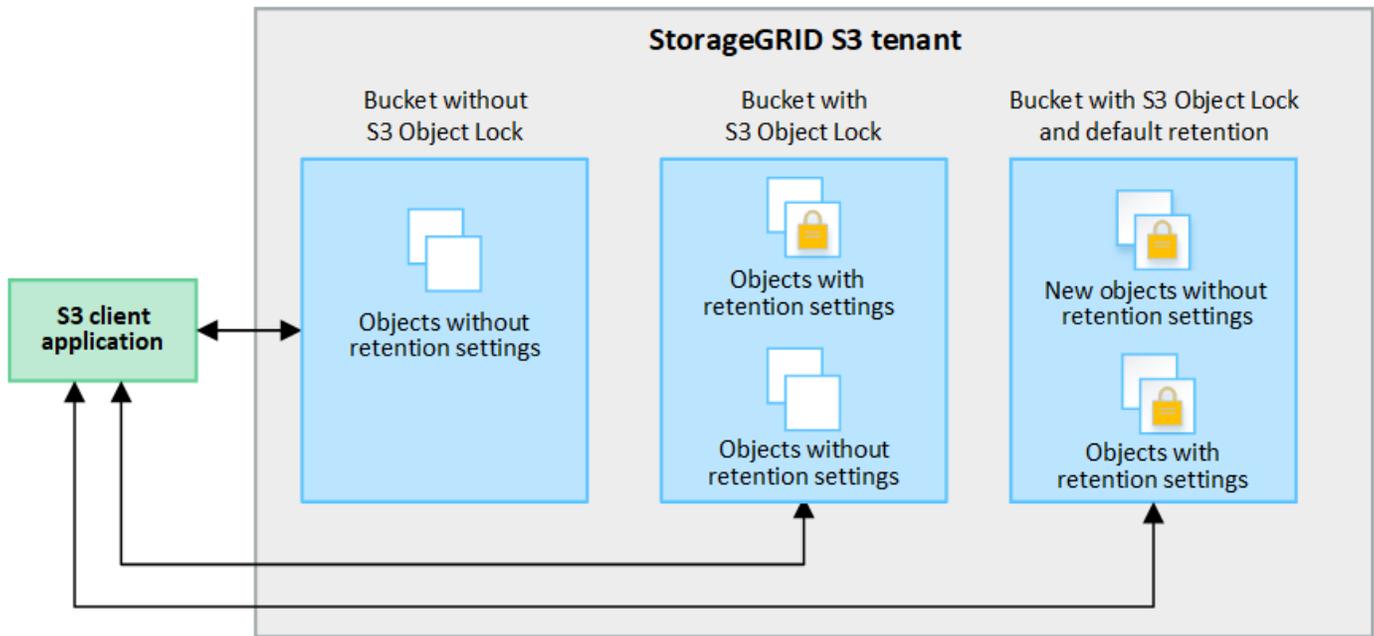
Die Funktion StorageGRID S3 Object Lock ist eine Objektschutzlösung, die der S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

Wenn die globale S3-Objektsperre für ein StorageGRID-System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn für einen Bucket die S3 Object Lock aktiviert ist, ist die Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Wenn für einen Bucket die S3 Object Lock aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion angeben, die in diesem Bucket gespeichert ist.

Darüber hinaus kann für einen Bucket, auf dem die S3 Object Lock aktiviert ist, optional ein Standardaufbewahrungsmodus und ein Aufbewahrungszeitraum verwendet werden. Die Standardeinstellungen gelten nur für Objekte, die ohne eigene Aufbewahrungseinstellungen zum Bucket hinzugefügt werden.

StorageGRID with S3 Object Lock setting enabled



Aufbewahrungsmodi

Die Objektsperrefunktion StorageGRID S3 unterstützt zwei Aufbewahrungsmodi, um verschiedene Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Amazon S3 Aufbewahrungsmodi.

- Im Compliance-Modus:
 - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
 - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
 - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
 - Benutzer mit besonderer Berechtigung können in Anfragen einen Überbrückungskopf verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
 - Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
 - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mithilfe der S3-Client-Applikation optional die folgenden Aufbewahrungseinstellungen für jedes Objekt angeben, das dem Bucket hinzugefügt wird:

- **Retention Mode:** Entweder Compliance oder Governance.
- **Rebeat-until-date:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Legal Hold:** Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflicht hat kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.



Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Weitere Informationen zu den Objekteinstellungen finden Sie unter ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

Standardeinstellung für die Aufbewahrung von Buckets

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wurde, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Default Retention Mode:** Entweder Compliance oder Governance.
- **Default Retention Period:** Wie lange neue Objektversionen, die zu diesem Bucket hinzugefügt wurden, beibehalten werden sollen, beginnend mit dem Tag, an dem sie hinzugefügt werden.

Die Standard-Bucket-Einstellungen gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Vorhandene Bucket-Objekte werden nicht beeinflusst, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

Siehe ["Erstellen eines S3-Buckets"](#) Und ["Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung"](#).

Vergleich der S3-Objektsperre mit älterer Compliance

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Da die S3-Objektsperrefunktion den Amazon S3-Anforderungen entspricht, depreziert sie die proprietäre StorageGRID-Compliance-Funktion, die jetzt als „` Legacy-Compliance“ bezeichnet wird.



Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung S3 Objektsperre automatisch aktiviert. Sie können die Einstellungen vorhandener konformer Buckets weiterhin mit StorageGRID managen. Es ist jedoch nicht möglich, neue konforme Buckets zu erstellen. Weitere Informationen finden Sie unter ["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#).

Wenn Sie die ältere Compliance-Funktion in einer früheren Version von StorageGRID verwendet haben, lesen Sie die folgende Tabelle, um zu erfahren, wie sie mit der S3-Objektsperrefunktion in StorageGRID verglichen wird.

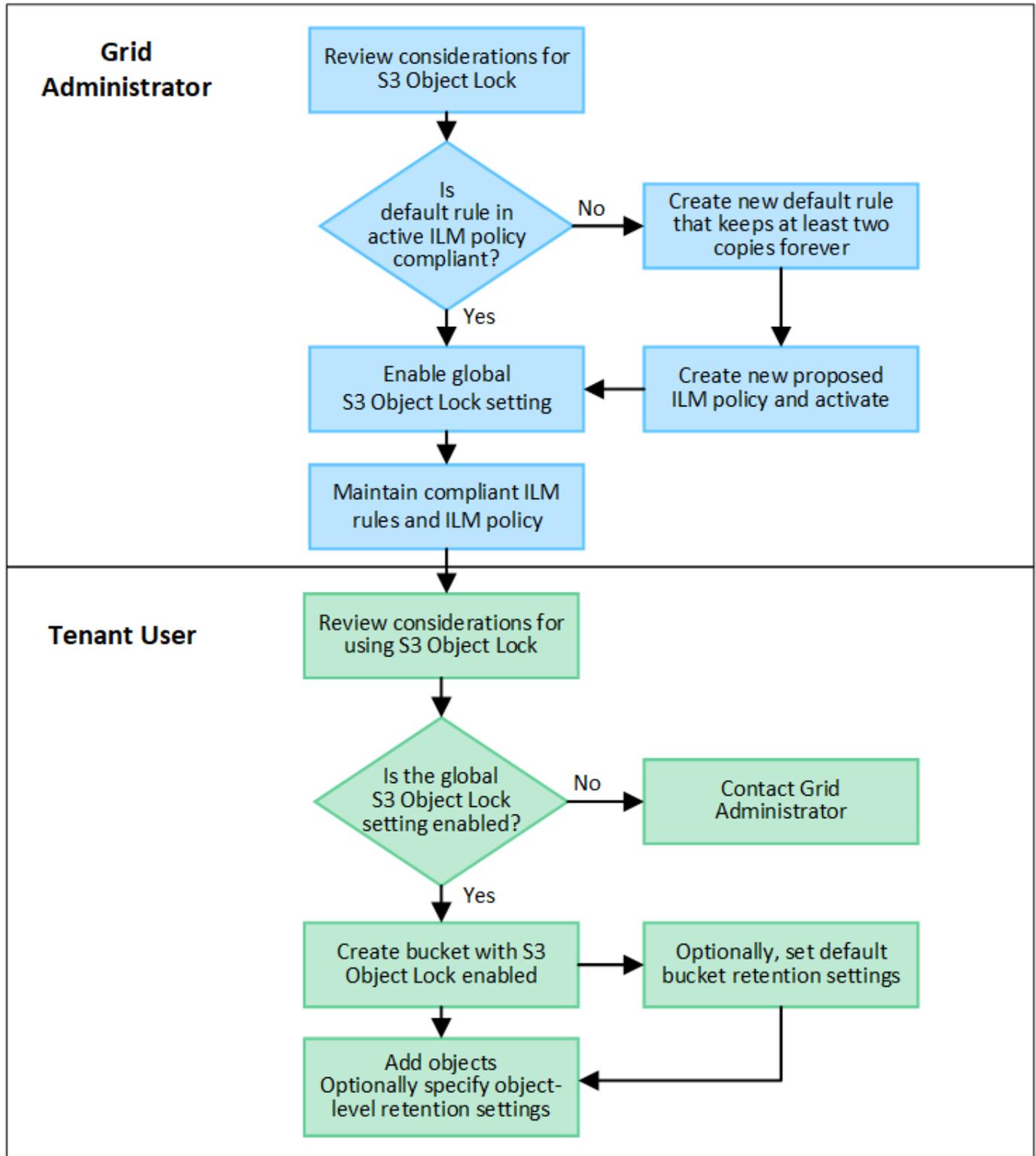
	S3-Objektsperre	Compliance (alt)
Wie wird die Funktion global aktiviert?	Wählen Sie im Grid Manager die Option KONFIGURATION > System > S3 Object Lock .	Wird nicht mehr unterstützt.
Wie wird die Funktion für einen Bucket aktiviert?	Benutzer müssen die S3-Objektsperre aktivieren, wenn ein neuer Bucket mithilfe des Mandantenmanagers, der Mandantenmanagement-API oder der S3-REST-API erstellt wird.	Wird nicht mehr unterstützt.

	S3-Objektsperre	Compliance (alt)
Wird die Bucket-Versionierung unterstützt?	Ja. Die Bucket-Versionierung ist erforderlich und wird automatisch aktiviert, wenn S3 Object Lock für den Bucket aktiviert ist.	Nein
Wie wird die Objektaufbewahrung festgelegt?	Benutzer können für jede Objektversion ein bis-Datum für die Aufbewahrung festlegen oder für jeden Bucket einen Standardaufbewahrungszeitraum festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Der Aufbewahrungszeitraum gilt für alle Objekte im Bucket.
Kann der Aufbewahrungszeitraum geändert werden?	<ul style="list-style-type: none"> • Im Compliance-Modus kann das Aufbewahrungsdatum für eine Objektversion erhöht, aber nicht verringert werden. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen die Aufbewahrungseinstellungen eines Objekts verringern oder sogar entfernen. 	Die Aufbewahrungsfrist eines Buckets kann erhöht, aber nie verringert werden.
Wo wird die gesetzliche Aufbewahrungspflichten kontrolliert?	Benutzer können für jede Objektversion im Bucket rechtliche Aufbewahrungspflichten platzieren oder eine gesetzliche Aufbewahrungspflichten aufheben.	Auf dem Bucket werden gesetzliche Aufbewahrungspflichten angebracht, die alle Objekte im Bucket betreffen.
Wann können Objekte gelöscht werden?	<ul style="list-style-type: none"> • Im Compliance-Modus kann eine Objektversion nach Erreichen des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt befindet sich nicht im Legal Hold. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen ein Objekt löschen, bevor das Aufbewahrungsdatum erreicht wird, vorausgesetzt, das Objekt befindet sich nicht unter Legal Hold. 	Ein Objekt kann nach Ablauf des Aufbewahrungszeitraums gelöscht werden, sofern der Bucket nicht unter der gesetzlichen Aufbewahrungspflichten liegt. Objekte können automatisch oder manuell gelöscht werden.
Wird die Bucket-Lifecycle-Konfiguration unterstützt?	Ja.	Nein

Workflow für S3 Objektsperre

Als Grid-Administrator müssen Sie sich eng mit den Mandantenbenutzern abstimmen, um sicherzustellen, dass die Objekte so geschützt sind, dass sie ihren Aufbewahrungsanforderungen entsprechen.

Das Workflow-Diagramm zeigt die grundlegenden Schritte zur Verwendung der S3-Objektsperre. Die Schritte werden vom Grid-Administrator und von Mandantenbenutzern durchgeführt.



Den Grid-Administratoren stehen

Wie das Workflow-Diagramm zeigt, muss ein Grid-Administrator zwei übergeordnete Aufgaben durchführen, bevor S3-Mandanten S3-Objektsperre verwenden können:

1. Erstellen Sie mindestens eine kompatible ILM-Regel und stellen Sie diese Regel in der aktiven ILM-Richtlinie zur Standardregel bereit.
2. Aktivieren Sie die globale S3-Objektsperre für das gesamte StorageGRID-System.

Aufgaben für Mandanten

Nach Aktivierung der globalen S3-Objektsperre können Mandanten die folgenden Aufgaben ausführen:

1. Erstellen Sie Buckets, für die S3-Objektsperre aktiviert ist.
2. Optional können Sie Standardaufbewahrungseinstellungen für den Bucket festlegen. Alle Standard-Bucket-Einstellungen werden nur auf neue Objekte angewendet, die keine eigenen Aufbewahrungseinstellungen haben.
3. Fügen Sie diesen Buckets Objekte hinzu und geben Sie optional Aufbewahrungszeiträume auf Objektebene und Einstellungen für Legal Hold an.
4. Aktualisieren Sie nach Bedarf die Standardaufbewahrung für den Bucket oder aktualisieren Sie die Aufbewahrungsfrist oder die Legal Hold-Einstellung für ein einzelnes Objekt.

Anforderungen für die S3-Objektsperre

Sie müssen die Anforderungen für die Aktivierung der globalen S3-Objektsperre, die Anforderungen für die Erstellung konformer ILM-Regeln und ILM-Richtlinien sowie die Einschränkungen prüfen, die StorageGRID für Buckets und Objekte, die S3 Objektsperre verwenden, festlegen.

Anforderungen für die Verwendung der globalen S3-Objektsperre

- Sie müssen die globale S3-Objektsperreneinstellung mithilfe des Grid-Managers oder der Grid-Management-API aktivieren, bevor ein S3-Mandant einen Bucket erstellen kann, dessen S3-Objektsperre aktiviert ist.
- Wenn Sie die globale S3-Objektsperre aktivieren, können alle S3-Mandantenkonten Buckets erstellen, wobei S3-Objektsperre aktiviert ist.
- Nachdem Sie die globale S3-Objektsperre aktiviert haben, können Sie die Einstellung nicht deaktivieren.
- Die globale S3 Object Lock kann nur aktiviert werden, wenn die Standardregel in der aktiven ILM-Richtlinie „compliant“ lautet. (Das heißt, die Standardregel muss die Anforderungen von Buckets mit aktivierter S3 Object Lock erfüllen.)
- Wenn die globale S3-Objektsperre aktiviert ist, können Sie keine neue vorgeschlagene ILM-Richtlinie erstellen oder eine vorhandene vorgeschlagene ILM-Richtlinie aktivieren, sofern die Standardregel in der Richtlinie nicht konform ist. Nach Aktivierung der globalen S3 Object Lock-Einstellung geben die ILM-Regeln und ILM-Richtlinien-Seiten an, welche ILM-Regeln konform sind.

Anforderungen für konforme ILM-Regeln

Wenn Sie die globale S3-Objektsperre aktivieren möchten, müssen Sie sicherstellen, dass die Standardregel in Ihrer aktiven ILM-Richtlinie konform ist. Eine konforme Regel erfüllt die Anforderungen beider Buckets durch aktivierte S3-Objektsperre und alle vorhandenen Buckets, für die Compliance aktiviert ist:

- Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
- Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Platzierung vorhanden sein.
- Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
- Objektkopien können nicht auf Archivknoten gespeichert werden.
- Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei **Ingest time** als Referenzzeit verwendet wird.
- Mindestens eine Zeile der Platzierungsanweisungen muss „Forever“ sein.

Anforderungen für aktive und vorgeschlagene ILM-Richtlinien

Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können aktive und vorgeschlagene ILM-Richtlinien sowohl konforme als auch nicht konforme Regeln umfassen.

- Die Standardregel in der aktiven oder einer vorgeschlagenen ILM-Richtlinie muss konform sein.
- Nicht konforme Regeln gelten nur für Objekte in Buckets, für die die S3-Objektsperre nicht aktiviert ist oder die die ältere Compliance-Funktion nicht aktiviert hat.
- Konforme Regeln können auf Objekte in jedem Bucket angewendet werden; S3-Objektsperre oder vorhandene Compliance muss für den Bucket nicht aktiviert werden.

Eine ILM-konforme Richtlinie kann folgende drei Regeln umfassen:

1. Eine konforme Regel, die Erasure-codierte Kopien der Objekte in einem bestimmten Bucket erstellt und bei aktivierter S3-Objektsperre aktiviert ist. Die EC-Kopien werden von Tag 0 bis für immer auf Storage-Nodes gespeichert.
2. Eine nicht konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes für ein Jahr erstellt und dann eine Objektkopie zu Archivierungs-Nodes verschiebt und die Kopie für immer speichert. Diese Regel gilt nur für Buckets, für die keine S3 Object Lock oder Legacy Compliance aktiviert ist, da nur eine Objektkopie dauerhaft gespeichert und Archive Nodes verwendet werden.
3. Eine konforme Standardregel, die zwei replizierte Objektkopien auf Storage-Nodes von Tag 0 bis für immer erstellt. Diese Regel gilt für alle Objekte in jedem Bucket, die nicht durch die ersten beiden Regeln herausgefiltert wurden.

Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktivierter S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.
- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket. Sie können S3 Object Lock nicht deaktivieren oder die Versionierung für den Bucket nicht unterbrechen.
- Optional können Sie mithilfe von Tenant Manager, der Mandanten-Management-API oder der S3-REST-API für jeden Bucket einen Standardaufbewahrungsmodus und einen Aufbewahrungszeitraum angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt wurden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen außer Kraft setzen, indem Sie einen Aufbewahrungsmodus und das

Aufbewahrungsdatum für jede Objektversion festlegen, wenn sie hochgeladen wird.

- Die Konfiguration des Bucket-Lebenszyklus wird für Buckets unterstützt, für die S3 Object Lock aktiviert ist.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

Anforderungen für Objekte in Buckets, bei denen die S3-Objektsperre aktiviert ist

- Zum Schutz einer Objektversion können Sie Standardaufbewahrungseinstellungen für den Bucket angeben oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mit der S3-Client-Applikation oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

Jedes in einem Bucket gespeicherte Objekt mit aktivierter S3 Object Lock durchlaufen die folgenden Phasen:

1. Objektaufnahme

Wenn einem Bucket eine Objektversion hinzugefügt wird, für die S3 Object Lock aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

- Wenn für das Objekt Aufbewahrungseinstellungen angegeben werden, werden die Einstellungen auf Objektebene angewendet. Alle standardmäßigen Bucket-Einstellungen werden ignoriert.
- Wenn für das Objekt keine Aufbewahrungseinstellungen angegeben sind, werden die Standard-Bucket-Einstellungen angewendet, sofern diese vorhanden sind.
- Wenn für das Objekt oder den Bucket keine Aufbewahrungseinstellungen angegeben wurden, ist das Objekt nicht durch S3 Object Lock geschützt.

Wenn Aufbewahrungseinstellungen angewendet werden, sind sowohl das Objekt als auch alle benutzerdefinierten S3-Metadaten geschützt.

2. Objektaufbewahrung und -Löschung

Von jedem geschützten Objekt werden innerhalb StorageGRID des angegebenen Aufbewahrungszeitraums mehrere Kopien gespeichert. Die genaue Anzahl und Art der Objektkopien sowie der Speicherort werden durch die konformen Regeln der aktiven ILM-Richtlinie bestimmt. Ob ein geschütztes Objekt gelöscht werden kann, bevor das Aufbewahrungsdatum erreicht ist, hängt vom Aufbewahrungsmodus ab.

- Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Verwandte Informationen

- ["Erstellen eines S3-Buckets"](#)
- ["Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung"](#)
- ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)
- ["Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"](#)

Aktivieren Sie die S3-Objektsperre global

Falls ein S3-Mandantenkonto Vorschriften beim Speichern von Objektdaten einhalten muss, muss die S3-Objektsperre für Ihr gesamtes StorageGRID System aktiviert werden. Wenn Sie die globale S3-Objektsperre aktivieren, können alle S3-Mandantenbenutzer Buckets und Objekte mit S3 Object Lock erstellen und verwalten.

Bevor Sie beginnen

- Sie haben die Root-Zugriffsberechtigung.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben den S3-Objektsperreworkflow überprüft und die Überlegungen verstanden.
- Sie haben bestätigt, dass die Standardregel in der aktiven ILM-Richtlinie konform ist. Siehe "[Erstellen einer Standard-ILM-Regel](#)" Entsprechende Details.

Über diese Aufgabe

Ein Grid-Administrator muss die globale S3-Objektsperre aktivieren, damit Mandantenbenutzer neue Buckets erstellen können, für die S3-Objektsperre aktiviert ist. Nachdem diese Einstellung aktiviert ist, kann sie nicht deaktiviert werden.



Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung S3 Objektsperre automatisch aktiviert. Sie können die Einstellungen vorhandener konformer Buckets weiterhin mit StorageGRID managen. Es ist jedoch nicht möglich, neue konforme Buckets zu erstellen. Weitere Informationen finden Sie unter "[NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5](#)".

Schritte

1. Wählen Sie **KONFIGURATION > System > S3 Objektsperre**.

Die Seite Einstellungen für die S3-Objektsperre wird angezeigt.

2. Wählen Sie **S3-Objektsperre aktivieren**.
3. Wählen Sie **Anwenden**.

Ein Bestätigungsdialogfeld wird angezeigt, in dem Sie daran erinnert werden, dass Sie die S3-Objektsperre nicht deaktivieren können, nachdem sie aktiviert wurde.

4. Wenn Sie sicher sind, dass Sie die S3-Objektsperre für Ihr gesamtes System dauerhaft aktivieren möchten, wählen Sie **OK**.

Wenn Sie **OK** wählen:

- Wenn die Standardregel in der aktiven ILM-Richtlinie konform ist, ist S3 Object Lock jetzt für das gesamte Grid aktiviert und kann nicht deaktiviert werden.
- Wenn die Standardregel nicht kompatibel ist, wird ein Fehler angezeigt. Sie müssen eine neue ILM-Richtlinie erstellen und aktivieren, die eine konforme Regel als Standardregel enthält. Wählen Sie **OK**. Erstellen Sie dann eine neue vorgeschlagene Richtlinie, simulieren Sie sie und aktivieren Sie sie. Siehe "[ILM-Richtlinie erstellen](#)" Weitere Anweisungen.

Nachdem Sie fertig sind

Nachdem Sie die globale S3-Objektsperre aktiviert haben, möchten Sie dies möglicherweise tun ["Neue ILM-Richtlinie erstellen"](#). Nach Aktivierung der Einstellung kann die ILM-Richtlinie optional sowohl eine konforme Standardregel als auch eine nicht konforme Standardregel enthalten. Beispielsweise könnte eine nicht konforme Regel verwendet werden, die keine Filter für Objekte in Buckets enthält, für die die S3-Objektsperre nicht aktiviert ist.

Beheben Sie die Konsistenzfehler beim Aktualisieren der S3-Objektsperre oder der alten Compliance-Konfiguration

Wenn ein Datacenter-Standort oder mehrere Storage-Nodes an einem Standort nicht mehr verfügbar sind, müssen Benutzer von S3-Mandanten unter Umständen Änderungen an der S3-Objektsperre oder älterer Compliance-Konfiguration vornehmen.

Mandantenbenutzer, deren Buckets mit aktivierter S3 Object Lock (oder älterer Compliance) vorhanden sind, können bestimmte Einstellungen ändern. Beispielsweise muss ein Mandantenbenutzer, der S3 Object Lock verwendet, eine Objektversion unter die gesetzliche Aufbewahrungspflichten legen.

Wenn ein Mandantenbenutzer die Einstellungen für einen S3-Bucket oder eine Objektversion aktualisiert, versucht StorageGRID, die Bucket- oder Objektmetadaten sofort im Grid zu aktualisieren. Wenn das System die Metadaten nicht aktualisieren kann, weil ein Datacenter-Standort oder mehrere Storage-Nodes nicht verfügbar sind, wird ein Fehler zurückgegeben:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Gehen Sie wie folgt vor, um diesen Fehler zu beheben:

1. Versuchen Sie, alle Storage-Nodes oder -Sites so schnell wie möglich wieder verfügbar zu machen.
2. Wenn Sie nicht in der Lage sind, an jedem Standort ausreichend Storage-Nodes zur Verfügung zu stellen, wenden Sie sich an den technischen Support, der Sie beim Wiederherstellen von Nodes unterstützt und sicherstellt, dass Änderungen konsistent im gesamten Grid angewendet werden.
3. Sobald das zugrunde liegende Problem behoben ist, erinnern Sie den Mandantenbenutzer daran, ihre Konfigurationsänderungen erneut zu versuchen.

Verwandte Informationen

- ["Verwenden Sie ein Mandantenkonto"](#)
- ["S3-REST-API VERWENDEN"](#)
- ["Recovery und Wartung"](#)

Beispiele für ILM-Regeln und -Richtlinien

Beispiel 1: ILM-Regeln und -Richtlinie für Objekt-Storage

Die folgenden Beispielregeln und -Richtlinien dienen als Ausgangspunkt bei der Definition einer ILM-Richtlinie zur Erfüllung der Anforderungen an Objektschutz und -Aufbewahrung.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1, z. B. 1: Objektdaten an zwei Standorte kopieren

Dieses Beispiel einer ILM-Regel kopiert Objektdaten in Storage-Pools an zwei Standorten.

Regeldefinition	Beispielwert
Speicherpools an einem Standort	Zwei Speicherpools, die jeweils unterschiedliche Standorte mit den Namen Standort 1 und Standort 2 enthalten.
Regelname	Zwei Kopien Zwei Standorte
Referenzzeit	Aufnahmezeit
Platzierungen	Bewahren Sie an Tag 0 bis für immer eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2 auf.

Im Abschnitt Regelanalyse des Aufbewahrungsdigramms steht Folgendes:

- Für die Dauer dieser Regel gilt eine StorageGRID-Sicherung gegen vor-Ort-Verlust.
- Von dieser Regel verarbeitete Objekte werden nicht durch ILM gelöscht.

ILM-Regel 2, z. B. 1: Profil für Erasure Coding mit Bucket-Matching

Diese Beispielregel verwendet ein Erasure Coding-Profil und einen S3-Bucket, um zu bestimmen, wo und wie lange das Objekt gespeichert ist.

Regeldefinition	Beispielwert
Speicherpool mit mehreren Standorten	<ul style="list-style-type: none">• Ein Speicherpool an drei Standorten (Standorte 1, 2, 3)• Verwenden Sie das Erasure Coding-Schema für 6+3
Regelname	S3 Bucket-Finanzdaten
Referenzzeit	Aufnahmezeit
Platzierungen	Erstellen Sie für Objekte in dem S3-Bucket mit dem Namen „Finance-Records“ eine Kopie, die nach Erasure Coding in dem Pool codiert wurde, der vom Profil für Erasure Coding angegeben wurde. Bewahren Sie diese Kopie für immer auf.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 store forever

Store objects by erasure coding using 6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.



ILM-Richtlinie z. B. 1

In der Praxis sind die meisten ILM-Richtlinien einfach, obwohl das StorageGRID System Ihnen die Entwicklung ausgefeilter und komplexer ILM-Richtlinien ermöglicht.

Eine typische ILM-Richtlinie für ein Grid mit mehreren Standorten kann beispielsweise folgende ILM-Regeln umfassen:

- Speichern Sie bei der Aufnahme alle Objekte, die zum S3-Bucket mit dem Namen `finance-records` gehören in einem Speicherpool, der drei Standorte enthält. Verwenden Sie 6+3 Erasure Coding.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, verwenden Sie die standardmäßige ILM-Regel der Richtlinie, zwei Kopien von zwei Rechenzentren, um eine Kopie dieses Objekts an Standort 1 und eine Kopie an Standort 2 zu speichern.

Proposed policy name

Reason for change

Manage rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	S3 Bucket finance-records ?	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Verwandte Informationen

- ["Erstellen Sie eine ILM-Richtlinie: Überblick"](#)
- ["Erstellen einer vorgeschlagenen ILM-Richtlinie"](#)

Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung

Die folgenden Beispielregeln und -Richtlinien dienen als Ausgangspunkt für die Definition einer ILM-Richtlinie, die nach Objektgröße gefiltert wird, um empfohlene EC-Anforderungen zu erfüllen.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 2: Verwenden Sie EC für Objekte über 1 MB

In diesem Beispiel werden Objekte mit einer ILM-Regel gelöscht, die größer als 1 MB sind.



Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

Regeldefinition	Beispielwert
Regelname	Nur EC-Objekte > 1 MB
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Platzierungen	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ↕ MB ▼ ✕

ILM-Regel 2 beispielsweise 2: Zwei replizierte Kopien

Diese Beispiel-ILM-Regel erstellt zwei replizierte Kopien und filtert nicht nach Objektgröße. Diese Regel ist die Standardregel für die Richtlinie. Da die erste Regel alle Objekte mit einer Größe von mehr als 1 MB filtert, gilt diese Regel nur für Objekte, die 1 MB oder kleiner sind.

Regeldefinition	Beispielwert
Regelname	Zwei Replizierte Kopien
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Keine
Platzierungen	Bewahren Sie an Tag 0 bis für immer eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2 auf.

ILM-Richtlinie beispielsweise 2: Verwenden Sie EC für Objekte über 1 MB

Dieses Beispiel für die ILM-Richtlinie umfasst zwei ILM-Regeln:

- Die erste Löschrregel kodiert alle Objekte, die größer als 1 MB sind.
- Die zweite (Standard-) ILM-Regel erstellt zwei replizierte Kopien. Da Objekte größer als 1 MB nach Regel 1 herausgefiltert wurden, gilt Regel 2 nur für Objekte, die 1 MB oder kleiner sind.

Beispiel 3: ILM-Regeln und -Richtlinie für besseren Schutz von Image-Dateien

Mithilfe der folgenden Beispielregeln und -Richtlinie können Sie sicherstellen, dass Bilder mit mehr als 1 MB gelöscht werden und dass zwei Kopien aus kleineren Images erstellt werden.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 3: Verwenden Sie EC für Bilddateien über 1 MB

Diese Beispiel ILM-Regel verwendet erweiterte Filterung zur Löschung von Code aller Bilddateien größer als 1 MB.



Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

Regeldefinition	Beispielwert
Regelname	EC-Bilddateien > 1 MB
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Erweiterte Filter für Schlüssel	<ul style="list-style-type: none">• Endet mit .jpg• Endet mit .png
Platzierungen	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

The screenshot shows the configuration for 'Filter group 1' and 'Filter group 2'. Both groups are defined by the text: 'Objects with all of following metadata will be evaluated by this rule:'.
Filter group 1 conditions:
- Object size: greater than 1 MB
- and Key: ends with .jpg
Filter group 2 conditions:
- Object size: greater than 1 MB
- and Key: ends with .png

Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Anweisung für die Platzierung von Löschkodes nur für Dateien mit einer Größe von mehr als 1 MB.

ILM-Regel 2 beispielsweise 3: Erstellen Sie 2 replizierte Kopien für alle verbleibenden Image-Dateien

Diese Beispiel-ILM-Regel verwendet erweiterte Filterung, um anzugeben, dass kleinere Bilddateien repliziert werden. Da die erste Regel in der Richtlinie bereits Bilddateien mit einer Größe von mehr als 1 MB übereinstimmt, gilt diese Regel für Bilddateien mit einer Größe von 1 MB.

Regeldefinition	Beispielwert
Regelname	2 Kopien für Bilddateien
Referenzzeit	Aufnahmezeit
Erweiterte Filter für Schlüssel	<ul style="list-style-type: none"> • Endet mit .jpg • Endet mit .png
Platzierungen	Erstellung von 2 replizierten Kopien in zwei Storage Pools

ILM-Richtlinie beispielsweise 3: Besserer Schutz für Image-Dateien

Dieses Beispiel enthält drei Regeln für die ILM-Richtlinie:

- Die erste Löschrregel kodiert alle Bilddateien größer als 1 MB.
- Die zweite Regel erstellt zwei Kopien aller verbleibenden Bilddateien (d. h. Bilder, die 1 MB oder kleiner sind).
- Die Standardregel gilt für alle übrigen Objekte (d. h. alle nicht-Image-Dateien).

Rule order	Rule name	Filters
1	 EC image files > 1 MB	Object size is greater than 1 MB
2	 2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3

Wenn Sie über einen S3-Bucket mit aktivierter Versionierung verfügen, können Sie die aktuellen Objektversionen verwalten, indem Sie Regeln in Ihre ILM-Richtlinie verwenden, die „noncurrent time“ als Referenzzeit verwenden.



Wenn Sie eine begrenzte Aufbewahrungszeit für Objekte angeben, werden diese Objekte nach Erreichen des Zeitraums dauerhaft gelöscht. Stellen Sie sicher, dass Sie verstehen, wie lange die Objekte beibehalten werden.

Wie in diesem Beispiel dargestellt, können Sie den von versionierten Objekten verwendeten Storage mithilfe unterschiedlicher Anweisungen zur Platzierung von nicht aktuellen Objektversionen steuern.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.



Um eine ILM-Richtliniensimulation für eine nicht aktuelle Version eines Objekts durchzuführen, müssen Sie die UUID oder CBID der Objektversion kennen. Um die UUID und die CBID zu finden, verwenden Sie ["Objekt-Metadaten-Suche"](#) Solange das Objekt noch aktuell ist.

Verwandte Informationen

- ["So werden Objekte gelöscht"](#)

ILM-Regel 1 beispielsweise 4: Speichern Sie drei Kopien für 10 Jahre

Diese ILM-Regel speichert eine Kopie jedes Objekts über einen Zeitraum von 10 Jahren an drei Standorten.

Diese Regel gilt für alle Objekte, unabhängig davon, ob sie versioniert sind.

Regeldefinition	Beispielwert
Storage-Pools	Drei Speicherpools, die jeweils aus verschiedenen Rechenzentren mit den Namen Standort 1, Standort 2 und Standort 3 bestehen.
Regelname	Drei Kopien Zehn Jahre
Referenzzeit	Aufnahmezeit
Platzierungen	An Tag 0 sollten Sie drei replizierte Kopien 10 Jahre (3,652 Tage), eine an Standort 1, eine an Standort 2 und eine an Standort 3 aufbewahren. Löschen Sie Ende 10 Jahre alle Kopien des Objekts.

ILM-Regel 2 beispielsweise 4: Speichern Sie zwei Kopien nicht aktueller Versionen für zwei Jahre

In diesem Beispiel wird eine ILM-Regel zwei Kopien der nicht aktuellen Versionen eines versionierten S3 Objekts für zwei Jahre gespeichert.

Da ILM-Regel 1 für alle Versionen des Objekts gilt, müssen Sie eine weitere Regel erstellen, um nicht aktuelle Versionen herauszufiltern.

Um eine Regel zu erstellen, die „noncurrent time“ als Referenzzeit verwendet, wählen Sie **Yes** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ aus. Gehen Sie in Schritt 1 (Details eingeben) des Assistenten zum Erstellen einer ILM-Regel vor. Wenn Sie **Yes** auswählen, wird *noncurrent time* automatisch für die Referenzzeit ausgewählt, und Sie können keine andere Referenzzeit auswählen.

1 Enter details — 2 Define placements — 3 Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ? Select tenant accounts

Bucket name ? matches all v

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

No Yes

In diesem Beispiel werden nur zwei Kopien der nicht aktuellen Versionen gespeichert und diese Kopien für zwei Jahre gespeichert.

Regeldefinition	Beispielwert
Storage-Pools	Zwei Speicherpools, jeweils in verschiedenen Rechenzentren, Standort 1 und Standort 2.
Regelname	Nicht Aktuelle Versionen: Zwei Kopien Zwei Jahre
Referenzzeit	Nicht aktuelle Zeit Wird automatisch ausgewählt, wenn Sie für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ auswählen. Im Assistenten zum Erstellen einer ILM-Regel.
Platzierungen	An Tag 0 relativ zur nicht aktuellen Zeit (d. h. ab dem Tag, an dem die Objektversion zur nicht aktuellen Version wird), behalten Sie zwei replizierte Kopien der nicht aktuellen Objektversionen für 2 Jahre (730 Tage), eine in Standort 1 und eine in Standort 2. Löschen Sie Ende 2 Jahre die nicht aktuellen Versionen.

ILM-Richtlinie z. B. 4: S3-versionierte Objekte

Wenn Sie ältere Versionen eines Objekts anders als die aktuelle Version verwalten möchten, müssen Regeln, die „aktuelle Zeit“ als Referenzzeit verwenden, in der ILM-Richtlinie vor Regeln erscheinen, die auf die aktuelle Objektversion angewendet werden.

Eine ILM-Richtlinie für S3-versionierte Objekte kann ILM-Regeln wie die folgenden umfassen:

- Bewahren Sie alle älteren (nicht aktuellen) Versionen jedes Objekts für 2 Jahre auf, beginnend mit dem Tag, an dem die Version nicht mehr aktuell wurde.



Die Regeln „nicht aktuelle Zeit“ müssen in der Richtlinie vor den Regeln erscheinen, die für die aktuelle Objektversion gelten. Andernfalls werden die nicht aktuellen Objektversionen niemals mit der Regel „nicht aktuelle Zeit“ abgeglichen.

- Bei der Einspeisung können Sie drei replizierte Kopien erstellen und eine Kopie an jedem der drei Standorte speichern. Bewahren Sie 10 Jahre lang Kopien der aktuellen Objektversion auf.

Wenn Sie die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Alle nicht aktuellen Objektversionen würden mit der ersten Regel abgeglichen. Wenn eine nicht aktuelle Objektversion älter als zwei Jahre ist, wird diese durch ILM dauerhaft gelöscht (alle Kopien der nicht aktuellen Version, die aus dem Grid entfernt wurde).



Um nicht aktuelle Objektversionen zu simulieren, müssen Sie die UUID oder CBID dieser Version verwenden. Solange das Objekt noch aktuell ist, können Sie verwenden "[Objekt-Metadaten-Suche](#)" Um seine UUID und CBID zu finden.

- Die aktuelle Objektversion würde mit der zweiten Regel abgeglichen. Wenn die aktuelle Objektversion über einen Zeitraum von 10 Jahren gespeichert wurde, fügt der ILM-Prozess eine Löschmarkierung als aktuelle Version des Objekts hinzu und macht die vorherige Objektversion „noncurrent“. Bei der nächsten ILM-Evaluierung stimmt diese nicht aktuelle Version mit der ersten Regel überein. Dadurch wird die Kopie an Standort 3 gelöscht und die beiden Kopien an Standort 1 und Standort 2 werden für weitere 2 Jahre gespeichert.

Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten

Ein Speicherortfilter und das strikte Aufnahmeverhalten in einer Regel verhindern, dass Objekte an einem bestimmten Datacenter-Standort gespeichert werden.

In diesem Beispiel will ein Mieter mit Sitz in Paris aufgrund von regulatorischen Bedenken einige Objekte nicht außerhalb der EU speichern. Andere Objekte, einschließlich aller Objekte aus anderen Mandantenkonten, können entweder im Rechenzentrum von Paris oder im Rechenzentrum der USA gespeichert werden.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Verwandte Informationen

- "[Aufnahmeoptionen](#)"
- "[Erstellen Sie eine ILM-Regel: Wählen Sie Ingest Behavior aus](#)"

ILM-Regel 1 beispielsweise 5: Strenge Einspeisung für das Pariser Rechenzentrum

In diesem Beispiel verwendet die ILM-Regel das strikte Ingest-Verhalten, um zu gewährleisten, dass Objekte, die von einem in Paris ansässigen Mieter in S3-Buckets gespeichert werden, wobei die Region auf eu-West-3 Region (Paris) eingestellt ist, nie im US-Rechenzentrum gespeichert werden.

Diese Regel gilt für Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 (Paris) eingestellt ist.

Regeldefinition	Beispielwert
Mandantenkonto	Mieter von Paris
Erweiterter Filter	Die Positionsbeschränkung entspricht eu-West-3
Storage-Pools	Standort 1 (Paris)
Regelname	Strenge Einspeisung für ein Pariser Rechenzentrum
Referenzzeit	Aufnahmezeit
Platzierungen	An Tag 0 bewahren Sie zwei replizierte Kopien für immer in Standort 1 (Paris) auf.
Aufnahmeverhalten	Streng. Verwenden Sie bei der Einspeisung immer die Platzierungen dieser Regel. Die Aufnahme schlägt fehl, wenn es nicht möglich ist, zwei Kopien des Objekts im Pariser Rechenzentrum zu speichern.

ILM-Regel 2 beispielsweise 5: Ausgewogene Aufnahme für andere Objekte

Diese Beispiel-ILM-Regel verwendet das ausgewogene Ingest-Verhalten, um optimale ILM-Effizienz für Objekte zu erzielen, die nicht der ersten Regel zugeordnet sind. Zwei Kopien aller Objekte, die dieser Regel entsprechen, werden gespeichert - eins im US-Rechenzentrum und eins im Pariser Rechenzentrum. Wenn die Regel nicht sofort erfüllt werden kann, werden Zwischenkopien an jedem verfügbaren Ort gespeichert.

Diese Regel gilt für Objekte, die einem beliebigen Mieter und einer beliebigen Region angehören.

Regeldefinition	Beispielwert
Mandantenkonto	Ignorieren
Erweiterter Filter	<i>Nicht angegeben</i>
Storage-Pools	Standort 1 (Paris) und Standort 2 (USA)
Regelname	2 Kopien 2 Datacenter
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Am Tag 0 werden zwei replizierte Kopien für immer in zwei Datacentern aufbewahrt
Aufnahmeverhalten	Ausgeglichen. Objekte, die dieser Regel entsprechen, werden nach Möglichkeit gemäß den Anweisungen zur Platzierung der Regel platziert. Andernfalls werden an jedem beliebigen Ort vorläufige Kopien angefertigt.

ILM-Richtlinie z. B. 5: Kombination von Aufnahmeverhalten

Die ILM-Beispielrichtlinie enthält zwei Regeln mit unterschiedlichen Aufnahmeverhalten.

Eine ILM-Richtlinie, die zwei unterschiedliche Aufnahmeverhalten nutzt, kann ILM-Regeln wie die folgenden umfassen:

- Speichern Sie Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 (Paris) gesetzt ist, nur im Datacenter in Paris. Aufnahme fehlgeschlagen, wenn das Pariser Rechenzentrum nicht verfügbar ist.
- Speichern Sie alle anderen Objekte (einschließlich solcher, die zum Pariser Mieter gehören, jedoch über eine andere Bucket-Region verfügen) sowohl im US-Rechenzentrum als auch im Pariser Rechenzentrum. Erstellen Sie Zwischenkopien an einem beliebigen verfügbaren Speicherort, wenn die Platzierungsanweisung nicht erfüllt werden kann.

Wenn Sie die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Alle Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 gesetzt haben, werden mit der ersten Regel abgeglichen und im Pariser Rechenzentrum gespeichert. Da die erste Regel strenge Einspeisung verwendet, werden diese Objekte nie im US-Rechenzentrum gespeichert. Wenn die Storage-Nodes im Pariser Datacenter nicht verfügbar sind, schlägt die Aufnahme fehl.
- Alle anderen Objekte werden mit der zweiten Regel abgeglichen, einschließlich Objekte, die zum Pariser Mieter gehören und für die die S3-Bucket-Region nicht auf eu-West-3 gesetzt ist. In jedem Datacenter wird eine Kopie jedes Objekts gespeichert. Da die zweite Regel jedoch eine ausgewogene Aufnahme verwendet und ein Datacenter nicht zur Verfügung steht, werden zwei Übergangskopien an jedem verfügbaren Standort gespeichert.

Beispiel 6: Ändern einer ILM-Richtlinie

Wenn Ihr Datenschutz geändert werden muss oder Sie neue Standorte hinzufügen, können Sie eine neue ILM-Richtlinie erstellen und aktivieren.

Vor dem Ändern einer Richtlinie muss verstanden werden, wie Änderungen an ILM-Platzierungen die Gesamt-Performance eines StorageGRID Systems vorübergehend beeinträchtigen können.

In diesem Beispiel wurde eine neue StorageGRID-Site mit einer Erweiterung hinzugefügt, und für die Speicherung von Daten am neuen Standort muss eine neue aktive ILM-Richtlinie implementiert werden. Um eine neue aktive Richtlinie zu implementieren, erstellen Sie zunächst eine vorgeschlagene Richtlinie von einer der beiden "[Klonen einer vorhandenen Richtlinie](#) *oder* [von Grund auf neu](#)". Danach müssen Sie "[Simulieren](#)" Und dann "[Aktivieren](#)" Die neue Politik.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Wie sich eine Änderung einer ILM-Richtlinie auf die Performance auswirkt

Wenn Sie eine neue ILM-Richtlinie aktivieren, wird die Performance Ihres StorageGRID Systems möglicherweise vorübergehend beeinträchtigt, insbesondere dann, wenn aufgrund der Platzierungsanweisungen in der neuen Richtlinie viele vorhandene Objekte an einen neuen Standort verschoben werden müssen.

Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Damit eine neue ILM-Richtlinie die Platzierung vorhandener replizierter und Erasure-Coded-Objekte nicht beeinträchtigt, können Sie folgende Möglichkeiten nutzen ["Erstellen Sie eine ILM-Regel mit einem Filter für die Aufnahmezeit"](#). Zum Beispiel ist **Ingest time am oder nach <date and time>**, so dass die neue Regel nur für Objekte gilt, die am oder nach dem angegebenen Datum und der angegebenen Uhrzeit aufgenommen wurden.

Folgende Arten von ILM-Richtlinienänderungen, die vorübergehend Auswirkungen auf die StorageGRID Performance haben:

- Anwenden eines anderen Erasure Coding-Profiles auf vorhandene Objekte, die zur Fehlerkorrektur codiert wurden



StorageGRID betrachtet jedes Erasure Coding-Profil als einzigartig und wiederverwendet bei der Verwendung eines neuen Profils keine Fragmente des Erasure Coding.

- Ändern des für vorhandene Objekte erforderlichen Kopientyps; z. B. Konvertieren eines großen Anteils replizierter Objekte in Objekte mit Erasure-Coding-Verfahren.
- Kopien vorhandener Objekte werden an einen völlig anderen Speicherort verschoben, z. B. um eine große Anzahl von Objekten in einen oder aus einem Cloud-Storage-Pool oder an einen Remote-Standort zu verschieben.

Aktive ILM-Richtlinie z. B. 6: Datensicherung an zwei Standorten

In diesem Beispiel wurde die aktive ILM-Richtlinie ursprünglich für ein StorageGRID System mit zwei Standorten konzipiert und verwendet zwei ILM-Regeln.

Active policy
Policy history

Policy name: Data Protection for Two Sites (2 rules)
Reason for change: Data protection for two sites (using 2 rules)
Start date: 2022-10-11 10:37:11 MDT

[Simulate](#)

Policy rules
Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

In dieser ILM-Richtlinie werden Objekte, die von Mandanten A gehören, durch Erasure Coding von 2+1 an einem Standort geschützt, während Objekte, die zu allen anderen Mandanten gehören, durch die Replizierung mit zwei Kopien über zwei Standorte hinweg geschützt sind.



Die erste Regel in diesem Beispiel verwendet einen erweiterten Filter, um sicherzustellen, dass das Erasure Coding nicht für kleine Objekte verwendet wird. Alle Objekte von Mandant A, die kleiner als 1 MB sind, werden durch die Standardregel geschützt, die Replikation verwendet.

Regel 1: Erasure Coding für einen Standort für Mandant A

Regeldefinition	Beispielwert
Regelname	Erasure Coding für einen Standort für Mandant A
Mandantenkonto	Mandant A
Storage-Pool	Standort 1
Platzierungen	2+1 Erasure Coding in Standort 1 vom Tag 0 bis ewig

Regel 2: Replizierung zwischen zwei Standorten für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Replizierung an zwei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Standort 1 und Standort 2

Regeldefinition	Beispielwert
Platzierungen	Zwei replizierte Kopien von Tag 0 auf ewig: Eine Kopie an Standort 1 und eine Kopie an Standort 2.

Vorgeschlagene ILM-Richtlinie z. B. 6: Datensicherung an drei Standorten

In diesem Beispiel wird die ILM-Richtlinie durch eine neue Richtlinie für ein StorageGRID System mit drei Standorten ersetzt.

Nach einer Erweiterung zum Hinzufügen des neuen Standorts erstellte der Grid-Administrator zwei neue Speicherpools: Einen Speicherpool für Standort 3 und einen Speicherpool mit allen drei Standorten (nicht mit dem Standardspeicherpool Alle Storage-Nodes). Anschließend erstellte der Administrator zwei neue ILM-Regeln und eine neue vorgeschlagene ILM-Richtlinie, die auf den Schutz von Daten an allen drei Standorten ausgelegt ist.

Bei Aktivierung dieser neuen ILM-Richtlinie werden Objekte, die von Mandant A gehören, an drei Standorten durch 2+1 Erasure Coding geschützt, während Objekte, die zu anderen Mandanten gehören (und kleinere Objekte von Mandanten A), durch Replizierung mit 3 Kopien über drei Standorte hinweg gesichert werden.

Regel 1: Erasure Coding für drei Standorte für Mandant A

Regeldefinition	Beispielwert
Regelname	Three-Site Erasure Coding für Mandant A
Mandantenkonto	Mandant A
Storage-Pool	Alle 3 Standorte (einschließlich Standort 1, Standort 2 und Standort 3)
Platzierungen	2+1 Erasure Coding in allen 3 Standorten vom Tag 0 bis für immer

Regel 2: Replizierung an drei Standorten für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Replikation von drei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Standort 1, Standort 2 und Standort 3
Platzierungen	Drei replizierte Kopien von Tag 0 bis ewig: Eine Kopie an Standort 1, eine Kopie an Standort 2 und eine Kopie an Standort 3.

Aktivierung der vorgeschlagenen ILM-Richtlinie beispielsweise 6

Wenn Sie eine neue vorgeschlagene ILM-Richtlinie aktivieren, können vorhandene Objekte an neue Orte verschoben oder neue Objektkopien für vorhandene Objekte erstellt werden, basierend auf den Anweisungen

zur Platzierung in neuen oder aktualisierten Regeln.



Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen. Prüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert.



Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Was passiert, wenn sich die Anweisungen zur Einhaltung von Datenkonsistenz ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel sind Objekte, die zu Mandant A gehören, durch den Erasure Coding 2+1 an Standort 1 geschützt. In der neuen vorgeschlagenen ILM-Richtlinie werden Objekte von Mandant A durch Erasure Coding 2+1 an Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert ist, werden die folgenden ILM-Vorgänge durchgeführt:

- Neue von Mandanten A aufgenommene Objekte werden in zwei Datenfragmente aufgeteilt und ein Paritätsfragment wird hinzugefügt. Dann wird jedes der drei Fragmente an einem anderen Ort gespeichert.
- Die vorhandenen Objekte, die von Mandant A gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die ILM-Anweisungen ein neues Erasure-Coding-Profil verwenden, werden völlig neue Fragmente erstellt und an die drei Standorte verteilt, die zur Fehlerkorrektur codiert wurden.



Die vorhandenen 2+1-Fragmente an Standort 1 werden nicht wiederverwendet. StorageGRID betrachtet jedes Erasure Coding-Profil als einzigartig und wiederverwendet bei der Verwendung eines neuen Profils keine Fragmente des Erasure Coding.

Was geschieht, wenn sich Replikationsanweisungen ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte anderer Mandanten mithilfe von zwei replizierten Kopien in Storage Pools an Standorten 1 und 2 geschützt. In der neuen vorgeschlagenen ILM-Richtlinie werden Objekte anderer Mandanten mit drei replizierten Kopien in Storage Pools an Standorten 1, 2 und 3 gesichert.

Wenn die neue ILM-Richtlinie aktiviert ist, werden die folgenden ILM-Vorgänge durchgeführt:

- Wenn ein anderer Mandant als Mandant A ein neues Objekt aufnimmt, erstellt StorageGRID drei Kopien und speichert eine Kopie an jedem Standort.
- Vorhandene Objekte, die zu diesen anderen Mandanten gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die vorhandenen Objektkopien an Standort 1 und Standort 2 weiterhin die 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 Performance

Wenn die vorgeschlagene ILM-Richtlinie in diesem Beispiel aktiviert ist, wird die Gesamtleistung dieses StorageGRID Systems vorübergehend beeinträchtigt. Wenn die Grid-Ressourcen höher als die normalen Level sind, werden neue Fragmente, die nach der Fehlerkorrektur codiert wurden, für vorhandene Objekte von

Mandant A und neue replizierte Kopien an Standort 3 für vorhandene Objekte anderer Mandanten erstellt.

Aufgrund der Änderung der ILM-Richtlinie können Lese- und Schreibanfragen von Clients vorübergehend höhere Latenzen aufweisen als die normalen Latenzen. Die Latenzen kehren wieder auf die normalen Werte zurück, nachdem die Anweisungen zur Platzierung im gesamten Grid vollständig implementiert wurden.

Um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter für die Aufnahmezeit in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie für die Aufnahme-Zeit den Wert fest, der ungefähr der Zeit entspricht, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.



Wenden Sie sich an den technischen Support, wenn Sie die Verarbeitungsgeschwindigkeit von Objekten nach einer ILM-Richtlinienänderung verlangsamen oder erhöhen müssen.

Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock

Sie können den S3-Bucket, ILM-Regeln und ILM-Richtlinie in diesem Beispiel als Ausgangspunkt verwenden, wenn Sie eine ILM-Richtlinie definieren, um die Objektschutz- und Aufbewahrungsanforderungen für Objekte in Buckets zu erfüllen, wenn S3-Objektsperre aktiviert ist.



Wenn Sie die Funktion „ältere Compliance“ in früheren StorageGRID Versionen verwendet haben, können Sie dieses Beispiel auch zur Verwaltung vorhandener Buckets verwenden, in denen die alte Compliance-Funktion aktiviert ist.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Verwandte Informationen

- ["Objekte managen mit S3 Object Lock"](#)
- ["ILM-Richtlinie erstellen"](#)

Bucket und Objekte für S3 Object Lock Beispiel

In diesem Beispiel hat ein S3-Mandantenkonto mit der Bezeichnung „Bank of ABC“ durch den Mandanten-Manager einen Bucket erstellt, der mit S3-Objektsperre aktiviert wurde, um kritische Bankdatensätze zu speichern.

Bucket-Definition	Beispielwert
Name Des Mandantenkontos	Bank von ABC
Bucket-Name	bankaufzeichnungen
Bucket-Region	US-East-1 (Standard)

Jedes Objekt und jede Objektversion, die dem Bucket für die Bankdatensätze hinzugefügt wird, verwenden die

folgenden Werte für `retain-until-date` Und `legal hold` Einstellungen.

Einstellung für jedes Objekt	Beispielwert
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30. Dezember 2030) Jede Objektversion hat ihre eigene <code>retain-until-date</code> Einstellung. Diese Einstellung kann erhöht, aber nicht verringert werden.
<code>legal hold</code>	"OFF" (Nicht wirksam) Eine gesetzliche Aufbewahrungsphase kann jederzeit während der Aufbewahrungsfrist auf jeder Objektversion platziert oder aufgehoben werden. Befindet sich ein Objekt unter einem Legal Hold, kann das Objekt auch dann nicht gelöscht werden, wenn das <code>retain-until-date</code> Wurde erreicht.

ILM-Regel 1 für S3 Object Lock Beispiel: Profil für Erasure Coding mit Bucket-Zuordnung

Diese Beispiel-ILM-Regel gilt nur für das S3-Mandantenkonto namens Bank of ABC. Sie entspricht jedem Objekt im `bank-records` Bucket und anschließend Erasure Coding zur Speicherung des Objekts auf Storage Nodes an drei Datacenter-Standorten mithilfe eines 6+3 Erasure Coding-Profiles Diese Regel erfüllt die Anforderungen von Buckets mit aktivierter S3 Object Lock: Eine Kopie wird auf Storage-Nodes vom Tag 0 bis dauerhaft aufbewahrt. Als Referenzzeit wird die Aufnahmezeit verwendet.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte in Bank-Records Bucket - Bank of ABC
Mandantenkonto	Bank von ABC
Bucket-Name	<code>bank-records</code>
Erweiterter Filter	Objektgröße (MB) größer als 1 Hinweis: dieser Filter stellt sicher, dass das Erasure Coding nicht für Objekte 1 MB oder kleiner verwendet wird.

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Ab Tag 0 dauerhaft speichern
Verfahren Zur Einhaltung Von Datenkonsistenz	<ul style="list-style-type: none"> • Erstellen einer mit Erasure Coding verschlüsselten Kopie auf Storage-Nodes an drei Datacenter-Standorten • Verwendet das Erasure Coding-Schema 6+3

ILM-Regel 2 für S3 Object Lock Beispiel: Nicht konforme Regel

Diese Beispiel-ILM-Regel speichert zunächst zwei replizierte Objektkopien auf Storage Nodes. Nach einem Jahr wird für immer eine Kopie auf einem Cloud-Storage-Pool gespeichert. Da diese Regel einen Cloud-Storage-Pool verwendet, ist diese nicht konform und gilt nicht für Objekte in Buckets, deren S3-Objektsperre aktiviert ist.

Regeldefinition	Beispielwert
Regelname	Nicht konforme Regel: Cloud Storage Pool
Mandantenkonten	Nicht angegeben
Bucket-Name	Nicht angegeben, gilt aber nur für Buckets, für die die S3-Objektsperre (oder die ältere Compliance-Funktion) nicht aktiviert ist.
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	<ul style="list-style-type: none">• Halten Sie am Tag 0 zwei replizierte Kopien auf Storage Nodes in Datacenter 1 und Datacenter 2 für 365 Tage• Nach einem Jahr sollte eine replizierte Kopie immer in einem Cloud-Storage-Pool aufbewahrt werden

ILM-Regel 3 für S3 Object Lock Beispiel: Standardregel

Diese Beispiel-ILM-Regel kopiert Objektdaten in Storage-Pools in zwei Datacentern. Diese konforme Regel wurde als Standardregel in der ILM-Richtlinie konzipiert. Es enthält keine Filter, verwendet keine nicht aktuelle Referenzzeit und erfüllt die Anforderungen von Buckets mit aktivierter S3 Objektsperre: Zwei Objektkopien werden auf Storage-Nodes aufbewahrt von Tag 0 bis für immer und verwenden die Aufnahme als Referenzzeit.

Regeldefinition	Beispielwert
Regelname	Standard-konforme Regel: Zwei Kopien zwei Rechenzentren
Mandantenkonto	Nicht angegeben
Bucket-Name	Nicht angegeben
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Halten Sie von Tag 0 bis für immer zwei replizierte Kopien bereit – eins auf Storage-Nodes im Datacenter 1 und eins auf Storage-Nodes im Datacenter 2.

Konforme ILM-Richtlinie für S3 Object Lock Beispiel

Zum Erstellen einer ILM-Richtlinie, die alle Objekte in Ihrem System effektiv schützt, auch in Buckets, deren S3-Objektsperre aktiviert ist, müssen Sie ILM-Regeln auswählen, die die Storage-Anforderungen für alle Objekte erfüllen. Anschließend müssen Sie die vorgeschlagene Richtlinie simulieren und aktivieren.

Fügen Sie der Richtlinie Regeln hinzu

In diesem Beispiel umfasst die ILM-Richtlinie drei ILM-Regeln in der folgenden Reihenfolge:

1. Eine konforme Regel, die Erasure Coding verwendet, um Objekte mit einer Größe von mehr als 1 MB in einem bestimmten Bucket zu schützen. Dabei ist S3 Object Lock aktiviert. Die Objekte werden von Tag 0 bis für immer auf Speicherknoten gespeichert.
2. Eine nicht konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes für ein Jahr erstellt und dann eine Objektkopie für immer in einen Cloud Storage Pool verschiebt. Diese Regel gilt nicht für Buckets, für die S3-Objektsperre aktiviert ist, da sie einen Cloud-Storage-Pool verwendet.
3. Die standardmäßige, konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes erstellt, von Tag 0 bis für immer.

Simulieren Sie die vorgeschlagene Richtlinie

Nachdem Sie in Ihrer vorgeschlagenen Richtlinie Regeln hinzugefügt, eine standardkonforme Regel ausgewählt und die anderen Regeln festgelegt haben, sollten Sie die Richtlinie simulieren, indem Sie Objekte aus dem Bucket testen, wobei S3 Object Lock aktiviert ist und aus anderen Buckets. Wenn Sie beispielsweise die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Die erste Regel entspricht nur Testobjekten, die mehr als 1 MB in den Bucket-Bankdatensätzen für den Mandanten der Bank of ABC enthalten sind.
- Die zweite Regel entspricht allen Objekten in allen nicht-konformen Buckets für alle anderen Mandantenkonten.
- Die Standardregel stimmt mit den folgenden Objekten überein:
 - Objekte 1 MB oder kleiner in den Bucket-Bankdatensätzen für die Bank of ABC-Mieter.
 - Objekte in jedem anderen Bucket, bei dem die S3-Objektsperre für alle anderen Mandantenkonten aktiviert ist

Aktivieren Sie die Richtlinie

Wenn Sie mit der neuen Richtlinie zufrieden sind, dass Objektdaten wie erwartet geschützt werden, können Sie sie aktivieren.

Systemhärtung

Systemhärtung: Übersicht

Systemhärtung ist der Prozess, bei dem so viele Sicherheitsrisiken wie möglich durch ein StorageGRID System beseitigt werden.

Dieses Dokument bietet einen Überblick über die StorageGRID-spezifischen Härtingsrichtlinien. Diese Richtlinien sind eine Ergänzung zu branchenüblichen Best Practices zur Systemhärtung. In diesen Richtlinien wird beispielsweise davon ausgegangen, dass Sie für StorageGRID starke Passwörter verwenden, HTTPS statt HTTP verwenden und sofern verfügbar die zertifikatbasierte Authentifizierung aktivieren.

Bei der Installation und Konfiguration von StorageGRID können Sie diese Richtlinien nutzen, um alle vorgeschriebenen Sicherheitsziele bezüglich Vertraulichkeit, Integrität und Verfügbarkeit des Informationssystems zu erfüllen.

StorageGRID folgt dem ["NetApp Richtlinie zur Bearbeitung von Schwachstellen"](#). Gemeldete Schwachstellen werden gemäß dem Prozess der Reaktion auf Produktsicherheitsvorfälle überprüft und behoben.

Allgemeine Überlegungen zur Erhöhung der StorageGRID-Systeme

Beim Härten eines StorageGRID Systems sind folgende Punkte zu beachten:

- Welches der drei implementierten StorageGRID-Netzwerke ist implementiert? Alle StorageGRID-Systeme müssen das Grid-Netzwerk verwenden, aber Sie können auch das Admin-Netzwerk, das Client-Netzwerk oder beide verwenden. Jedes Netzwerk weist unterschiedliche Sicherheitsüberlegungen auf.
- Die Art der Plattformen, die Sie für die einzelnen Nodes Ihres StorageGRID Systems verwenden. StorageGRID Nodes können auf VMware Virtual Machines innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattfortyp verfügt über eigene Best Practices zur Härtung.
- Wie vertrauenswürdig sind die Mandantenkonten? Wenn Sie ein Service-Provider mit nicht vertrauenswürdigen Mandantenkonten sind, haben Sie andere Sicherheitsbedenken als, wenn Sie nur vertrauenswürdige interne Mandanten verwenden.
- Welche Sicherheitsanforderungen und -Konventionen von Ihrem Unternehmen erfüllt werden? Möglicherweise müssen Sie bestimmte gesetzliche oder unternehmensbezogene Anforderungen einhalten.

Hardening-Richtlinien für Software Upgrades

Sie müssen Ihr StorageGRID-System und die zugehörigen Services immer auf dem neuesten Stand halten, um sich gegen Angriffe zu wehren.

Upgrades auf StorageGRID Software

Sofern möglich, sollten Sie ein Upgrade der StorageGRID Software auf das neueste Hauptversion oder auf das vorherige Hauptversion durchführen. Durch die aktuelle Nutzung von StorageGRID lässt sich die Zeit bis zur aktiven Nutzung bekannter Schwachstellen reduzieren und gleichzeitig die Angriffsfläche insgesamt verringern. Darüber hinaus enthalten die neuesten StorageGRID Versionen häufig Funktionen zur Erhöhung der Sicherheit, die in früheren Versionen nicht enthalten sind.

Konsultieren Sie die ["NetApp Interoperabilitäts-Matrix-Tool"](#) (IMT), um zu ermitteln, welche Version der StorageGRID-Software Sie verwenden sollen. Wenn ein Hotfix erforderlich ist, priorisiert NetApp die Erstellung von Updates der letzten Versionen. Einige Patches sind möglicherweise nicht mit früheren Versionen kompatibel.

- Die neuesten StorageGRID Versionen und Hotfixes können Sie unter herunterladen "[NetApp Downloads: StorageGRID](#)".
- Informationen zum Aktualisieren der StorageGRID-Software finden Sie im "[Upgrade-Anweisungen](#)".
- Informationen zum Anwenden eines Hotfix finden Sie im "[StorageGRID Hotfix Verfahren](#)".

Upgrades auf externe Dienste

Externe Services können Schwachstellen aufweisen, die StorageGRID indirekt beeinträchtigen. Sie sollten sicherstellen, dass die Services, von denen StorageGRID abhängig sind, immer auf dem neuesten Stand sind. Zu diesen Services gehören LDAP, KMS (oder KMIP Server), DNS und NTP.

Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool](#)" Um eine Liste der unterstützten Versionen zu erhalten.

Upgrades auf Hypervisoren

Wenn die StorageGRID-Nodes auf VMware oder einem anderen Hypervisor ausgeführt werden, müssen Sie sicherstellen, dass die Hypervisor-Software und die Firmware auf dem neuesten Stand sind.

Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool](#)" Um eine Liste der unterstützten Versionen zu erhalten.

Upgrades auf Linux-Knoten

Wenn Ihre StorageGRID-Knoten Linux-Hostplattformen verwenden, müssen Sie sicherstellen, dass Sicherheitsupdates und Kernel-Updates auf das Host-Betriebssystem angewendet werden. Darüber hinaus müssen Sie Firmware-Updates auf anfällige Hardware anwenden, wenn diese Updates verfügbar sind.

Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool](#)" Um eine Liste der unterstützten Versionen zu erhalten.

Hardening Guidelines for StorageGRID Networks

Das StorageGRID System unterstützt bis zu drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass er Ihren Sicherheits- und Zugriffsanforderungen entspricht.

Ausführliche Informationen zu StorageGRID-Netzwerken finden Sie im "[StorageGRID-Netzwerktypen](#)".

Richtlinien für Grid Network

Sie müssen ein Grid-Netzwerk für den gesamten internen StorageGRID-Datenverkehr konfigurieren. Alle Grid-Nodes sind im Grid-Netzwerk und müssen mit allen anderen Nodes kommunizieren können.

Befolgen Sie bei der Konfiguration des Grid-Netzwerks die folgenden Richtlinien:

- Stellen Sie sicher, dass das Netzwerk von nicht vertrauenswürdigen Clients, wie denen im offenen Internet, geschützt ist.
- Wenn möglich, verwenden Sie das Grid-Netzwerk ausschließlich für den internen Datenverkehr. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk haben zusätzliche Firewall-Einschränkungen, die externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Datenverkehr wird unterstützt, aber diese Verwendung bietet weniger Schutzebenen.

- Wenn die StorageGRID Implementierung mehrere Datacenter umfasst, verwenden Sie ein virtuelles privates Netzwerk (VPN) oder eine vergleichbare Position im Grid-Netzwerk, um den internen Datenverkehr zusätzlich zu schützen.
- Einige Wartungsverfahren erfordern einen sicheren SSH-Zugriff (Shell) auf Port 22 zwischen dem primären Admin-Node und allen anderen Grid-Nodes. Verwenden Sie eine externe Firewall, um den SSH-Zugriff auf vertrauenswürdige Clients zu beschränken.

Richtlinien für Admin Network

Das Admin-Netzwerk wird normalerweise für administrative Aufgaben verwendet (vertrauenswürdige Mitarbeiter, die den Grid Manager oder SSH verwenden) und für die Kommunikation mit anderen vertrauenswürdigen Services wie LDAP, DNS, NTP oder KMS (oder KMIP Server). StorageGRID ist jedoch nicht intern durchsetzen.

Wenn Sie das Admin-Netzwerk verwenden, befolgen Sie die folgenden Richtlinien:

- Blockieren Sie alle internen Traffic-Ports im Admin-Netzwerk. Siehe "[Liste der internen Ports](#)".
- Wenn nicht vertrauenswürdige Clients auf das Admin-Netzwerk zugreifen können, blockieren Sie den Zugriff auf StorageGRID im Admin-Netzwerk mit einer externen Firewall.

Richtlinien für Client Network

Das Client-Netzwerk wird typischerweise für Mandanten und zur Kommunikation mit externen Services wie dem CloudMirror Replikationsservice oder einem anderen Plattformservice verwendet. StorageGRID ist jedoch nicht intern durchsetzen.

Wenn Sie das Client-Netzwerk verwenden, befolgen Sie die folgenden Richtlinien:

- Blockieren Sie alle internen Traffic-Ports im Client-Netzwerk. Siehe "[Liste der internen Ports](#)".
- Eingehende Clientdatenverkehr nur an explizit konfigurierten Endpunkten akzeptieren. Weitere Informationen finden Sie unter "[Management der Firewall-Kontrollen](#)".

Hardening-Richtlinien für StorageGRID-Knoten

StorageGRID Nodes können auf VMware Virtual Machines innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattfortyp und jeder Node-Typ verfügt über eigene Best Practices zur Härtung.

Firewall-Konfiguration

Im Rahmen des System-Hardening-Prozesses müssen Sie externe Firewall-Konfigurationen überprüfen und ändern, damit der Datenverkehr nur von den IP-Adressen und den Ports akzeptiert wird, von denen er unbedingt benötigt wird.

StorageGRID verfügt über eine interne Firewall auf jedem Node, die die Sicherheit Ihres Grids erhöht, indem Sie den Netzwerkzugriff auf den Node kontrollieren können. Sollten Sie "[Interne Firewall-Kontrollen verwalten](#)". Um den Netzwerkzugriff auf allen Ports zu verhindern, mit Ausnahme der Ports, die für Ihre spezifische Grid-Bereitstellung erforderlich sind. Die Konfigurationsänderungen, die Sie auf der Seite Firewall-Steuerung vornehmen, werden für jeden Knoten bereitgestellt.

Sie können insbesondere diese Bereiche managen:

- **Privilegierte Adressen:** Sie können ausgewählten IP-Adressen oder Subnetzen erlauben, auf Ports zuzugreifen, die durch Einstellungen auf der Registerkarte externen Zugriff verwalten geschlossen werden.
- **Externen Zugriff verwalten:** Sie können Ports schließen, die standardmäßig geöffnet sind, oder zuvor geschlossene Ports wieder öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk:** Sie können angeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk sowie die zusätzlichen Ports, die geöffnet werden sollen, wenn nicht vertrauenswürdige Client-Netzwerke konfiguriert ist, anvertraut.

Diese interne Firewall bietet zwar eine zusätzliche Schutzschicht gegen häufig vorkommende Bedrohungen, sie macht aber keine externe Firewall erforderlich.

Eine Liste aller internen und externen Ports, die von StorageGRID verwendet werden, finden Sie unter ["Referenz für Netzwerk-Ports"](#).

Deaktivieren Sie nicht verwendete Dienste

Bei allen StorageGRID-Knoten sollten Sie den Zugriff auf nicht genutzte Services deaktivieren oder blockieren. Wenn Sie beispielsweise nicht planen, den Clientzugriff auf die Audit-Freigaben für NFS zu konfigurieren, blockieren oder deaktivieren Sie den Zugriff auf diese Services.

Virtualisierung, Container und gemeinsam genutzte Hardware

Vermeiden Sie bei allen StorageGRID Nodes die Ausführung von StorageGRID auf derselben physischen Hardware wie die nicht vertrauenswürdige Software. Setzen Sie nicht voraus, dass ein Hypervisor-Schutz Malware den Zugriff auf StorageGRID geschützte Daten verhindert, wenn sich sowohl StorageGRID als auch Malware auf derselben physischen Hardware befinden. So nutzen beispielsweise die Meltdown- und Specter-Angriffe kritische Schwachstellen in modernen Prozessoren und ermöglichen Programmen, Daten im Arbeitsspeicher auf demselben Computer zu stehlen.

Schutz von Nodes während der Installation

Erlauben Sie nicht vertrauenswürdigen Benutzern den Zugriff auf StorageGRID-Knoten über das Netzwerk, wenn die Knoten installiert werden. Nodes sind erst dann vollständig sicher, wenn sie sich dem Grid angeschlossen haben.

Richtlinien für Admin-Nodes

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Wenn Sie sich beim Grid Manager oder dem Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her.

Befolgen Sie diese Richtlinien, um die Admin-Knoten in Ihrem StorageGRID-System zu sichern:

- Sichern Sie alle Admin-Knoten von nicht vertrauenswürdigen Clients, wie denen im offenen Internet. Stellen Sie sicher, dass kein nicht vertrauenswürdiger Client auf einen beliebigen Admin-Node im Grid-Netzwerk, auf das Admin-Netzwerk oder auf das Client-Netzwerk zugreifen kann.
- StorageGRID-Gruppen steuern den Zugriff auf Grid Manager- und Mandantenmanager-Funktionen. Gewähren Sie jeder Gruppe von Benutzern die erforderlichen Mindestberechtigungen für ihre Rolle, und verwenden Sie den schreibgeschützten Zugriffsmodus, um zu verhindern, dass Benutzer die Konfiguration ändern.
- Verwenden Sie bei der Verwendung von StorageGRID Load Balancer-Endpunkten Gateway-Nodes anstelle von Admin-Nodes für nicht vertrauenswürdigen Client-Datenverkehr.

- Wenn Sie nicht vertrauenswürdige Mandanten haben, erlauben Sie ihnen keinen direkten Zugriff auf den Mandantenmanager oder die Mandantenmanagement-API. Verwenden Sie stattdessen ein Mandantenportal oder ein externes Mandantenmanagement-System, das mit der Mandantenmanagement-API interagiert.
- Optional können Sie einen Admin-Proxy verwenden, um die AutoSupport-Kommunikation zwischen Admin-Nodes und dem NetApp Support besser zu steuern. Siehe die Schritte für "[Erstellen eines Admin-Proxys](#)".
- Verwenden Sie optional die eingeschränkten 8443- und 9443-Ports, um die Kommunikation zwischen Grid Manager und Tenant Manager voneinander zu trennen. Blockieren Sie den gemeinsam genutzten Port 443 und beschränken Sie Mandantenanforderungen auf Port 9443, um zusätzlichen Schutz zu bieten.
- Verwenden Sie optional separate Admin-Nodes für Grid-Administratoren und Mandantenbenutzer.

Weitere Informationen finden Sie in den Anweisungen für "[Administration von StorageGRID](#)".

Richtlinien für Storage-Nodes

Storage-Nodes managen und speichern Objektdaten und Metadaten. Befolgen Sie diese Richtlinien, um die Speicherknoten in Ihrem StorageGRID System zu sichern.

- Nicht vertrauenswürdige Clients dürfen keine direkte Verbindung zu Storage-Nodes herstellen. Verwenden Sie einen Load Balancer-Endpunkt, der von einem Gateway-Node oder einem Load Balancer eines Drittanbieters bereitgestellt wird.
- Aktivieren Sie keine ausgehenden Dienste für nicht vertrauenswürdige Mandanten. Wenn Sie beispielsweise das Konto für einen nicht vertrauenswürdigen Mandanten erstellen, erlauben Sie dem Mandanten nicht, seine eigene Identitätsquelle zu verwenden, und erlauben Sie nicht die Nutzung von Plattformdiensten. Siehe die Schritte für "[Erstellen eines Mandantenkontos](#)".
- Verwenden Sie einen Drittanbieter-Load-Balancer für nicht vertrauenswürdigen Client-Datenverkehr. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen.
- Optional können Sie einen Storage Proxy verwenden, um mehr Kontrolle über Cloud Storage Pools und die Kommunikation von Plattform-Services von Storage Nodes zu externen Services zu erhalten. Siehe die Schritte für "[Erstellen eines Speicherproxys](#)".
- Optional können Sie über das Client-Netzwerk eine Verbindung zu externen Diensten herstellen. Wählen Sie dann **CONFIGURATION > Security > Firewall Control > UnTrusted Client Networks** aus und geben Sie an, dass das Client-Netzwerk auf dem Storage Node nicht vertrauenswürdig ist. Der Speicherknoten akzeptiert keinen eingehenden Datenverkehr im Client-Netzwerk mehr, aber er erlaubt weiterhin ausgehende Anfragen für Platform Services.

Richtlinien für Gateway-Nodes

Gateway-Knoten stellen eine optionale Schnittstelle zum Lastausgleich bereit, über die Client-Anwendungen eine Verbindung zu StorageGRID herstellen können. Befolgen Sie die folgenden Richtlinien zum Sichern aller Gateway-Knoten in Ihrem StorageGRID System:

- Konfigurieren und verwenden Sie Load Balancer-Endpunkte. Siehe "[Überlegungen zum Lastausgleich](#)".
- Verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr einen Drittanbieter-Load-Balancer zwischen Client und Gateway-Node oder Storage-Nodes. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen. Wenn Sie einen Load Balancer eines Drittanbieters verwenden, kann der Netzwerk-Traffic optional auch so konfiguriert werden, dass er über einen internen Load Balancer-Endpunkt geleitet oder direkt an Storage Nodes gesendet wird.
- Wenn Sie Load Balancer-Endpunkte verwenden, lassen Sie optional Clients über das Client-Netzwerk verbinden. Wählen Sie dann **CONFIGURATION > Security > Firewall Control > UnTrusted Client**

Networks aus und geben Sie an, dass das Client-Netzwerk auf dem Gateway Node nicht vertrauenswürdig ist. Der Gateway-Node akzeptiert nur eingehenden Datenverkehr an den Ports, die explizit als Load Balancer-Endpunkte konfiguriert wurden.

Richtlinien für die Nodes von Hardware-Appliances

StorageGRID Hardware-Appliances wurden speziell für den Einsatz in einem StorageGRID System entwickelt. Einige Geräte können als Storage-Nodes verwendet werden. Andere Appliances können als Admin-Nodes oder Gateway-Nodes verwendet werden. Appliance-Nodes können mit softwarebasierten Nodes kombiniert oder voll entwickelten All-Appliance-Grids implementiert werden.

Beachten Sie diese Richtlinien zum Schutz aller Hardware-Appliance-Nodes in Ihrem StorageGRID System:

- Wenn die Appliance SANtricity System Manager zum Management des Storage Controllers verwendet, verhindern Sie, dass nicht vertrauenswürdige Clients über das Netzwerk auf SANtricity System Manager zugreifen.
- Wenn die Appliance über einen Baseboard Management Controller (BMC) verfügt, beachten Sie, dass der BMC-Management-Port einen niedrigen Hardwarezugriff ermöglicht. Schließen Sie den BMC-Management-Port nur an ein sicheres, vertrauenswürdiges, internes Management-Netzwerk an. Wenn kein solches Netzwerk verfügbar ist, lassen Sie den BMC-Management-Port unverbunden oder blockiert, es sei denn, eine BMC-Verbindung wird vom technischen Support angefordert.
- Wenn die Appliance die Remote-Verwaltung der Controller-Hardware über Ethernet mit dem IPMI-Standard (Intelligent Platform Management Interface) unterstützt, blockieren Sie den nicht vertrauenswürdigen Datenverkehr auf Port 623.



Sie können den Remote-IPMI-Zugriff für alle Appliances aktivieren oder deaktivieren, die einen BMC enthalten, indem Sie den privaten Endpunkt der Management-API VERWENDEN, PUT /private/bmc.

- Wenn der Storage Controller in der Appliance Laufwerke mit FDE- oder FIPS-Laufwerken umfasst und die Laufwerkssicherheitsfunktion aktiviert ist, konfigurieren Sie die Schlüssel zur Laufwerksicherheit mithilfe von SANtricity. Siehe "[Konfiguration von SANtricity System Manager \(SG6000 und SG5700\)](#)".
- Bei Appliances ohne FDE- oder FIPS-Laufwerke ermöglicht die Node-Verschlüsselung mithilfe eines Key Management Servers (KMS). Siehe "[Optional: Node-Verschlüsselung aktivieren](#)".

Härtungsrichtlinien für TLS und SSH

Sie sollten die während der Installation erstellten Standardzertifikate ersetzen und die entsprechende Sicherheitsrichtlinie für TLS- und SSH-Verbindungen auswählen.

Richtlinien für die Härtung von Zertifikaten

Sie sollten die während der Installation erstellten Standardzertifikate durch eigene benutzerdefinierte Zertifikate ersetzen.

Für viele Unternehmen entspricht das selbstsignierte digitale Zertifikat für den StorageGRID-Webzugriff nicht den Richtlinien für die Informationssicherheit. Auf Produktionssystemen sollten Sie ein CA-signiertes digitales Zertifikat zur Verwendung bei der Authentifizierung von StorageGRID installieren.

Sie sollten insbesondere anstelle der folgenden Standardzertifikate benutzerdefinierte Serverzertifikate verwenden:

- **Zertifikat der Verwaltungsschnittstelle:** Zur Sicherung des Zugriffs auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API.
- **S3- und Swift-API-Zertifikat:** Dient zum sicheren Zugriff auf Storage-Nodes und Gateway-Nodes, die S3- und Swift-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

Siehe "[Verwalten von Sicherheitszertifikaten](#)" Für Details und Anweisungen.



StorageGRID managt die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie unter "[Konfigurieren von Load Balancer-Endpunkten](#)".

Wenn Sie benutzerdefinierte Serverzertifikate verwenden, befolgen Sie die folgenden Richtlinien:

- Zertifikate sollten ein haben `subjectAltName` Das stimmt mit DNS-Einträgen für StorageGRID überein. Weitere Informationen finden Sie in Abschnitt 4.2.1.6, „`sAlternative Name des Subject`“ in "[RFC 5280: PKIX-Zertifikat und CRL-Profil](#)".
- Wenn möglich, vermeiden Sie die Verwendung von Platzhalterzertifikaten. Eine Ausnahme dieser Richtlinie ist das Zertifikat für einen S3-Endpunkt im virtuellen Hosted-Stil, der die Verwendung eines Platzhalters erfordert, wenn Bucket-Namen nicht im Voraus bekannt sind.
- Wenn Sie Wildcards in Zertifikaten verwenden müssen, sollten Sie weitere Schritte zur Reduzierung der Risiken Unternehmen. Verwenden Sie ein Platzhalter-Muster z. B. `*.s3.example.com`` Und verwenden Sie nicht die ``s3.example.com` Suffix für andere Applikationen Dieses Muster funktioniert auch mit Path-Style S3-Zugriff, z. B. `dc1-s1.s3.example.com/mybucket`.
- Legen Sie die Ablaufzeiten für das Zertifikat auf kurz (z. B. 2 Monate) fest, und automatisieren Sie die Zertifikatrotation mithilfe der Grid Management API. Dies ist besonders wichtig für Platzhalterzertifikate.

Darüber hinaus sollten Kunden bei der Kommunikation mit StorageGRID strenge Hostnamen-Kontrollen verwenden.

Richtlinien für die Härtung von TLS- und SSH-Richtlinien

Sie können eine Sicherheitsrichtlinie auswählen, um festzulegen, welche Protokolle und Chiffren zum Aufbau sicherer TLS-Verbindungen mit Clientanwendungen und sicherer SSH-Verbindungen zu internen StorageGRID-Diensten verwendet werden.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten in Bewegung verschlüsseln. Als Best Practice sollten Sie Verschlüsselungsoptionen deaktivieren, die für die Anwendungscompatibilität nicht erforderlich sind. Verwenden Sie die moderne Standardrichtlinie, es sei denn, Ihr System muss Common Criteria-konform sein oder Sie müssen andere Chiffren verwenden.

Siehe "[Verwalten Sie die TLS- und SSH-Richtlinie](#)" Für Details und Anweisungen.

Andere Hinweise zur Verhärtung

Beachten Sie zusätzlich die Hinweise zur Verhärtung von StorageGRID-Netzwerken und -Knoten die Härtungsrichtlinien für andere Bereiche des StorageGRID-Systems.

Protokolle und Prüfmeldungen

Sichern Sie StorageGRID-Protokolle und die Ausgabe von Prüfnachrichten sicher. StorageGRID-Protokolle und Audit-Meldungen bieten wertvolle Informationen aus Sicht der Support- und Systemverfügbarkeit. Darüber

hinaus handelt es sich bei den Informationen und Details der StorageGRID-Protokolle und der Ausgabe von Audit-Meldungen in der Regel um sensible Daten.

Konfigurieren Sie StorageGRID, um Sicherheitsereignisse an einen externen Syslog-Server zu senden. Wenn Sie syslog-Export verwenden, wählen Sie TLS und RELP/TLS für die Transportprotokolle aus.

Siehe ["Referenz für Protokolldateien"](#) Weitere Informationen zu StorageGRID-Protokollen. Siehe ["Audit-Meldungen"](#) Weitere Informationen zu StorageGRID-Überwachungsmeldungen.

NetApp AutoSupport

Mit der AutoSupport Funktion von StorageGRID überwachen Sie proaktiv den Zustand Ihres Systems und senden automatisch Nachrichten und Details an den NetApp Technical Support, das interne Support-Team Ihres Unternehmens oder einen Support-Partner. Standardmäßig werden AutoSupport Meldungen an den technischen Support von NetApp aktiviert, wenn StorageGRID zum ersten Mal konfiguriert wird.

Die AutoSupport-Funktion kann deaktiviert werden. NetApp empfiehlt jedoch die Aktivierung, da AutoSupport die Identifizierung von Problemen und die Behebung von Problemen beschleunigt, wenn es auf Ihrem StorageGRID System zu Problemen kommt.

AutoSupport unterstützt HTTPS, HTTP und SMTP für Transportprotokolle. Aufgrund der sensiblen Eigenschaften von AutoSupport Meldungen empfiehlt NetApp dringend die Verwendung von HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an den NetApp Support.

Cross-Origin Resource Sharing (CORS)

Sie können CORS (Cross-Origin Resource Sharing) für einen S3-Bucket konfigurieren, wenn Webapplikationen in anderen Domänen auf diesen Bucket und die Objekte in diesem Bucket zugreifen sollen. Im Allgemeinen sollten Sie CORS nur aktivieren, wenn dies erforderlich ist. Wenn CORS erforderlich ist, beschränken Sie es auf vertrauenswürdige Herkunft.

Siehe die Schritte für ["Konfigurieren der Cross-Origin Resource Sharing \(CORS\)"](#).

Externe Sicherheitsgeräte

Eine vollständige Härtungslösung muss auch Sicherheitsmechanismen außerhalb von StorageGRID berücksichtigen. Der Einsatz zusätzlicher Infrastrukturgeräte zum Filtern und zur Einschränkung des Zugriffs auf StorageGRID ist eine effektive Möglichkeit, eine anspruchsvolle Sicherheit zu schaffen und zu erhalten. Zu diesen externen Sicherheitsgeräten gehören Firewalls, Intrusion Prevention Systems (IPSs) und andere Sicherheitsgeräte.

Für nicht vertrauenswürdigen Client-Datenverkehr wird ein Load Balancer eines Drittanbieters empfohlen. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen.

Ransomware-Minderung

Befolgen Sie die Empfehlungen in, um Ihre Objektdaten vor Ransomware-Angriffen zu schützen ["Ransomware-Verteidigung mit StorageGRID"](#).

Konfigurieren Sie StorageGRID für FabricPool

Configure StorageGRID for FabricPool: Übersicht

Wenn Sie NetApp ONTAP Software verwenden, können Sie NetApp FabricPool verwenden, um inaktive Daten auf ein NetApp StorageGRID Objekt-Storage-System zu verschieben.

Mithilfe dieser Anweisungen können Sie:

- Erfahren Sie mehr über die Überlegungen und Best Practices bei der Konfiguration von StorageGRID für einen FabricPool-Workload.
- Erfahren Sie, wie Sie ein StorageGRID Objekt-Storage-System zur Verwendung mit FabricPool konfigurieren.
- Erfahren Sie, wie Sie ONTAP die erforderlichen Werte vermitteln, wenn Sie StorageGRID als FabricPool Cloud Tier einbinden.

Schnellstart für die Konfiguration von StorageGRID für FabricPool

1

Planen Sie Ihre Konfiguration

- Legen Sie fest, welche FabricPool Volume Tiering-Richtlinie Sie für das Tiering inaktiver ONTAP-Daten an StorageGRID verwenden möchten.
- Planen und installieren Sie ein StorageGRID System, um Ihre Storage-Kapazitäts- und Performance-Anforderungen zu erfüllen.
- Machen Sie sich mit der StorageGRID System-Software vertraut, einschließlich der "[Grid Manager](#)" Und das "[Mandanten-Manager](#)".
- Lesen Sie die FabricPool Best Practices für "[HA-Gruppen](#)", "[Lastverteilung](#)", "[ILM](#)", und "[Mehr](#)".
- Lesen Sie diese zusätzlichen Ressourcen mit Details zur Verwendung und Konfiguration von ONTAP und FabricPool:

["TR-4598: FabricPool Best Practices in ONTAP"](#)

["ONTAP 9: FabricPool Tier-Management-Überblick mit System Manager"](#)

2

Durchführung von erforderlichen Aufgaben

Beziehen Sie die "[Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier](#)", Einschließlich:

- IP-Adressen
- Domain-Namen
- SSL-Zertifikat

Optional konfigurieren "[Identitätsföderation](#)" Und "[Single Sign On](#)".

3

Konfigurieren Sie die StorageGRID-Einstellungen

Verwenden Sie StorageGRID, um die Werte zu ermitteln, die ONTAP für die Verbindung mit dem Grid benötigt.

Verwenden der "[FabricPool Setup-Assistent](#)" Dies ist die empfohlene und schnellste Methode zum Konfigurieren aller Elemente, Sie können aber auch jede Einheit manuell konfigurieren, falls erforderlich.

4

Konfigurieren Sie ONTAP und DNS

Verwenden Sie ONTAP für "[Fügen Sie eine Cloud-Schicht hinzu](#)" Das verwendet die StorageGRID-Werte. Dann, "[DNS-Einträge konfigurieren](#)" Um IP-Adressen mit beliebigen Domänennamen zu verknüpfen, die Sie verwenden möchten.

5

Überwachen und verwalten

Führen Sie nach der Inbetriebnahme Ihres Systems fortlaufende Aufgaben in ONTAP und StorageGRID durch, um FabricPool Daten-Tiering über einen längeren Zeitraum zu managen und zu überwachen.

Was ist FabricPool?

FabricPool ist eine ONTAP Hybrid-Storage-Lösung mit einem hochperformanten Flash-Aggregat als Performance-Tier und einem Objektspeicher als Cloud-Tier. Mit FabricPool-fähigen Aggregaten senken Sie die Storage-Kosten, ohne dabei Einbußen bei Performance, Effizienz oder Sicherheit hinnehmen zu müssen.

FabricPool ordnet eine Cloud-Tier (einen externen Objektspeicher wie StorageGRID) einer lokalen Tier (ein ONTAP Storage-Aggregat) zu, um eine zusammengesetzte Sammlung von Discs zu erstellen. Volumes innerhalb der FabricPool können dann von dem Tiering profitieren, indem häufig verwendete Daten auf hochperformantem Storage (dem lokalen Tier) bleiben und Tiering für inaktive („kalte“) Daten auf dem externen Objektspeicher (der Cloud-Tier) verschoben werden.

Es sind keine Änderungen an der Architektur erforderlich und die Daten- und Applikationsumgebung lässt sich weiterhin über das zentrale ONTAP Storage-System managen.

Was ist StorageGRID?

NetApp StorageGRID ist eine Storage-Architektur, die Daten als Objekte managt und sich nicht auf andere Storage-Architekturen wie File- oder Block-Storage unterscheidet. Objekte werden in einem einzelnen Container (z. B. Bucket) aufbewahrt und nicht als Dateien in einem Verzeichnis in anderen Verzeichnissen verschachtelt. Obwohl Objekt-Storage im Allgemeinen eine geringere Performance als Datei- oder Block-Storage bietet, ist sie deutlich skalierbarer. StorageGRID Buckets können Daten im Petabyte-Bereich und Milliarden Objekte enthalten.

Vorteile von StorageGRID als Cloud-Tier von FabricPool

FabricPool kann ONTAP-Daten auf eine Reihe von Objekt-Storage-Providern, einschließlich StorageGRID, verschieben. Im Gegensatz zu Public Clouds, bei denen eine maximale Anzahl unterstützter IOPS (Input/Output Operations per Second) auf Bucket- oder Container-Ebene festgelegt werden kann, lässt sich die StorageGRID-Performance mit der Anzahl der Nodes in einem System skalieren. Durch den Einsatz von StorageGRID als FabricPool Cloud-Tier können kalte Daten in Ihrer eigenen Private Cloud vorgehalten werden, um höchste Performance und vollständige Kontrolle über Ihre Daten zu erzielen.

Zudem ist keine FabricPool Lizenz erforderlich, wenn Sie StorageGRID als Cloud-Tier verwenden.

Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier

Bevor Sie StorageGRID als Cloud-Tier für FabricPool hinzufügen können, müssen Sie

die Konfigurationsschritte in StorageGRID durchführen und bestimmte Werte für die Verwendung in ONTAP abrufen.

Welche Werte brauche ich?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen und wie diese Werte von ONTAP und dem DNS-Server verwendet werden.

Wert	Wobei der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Endpunkt des Load Balancer	ONTAP System Manager > Cloud Tiering hinzufügen
SSL-Zertifikat	StorageGRID > Endpunkt des Load Balancer	ONTAP System Manager > Cloud Tiering hinzufügen
Servername (FQDN)	StorageGRID > Endpunkt des Load Balancer	DNS-Eintrag
Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	ONTAP System Manager > Cloud Tiering hinzufügen
Bucket/Container-Name	StorageGRID > Mandant und Bucket	ONTAP System Manager > Cloud Tiering hinzufügen

Wie erhalte ich diese Werte?

Je nach Ihren Anforderungen können Sie eine der folgenden Möglichkeiten nutzen, um die benötigten Informationen zu erhalten:

- Verwenden Sie die ["FabricPool Setup-Assistent"](#). Der FabricPool Setup-Assistent unterstützt Sie beim schnellen Konfigurieren der erforderlichen Werte in StorageGRID und gibt eine Datei aus, die Sie für die Konfiguration von ONTAP System Manager verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und stellt sicher, dass Ihre Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.
- Konfigurieren Sie jedes Element manuell. Geben Sie dann die Werte in ONTAP System Manager oder in die ONTAP CLI ein. Führen Sie hierzu folgende Schritte aus:
 - a. ["Konfigurieren Sie eine HA-Gruppe \(High Availability, Hochverfügbarkeit\) für FabricPool"](#).
 - b. ["Erstellen eines Load Balancer-Endpunkts für FabricPool"](#).
 - c. ["Erstellen eines Mandantenkontos für FabricPool"](#).
 - d. Melden Sie sich beim Mandantenkonto an, und ["Erstellen Sie den Bucket und die Zugriffsschlüssel für den Root-Benutzer"](#).
 - e. Erstellen Sie eine ILM-Regel für FabricPool-Daten und fügen Sie sie zu Ihrer aktiven ILM-Richtlinie hinzu. Siehe ["Konfigurieren Sie ILM für FabricPool-Daten"](#).
 - f. Optional ["Eine Richtlinie zur Verkehrsklassifizierung für FabricPool erstellen"](#).

Verwenden Sie den FabricPool-Einrichtungsassistenten

Überlegungen und Anforderungen im FabricPool Setup-Assistenten

Mit dem FabricPool-Einrichtungsassistenten können Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier konfigurieren. Nach Abschluss des Setup-Assistenten können Sie die erforderlichen Details in den ONTAP System Manager eingeben.

Wann der FabricPool-Einrichtungsassistent verwendet werden soll

Der FabricPool Setup-Assistent führt Sie durch die einzelnen Schritte der Konfiguration von StorageGRID für die Verwendung mit FabricPool und konfiguriert automatisch bestimmte Einheiten, z. B. ILM- und Traffic-Klassifizierungsrichtlinien. Im Rahmen der Ausführung des Assistenten laden Sie eine Datei herunter, mit der Sie Werte in den ONTAP System Manager eingeben können. Mit dem Assistenten konfigurieren Sie Ihr System schneller und stellen sicher, dass Ihre Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.

Wenn Sie über die Berechtigung für den Stammzugriff verfügen, können Sie den FabricPool-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID-Grid-Manager verwenden, oder Sie können den Assistenten zu einem späteren Zeitpunkt aufrufen und abschließen. Je nach Ihren Anforderungen können Sie auch einige oder alle erforderlichen Elemente manuell konfigurieren und dann mithilfe des Assistenten die von ONTAP benötigten Werte in einer einzigen Datei zusammenfügen.



Verwenden Sie den FabricPool Setup-Assistenten, es sei denn, Sie wissen, dass Sie besondere Anforderungen haben oder dass Ihre Implementierung umfangreiche Anpassungen erfordern wird.

Bevor Sie den Assistenten verwenden

Bestätigen Sie, dass Sie die erforderlichen Schritte abgeschlossen haben.

Besprechen der Best Practices

- Sie haben ein allgemeines Verständnis der "[Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier](#)".
- Sie haben die FabricPool Best Practices für folgende Zwecke überprüft:
 - "[Hochverfügbarkeitsgruppen \(High Availability groups, HA-Gruppen\)](#)"
 - "[Lastverteilung](#)"
 - "[ILM-Regeln und -Richtlinie](#)"

Beziehen Sie IP-Adressen, und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine HA-Gruppe konfigurieren, wissen Sie, mit welchen Nodes ONTAP eine Verbindung herstellen und welches StorageGRID-Netzwerk verwendet werden soll. Sie wissen auch, welche Werte für das Subnetz CIDR, die Gateway-IP-Adresse und die virtuelle IP (VIP)-Adresse eingegeben werden sollen.

Wenn Sie planen, einen virtuellen LAN zur Trennung des FabricPool-Datenverkehrs zu verwenden, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)".

Konfigurieren Sie Identity Federation und SSO

Wenn Sie planen, Identity Federation oder Single Sign-On (SSO) für Ihr StorageGRID-System zu verwenden, haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff für das Mandantenkonto haben soll, das ONTAP verwenden wird. Siehe "[Verwenden Sie den Identitätsverbund](#)" Und "[Konfigurieren Sie Single Sign-On](#)".

Abrufen und Konfigurieren von Domännennamen

- Sie wissen, welcher vollständig qualifizierte Domänenname (FQDN) für StorageGRID verwendet werden soll. DNS-Einträge (Domain Name Server) weisen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen. Siehe "[Konfigurieren Sie den DNS-Server](#)".
- Wenn Sie Anforderungen im virtuellen Hosted-Style von S3 verwenden möchten, haben Sie die Möglichkeit "[Domännennamen des S3-Endpunkts wurden konfiguriert](#)". ONTAP verwendet standardmäßig URLs im Pfadstil, es wird jedoch empfohlen, Anforderungen im virtuellen Hosted-Stil zu verwenden.

Anforderungen für Load Balancer und Sicherheitszertifikate prüfen

Wenn Sie den StorageGRID Load Balancer verwenden möchten, haben Sie die allgemeinen Informationen gelesen "[Überlegungen zum Lastausgleich](#)". Sie verfügen über die hochgeladenen Zertifikate oder die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn Sie einen externen (Drittanbieter-)Load Balancer-Endpunkt verwenden möchten, verfügen Sie über den vollständig qualifizierten Domännennamen (FQDN), den Port und das Zertifikat für diesen Load Balancer.

Bestätigen Sie die ILM-Speicherpoolkonfiguration

Wenn Sie von einer früheren StorageGRID-Version auf StorageGRID 11.7 aktualisiert haben, haben Sie den zu verwendenden Speicherpool konfiguriert. Im Allgemeinen sollten Sie für jeden StorageGRID-Standort, den Sie zum Speichern von ONTAP-Daten verwenden, einen Speicherpool erstellen.



Diese Voraussetzung gilt nicht für neue StorageGRID 11.7-Installationen. Wenn Sie StorageGRID 11.7 in einem neuen Grid installieren, werden für jeden Standort automatisch Speicherpools erstellt.

Beziehung zwischen ONTAP und StorageGRID Cloud-Tier

Der FabricPool Assistent führt Sie durch die Erstellung einer einzelnen StorageGRID-Cloud-Tier mit einem StorageGRID-Mandanten, einem Satz an Zugriffsschlüsseln und einem StorageGRID-Bucket. Sie können diese StorageGRID-Cloud-Tier an eine oder mehrere lokale ONTAP-Tiers anbinden.

Die allgemeine Best Practice ist die Anbindung einer einzelnen Cloud-Tier an mehrere lokale Tiers in einem Cluster. Je nach Anforderungen sollten Sie jedoch möglicherweise mehr als einen Bucket oder sogar mehr als einen StorageGRID-Mandanten für die lokalen Tiers in einem einzelnen Cluster verwenden. Die Verwendung verschiedener Buckets und Mandanten ermöglicht die Isolierung von Daten und Datenzugriff zwischen lokalen ONTAP Tiers, allerdings ist die Konfiguration und das Management etwas komplexer.

NetApp empfiehlt, keine einzelne Cloud-Tier an lokale Tiers in mehreren Clustern anzubinden.



Best Practices für die Verwendung von StorageGRID mit NetApp MetroCluster™ und FabricPool Mirror finden Sie unter "[TR-4598: FabricPool Best Practices in ONTAP](#)".

Optional: Verwenden Sie einen anderen Bucket für jeden lokalen Tier

Wenn Sie mehr als einen Bucket für die lokalen Tiers in einem ONTAP-Cluster verwenden möchten, fügen Sie mehr als eine StorageGRID-Cloud-Tier in ONTAP hinzu. Jede Cloud-Tier verwendet dieselbe HA-Gruppe, denselben Load-Balancer-Endpunkt, dieselben Mandanten und Zugriffsschlüssel, verwendet jedoch einen anderen Container (StorageGRID Bucket). Führen Sie die folgenden allgemeinen Schritte aus:

1. Vervollständigen Sie über den StorageGRID Grid Manager den FabricPool-Einrichtungsassistenten für die erste Cloud-Tier.
2. Fügen Sie im ONTAP System Manager eine Cloud-Ebene hinzu und verwenden Sie die von StorageGRID heruntergeladene Datei, um die erforderlichen Werte bereitzustellen.
3. Melden Sie sich über den StorageGRID-Mandantenmanager bei dem Mandanten an, der vom Assistenten erstellt wurde, und erstellen Sie einen zweiten Bucket.
4. Schließen Sie den FabricPool-Assistenten erneut ab. Wählen Sie die vorhandene HA-Gruppe, den Load-Balancer-Endpunkt und den Mandanten aus. Wählen Sie dann den neuen Bucket aus, den Sie manuell erstellt haben. Erstellen einer neuen ILM-Regel für den neuen Bucket und Aktivieren einer ILM-Richtlinie, um diese Regel aufzunehmen
5. Fügen Sie in ONTAP eine zweite Cloud-Tier hinzu, geben Sie aber den neuen Bucket-Namen an.

Optional: Verwenden Sie einen anderen Mandanten und Bucket für jede lokale Tier

Wenn Sie mehr als einen Mandanten und unterschiedliche Zugriffssätze für die lokalen Tiers in einem ONTAP-Cluster verwenden möchten, fügen Sie mehr als ein StorageGRID-Cloud-Tier in ONTAP hinzu. Jede Cloud-Tier verwendet dieselbe HA-Gruppe und denselben Load-Balancer-Endpunkt, verwendet jedoch einen anderen Mandanten, Zugriffsschlüssel und Container (StorageGRID Bucket). Führen Sie die folgenden allgemeinen Schritte aus:

1. Vervollständigen Sie über den StorageGRID Grid Manager den FabricPool-Einrichtungsassistenten für die erste Cloud-Tier.
2. Fügen Sie im ONTAP System Manager eine Cloud-Ebene hinzu und verwenden Sie die von StorageGRID heruntergeladene Datei, um die erforderlichen Werte bereitzustellen.
3. Schließen Sie den FabricPool-Assistenten erneut ab. Wählen Sie die vorhandene HA-Gruppe und den Endpunkt des Load Balancer aus. Erstellen eines neuen Mandanten und Buckets Erstellen einer neuen ILM-Regel für den neuen Bucket und Aktivieren einer ILM-Richtlinie, um diese Regel aufzunehmen
4. Von ONTAP fügen Sie eine zweite Cloud-Tier hinzu, liefern aber den neuen Zugriffsschlüssel, den geheimen Schlüssel und den Bucket-Namen.

Öffnen und Abschließen des FabricPool Setup-Assistenten

Mit dem FabricPool-Einrichtungsassistenten können Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier konfigurieren.

Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen](#)" Zur Verwendung des FabricPool Setup-Assistenten.



Wenn Sie StorageGRID für die Verwendung mit einer anderen S3-Client-Anwendung konfigurieren möchten, gehen Sie zu "[Verwenden Sie den S3-Einrichtungsassistenten](#)".

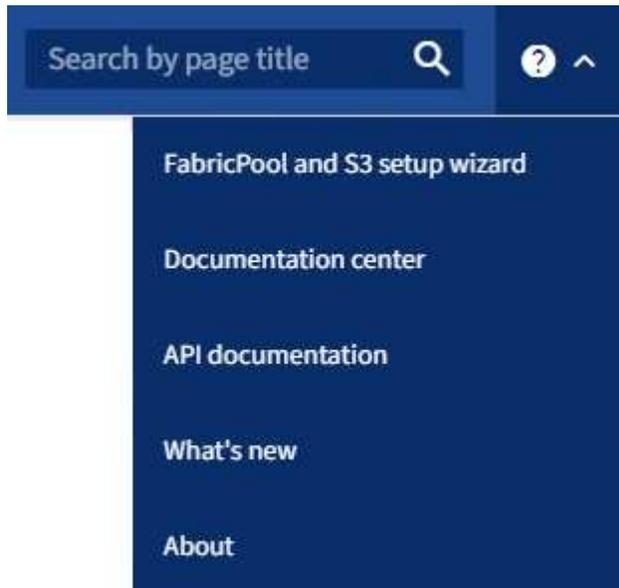
- Sie haben die Root-Zugriffsberechtigung.

Greifen Sie auf den Assistenten zu

Sie können den FabricPool-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID Grid-Manager verwenden, oder Sie können den Assistenten zu einem späteren Zeitpunkt aufrufen und abschließen.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an "[Unterstützter Webbrowser](#)".
2. Wenn das Banner **FabricPool and S3 Setup Wizard** auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie in der Kopfzeile des Grid-Managers das Hilfesymbol aus und wählen Sie **FabricPool und S3-Setup-Assistent** aus.



3. Wählen Sie im Abschnitt FabricPool der Seite mit dem FabricPool- und S3-Setup-Assistenten **Jetzt konfigurieren** aus.

Schritt 1 von 9: Konfigurieren der HA-Gruppe wird angezeigt.

Schritt 1 von 9: Konfigurieren Sie die HA-Gruppe

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um FabricPool-Datenverbindungen verfügbar zu halten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Service zu ermöglichen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den FabricPool-Betrieb managen

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Management von Hochverfügbarkeitsgruppen](#)" Und "[Best Practices für Hochverfügbarkeitsgruppen](#)".

Schritte

1. Wenn Sie einen externen Load Balancer verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **diesen Schritt überspringen** und gehen Sie zu [Schritt 2 von 9: Konfigurieren Sie den Load Balancer-Endpunkt](#).
2. Um den StorageGRID Load Balancer zu verwenden, erstellen Sie eine neue HA-Gruppe oder verwenden

Sie eine vorhandene HA-Gruppe.

Erstellen Sie eine HA-Gruppe

- a. Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.
- b. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

Feld	Beschreibung
Name DER HA-Gruppe	Ein eindeutiger Anzeigename für diese HA-Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

- c. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

- d. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

Ziehen Sie Zeilen, um die Werte in der Spalte **Priority order** zu ändern.

Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Ausfälle behoben werden, werden die VIP-Adressen wieder auf die Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist.

- e. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR Notation—eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: 192.16.0.0/22.
Gateway-IP-Adresse (optional)	Optional Wenn sich die ONTAP-IP-Adressen, die für den Zugriff auf StorageGRID verwendet werden, nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die IP-Adresse des lokalen StorageGRID-VIP-Gateways ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden, und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein. Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

f. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**, um zum FabricPool-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Verwenden Sie die vorhandene HA-Gruppe

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus der Dropdown-Liste **Select an HA Group** aus.

b. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Schritt 2 von 9: Konfigurieren Sie den Load Balancer-Endpunkt

StorageGRID verwendet einen Load Balancer zum Managen des Workloads von Client-Applikationen wie FabricPool. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Sie können den StorageGRID Load Balancer-Dienst verwenden, der auf allen Gateway- und Admin-Nodes vorhanden ist, oder eine Verbindung zu einem externen Load Balancer (Drittanbieter) herstellen. Die Verwendung des StorageGRID Load Balancer wird empfohlen.

Weitere Informationen zu dieser Aufgabe finden Sie im Abschnitt Allgemein "[Überlegungen zum Lastausgleich](#)" Und das "[Best Practices für Lastausgleich für FabricPool](#)".

Schritte

1. Wählen oder erstellen Sie einen StorageGRID Load Balancer-Endpunkt oder verwenden Sie einen externen Load Balancer.

Endpoint erstellen

- a. Wählen Sie **Endpoint erstellen**.
- b. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpoint.
Port	<p>Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpoint standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpoint nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind.</p> <p>Hinweis: von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe "Referenz für Netzwerk-Ports".</p>
Client-Typ	Muss S3 sein.
Netzwerkprotokoll	<p>Wählen Sie HTTPS.</p> <p>Hinweis: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.</p>

- c. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpoint zugegriffen wird—Verwendung einer beliebigen IP-Adresse oder Verwendung bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	<p>Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpoint zugreifen.</p> <p>Verwenden Sie die Global-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.</p>
Virtuelle IPs von HA-Gruppen	<p>Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpoint zuzugreifen.</p> <p>Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.</p>

Option	Beschreibung
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

d. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	<p>Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.</p> <p>Alle Mandanten zulassen ist fast immer die geeignete Option für den für FabricPool verwendeten Load Balancer Endpunkt.</p> <p>Sie müssen diese Option auswählen, wenn Sie den FabricPool-Einrichtungsassistenten für ein neues StorageGRID-System verwenden und noch keine Mandantenkonten erstellt haben.</p>
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

e. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Siehe " Konfigurieren von Load Balancer-Endpunkten " Für Details, was eingegeben werden soll.
StorageGRID S3 und Swift-Zertifikat verwenden	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Siehe " Konfigurieren von S3- und Swift-API-Zertifikaten " Entsprechende Details.

f. Wählen Sie **Fertig**, um zum FabricPool-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Verwenden Sie den vorhandenen Endpunkt des Load Balancer

a. Wählen Sie den Namen eines vorhandenen Endpunkts aus der Dropdown-Liste **Select a Load Balancer Endpoint** aus.

b. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Externen Load Balancer verwenden

a. Füllen Sie die folgenden Felder für den externen Load Balancer aus.

Feld	Beschreibung
FQDN	Der vollständig qualifizierte Domänenname (FQDN) des externen Load Balancer.
Port	Die Portnummer, die FabricPool zur Verbindung mit dem externen Load Balancer verwendet.
Zertifikat	Kopieren Sie das Serverzertifikat für den externen Load Balancer und fügen Sie es in dieses Feld ein.

b. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Schritt 3 von 9: Mieter und Eimer

Ein Mandant ist eine Einheit, die S3-Applikationen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und bestimmte Funktionen. Sie müssen einen StorageGRID-Mandanten erstellen, bevor Sie den Bucket erstellen können, den FabricPool verwenden wird.

Ein Bucket ist ein Container, mit dem die Objekte und Objektmetadaten eines Mandanten gespeichert werden können. Obwohl einige Mandanten möglicherweise über mehrere Buckets verfügen, können Sie mit dem Assistenten immer nur einen Mandanten und jeweils nur einen Bucket erstellen oder auswählen. Sie können den Tenant Manager später verwenden, um zusätzliche Buckets hinzuzufügen, die Sie benötigen.

Sie können einen neuen Mandanten und Bucket für die FabricPool-Verwendung erstellen oder einen vorhandenen Mandanten und Bucket auswählen. Wenn Sie einen neuen Mandanten erstellen, erstellt das System automatisch die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer des Mandanten.

Weitere Informationen zu dieser Aufgabe finden Sie unter ["Erstellen eines Mandantenkontos für FabricPool"](#) Und ["Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels"](#).

Schritte

Erstellen Sie einen neuen Mandanten und Bucket oder wählen Sie einen vorhandenen Mandanten aus.

Neuer Mandant und Bucket

1. Um einen neuen Mandanten und Bucket zu erstellen, geben Sie einen **Tenant Name** ein. Beispiel: `FabricPool tenant`.
2. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System verwendet "Identitätsföderation", "Single Sign On (SSO)" Oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	<ol style="list-style-type: none">a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten.b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

3. Geben Sie für **Bucket Name** den Namen des Buckets ein, den FabricPool zum Speichern von ONTAP-Daten verwendet. Beispiel: `fabricpool-bucket`.



Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

4. Wählen Sie die **Region** für diesen Bucket aus.

Verwenden Sie die Standardregion (US-East-1), es sei denn, Sie möchten ILM zukünftig verwenden, um Objekte basierend auf der Region des Buckets zu filtern.

5. Wählen Sie **Erstellen und Fortfahren**, um den Mandanten und den Bucket zu erstellen und zum Datenschnitt Download zu gehen

Wählen Sie Mandant und Bucket aus

Das vorhandene Mandantenkonto muss über mindestens einen Bucket verfügen, für den die Versionierung nicht aktiviert ist. Sie können kein vorhandenes Mandantenkonto auswählen, wenn für diesen Mandanten kein Bucket vorhanden ist.

1. Wählen Sie den vorhandenen Mandanten aus der Dropdown-Liste **Tenant Name** aus.
2. Wählen Sie den vorhandenen Bucket aus der Dropdown-Liste **Bucket Name** aus.

FabricPool unterstützt keine Objektversionierung, daher werden Buckets mit aktivierter Versionierung nicht angezeigt.



Wählen Sie keinen Bucket aus, für den die S3-Objektsperre zur Verwendung mit FabricPool aktiviert ist.

3. Wählen Sie **Weiter**, um zum Schritt Download-Daten zu gelangen.

Schritt 4 von 9: ONTAP-Einstellungen herunterladen

In diesem Schritt laden Sie eine Datei herunter, mit der Sie Werte in den ONTAP System Manager eingeben können.

Schritte

1. Wählen Sie optional das Kopieren-Symbol () Um sowohl die Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.

Diese Werte sind in der Download-Datei enthalten, sollten jedoch separat gespeichert werden.

2. Wählen Sie **ONTAP-Einstellungen herunterladen**, um eine Textdatei herunterzuladen, die die bisher eingegebenen Werte enthält.

Der `ONTAP_FabricPool_settings_bucketname.txt` Datei enthält die Informationen, die Sie benötigen, um StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Ebene zu konfigurieren, darunter:

- Verbindungsdetails des Load Balancer, einschließlich des Servernamens (FQDN), des Ports und des Zertifikats
 - Bucket-Name
 - Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel für den Root-Benutzer des Mandantenkontos
3. Speichern Sie die kopierten Schlüssel und die heruntergeladene Datei an einem sicheren Speicherort.



Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert, die ONTAP-Einstellungen heruntergeladen oder beides haben. Die Tasten sind nach dem Schließen dieser Seite nicht mehr verfügbar. Speichern Sie diese Informationen an einem sicheren Ort, da sie zum Abrufen von Daten von Ihrem StorageGRID-System verwendet werden können.

4. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter**, um zum ILM-Speicherpoolschritt zu gelangen.

Schritt 5 von 9: Wählen Sie einen Speicherpool aus

Ein Speicherpool ist eine Gruppe von Storage-Nodes. Wenn Sie einen Speicherpool auswählen, legen Sie fest, welche Nodes StorageGRID zum Speichern der von ONTAP gestaffelten Daten verwendet.

Weitere Informationen zu diesem Schritt finden Sie unter "[Erstellen Sie einen Speicherpool](#)".

Schritte

1. Wählen Sie aus der Drop-down-Liste **Standort** die StorageGRID-Site aus, die Sie für die Daten mit ONTAP-Tiering verwenden möchten.
2. Wählen Sie aus der Dropdown-Liste **Speicherpool** den Speicherpool für diesen Standort aus.

Der Speicherpool für einen Standort umfasst alle Storage-Nodes an diesem Standort.

3. Wählen Sie **Weiter**, um zum ILM-Regelschritt zu gelangen.

Schritt 6 von 9: Überprüfen Sie die ILM-Regel für FabricPool

Informationen Lifecycle Management-Regeln (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte im StorageGRID System.

Der FabricPool-Einrichtungsassistent erstellt automatisch die empfohlene ILM-Regel für die Verwendung mit FabricPool. Diese Regel gilt nur für den von Ihnen angegebenen Bucket. Dabei werden 2+1 Erasure Coding an einem einzigen Standort verwendet, um die aus ONTAP Tiering-Daten zu speichern.

Weitere Informationen zu diesem Schritt finden Sie unter ["ILM-Regel erstellen"](#) Und ["Best Practices für die Verwendung von ILM mit FabricPool-Daten"](#).

Schritte

1. Überprüfen Sie die Regeldetails.

Feld	Beschreibung
Regelname	Automatisch generiert und kann nicht geändert werden
Beschreibung	Automatisch generiert und kann nicht geändert werden
Filtern	Der Bucket-Name Diese Regel gilt nur für Objekte, die in dem von Ihnen angegebenen Bucket gespeichert wurden.
Referenzzeit	Aufnahmezeit Die Platzierungsanweisung beginnt, wenn Objekte zunächst im Bucket gespeichert werden.
Platzierungsanweisung	Verwenden Sie 2+1 Erasure Coding vom Tag 0 bis für immer

2. Sortieren Sie das Aufbewahrungsdiagramm nach **time period** und **Storage Pool**, um die Platzierungsanweisung zu bestätigen.
 - Der **Zeitraum** für die Regel ist **Tag 0 - für immer**. **Tag 0** bedeutet, dass die Regel angewendet wird, wenn Daten aus ONTAP verschoben werden. **Für immer** bedeutet, dass StorageGRID ILM keine Daten löscht, die aus ONTAP verschoben wurden.
 - Der **Speicherpool** für die Regel ist der von Ihnen ausgewählte Speicherpool. **EC 2+1** bedeutet, dass die Daten mit 2+1 Erasure Coding gespeichert werden. Jedes Objekt wird als zwei Datenfragmente und ein Paritätsfragment gespeichert. Die drei Fragmente für jedes Objekt werden in verschiedenen Storage Nodes an einem einzigen Standort gespeichert.
3. Wählen Sie **Erstellen und Fortfahren**, um diese Regel zu erstellen und zum ILM-Richtlinienschritt zu wechseln.

Schritt 7 von 9: Prüfen und aktivieren Sie die ILM-Richtlinie

Nachdem der FabricPool Setup-Assistent die ILM-Regel für die Verwendung von FabricPool erstellt hat, wird eine vorgeschlagene ILM-Richtlinie erstellt. Sie müssen diese Richtlinie sorgfältig prüfen, bevor Sie sie aktivieren.

Weitere Informationen zu diesem Schritt finden Sie unter ["ILM-Richtlinie erstellen"](#) Und ["Best Practices für die Verwendung von ILM mit FabricPool-Daten"](#).



Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese Richtlinie, um die Platzierung, Dauer und Datensicherung aller Objekte im Grid zu managen, einschließlich vorhandener und neu aufgenommenen Objekte. In einigen Fällen kann die Aktivierung einer neuen Richtlinie dazu führen, dass vorhandene Objekte an neue Speicherorte verschoben werden.



Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Setzen Sie die Aufbewahrungsfrist auf **Forever**, um sicherzustellen, dass FabricPool-Objekte nicht durch StorageGRID ILM gelöscht werden.

Schritte

1. Optional können Sie den vom System generierten **Richtliniennamen** aktualisieren. Standardmäßig hängt das System „+ FabricPool“ an den Namen Ihrer aktiven oder vorgeschlagenen Richtlinie an, Sie können jedoch Ihren eigenen Namen angeben.
2. Überprüfen Sie die Liste der Regeln in der vorgeschlagenen Richtlinie.
 - Wenn Ihr Raster keine vorgeschlagene ILM-Richtlinie enthält, erstellt der Assistent eine vorgeschlagene Richtlinie, indem Sie Ihre aktive Richtlinie klonen und die neue Regel oben hinzufügen.
 - Wenn Ihr Raster bereits über eine vorgeschlagene ILM-Richtlinie verfügt und diese Richtlinie dieselben Regeln und dieselbe Reihenfolge wie die aktive ILM-Richtlinie verwendet, fügt der Assistent die neue Regel oben auf der vorgeschlagenen Richtlinie hinzu.
 - Wenn Ihre vorgeschlagene Richtlinie andere Regeln oder eine andere Reihenfolge als die aktive Richtlinie enthält, wird eine Meldung angezeigt. Sie müssen die neue FabricPool-Regel manuell zur ILM-Richtlinie hinzufügen. Befolgen Sie diese Schritte, je nachdem, ob Sie von der aktiven Richtlinie oder der vorgeschlagenen Richtlinie beginnen möchten.

Richtlinie, die von beginnen soll	Schritte
Aktive Richtlinie	<ol style="list-style-type: none"> i. Wählen Sie im linken Menü im Grid Manager ILM > Policies aus. ii. Wählen Sie die Registerkarte vorgeschlagene Richtlinie aus. iii. Wählen Sie actions > Delete, um die vorhandene vorgeschlagene Richtlinie zu entfernen. iv. Kehren Sie zum FabricPool-Einrichtungsassistenten zurück. <p>Der Assistent kann jetzt Ihre aktive Richtlinie klonen, um eine neue vorgeschlagene Richtlinie zu erstellen. Die neue FabricPool-Regel wird oben hinzugefügt.</p>

Richtlinie, die von beginnen soll	Schritte
Vorgeschlagene Richtlinie	<ul style="list-style-type: none"> i. Wählen Sie im linken Menü im Grid Manager ILM > Policies aus. ii. Wählen Sie die Registerkarte vorgeschlagene Richtlinie aus. iii. Wählen Sie actions > Edit, um die vorhandene vorgeschlagene Richtlinie zu bearbeiten. iv. Fügen Sie die neue FabricPool-Regel oben hinzu. v. Aktivieren Sie die aktualisierte Richtlinie. vi. Wechseln Sie zum Verkehrsklassifizierung Schritt:

Siehe "[Vorgeschlagene ILM-Richtlinie erstellen](#)" Wenn Sie detailliertere Anweisungen benötigen.

3. Überprüfen Sie die Reihenfolge der Regeln in der neuen Richtlinie.

Da es sich bei der FabricPool-Regel um die erste Regel handelt, werden alle Objekte im FabricPool-Bucket vor die anderen Regeln in der Richtlinie platziert. Objekte in anderen Buckets werden durch nachfolgende Regeln in der Richtlinie platziert.

4. Sehen Sie sich das Aufbewahrungsdigramm an, um zu erfahren, wie verschiedene Objekte beibehalten werden.

- a. Wählen Sie **Expand all**, um ein Aufbewahrungsdigramm für jede Regel in der vorgeschlagenen Richtlinie anzuzeigen.
- b. Wählen Sie **time period** und **Storage Pool** aus, um das Aufbewahrungsdigramm zu überprüfen. Vergewissern Sie sich, dass alle Regeln, die auf den FabricPool-Bucket oder Mandanten zutreffen, Objekte **für immer** behalten.

5. Wenn Sie die vorgeschlagene Richtlinie überprüft haben, wählen Sie **Aktivieren und fortfahren**, um die Richtlinie zu aktivieren und zum Schritt Verkehrsklassifizierung zu wechseln.



Fehler in einer ILM-Richtlinie können zu irreparablen Datenverlusten führen. Überprüfen Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren.

Schritt 8 von 9: Verkehrsklassifizierungsrichtlinie erstellen

Optional kann der FabricPool-Einrichtungsassistent eine Richtlinie zur Verkehrsklassifizierung erstellen, die Sie zur Überwachung des FabricPool-Workloads verwenden können. Die vom System erstellte Richtlinie verwendet eine übereinstimmende Regel, um den gesamten Netzwerkverkehr in Bezug auf den erstellten Bucket zu identifizieren. Diese Richtlinie überwacht nur den Datenverkehr; sie beschränkt nicht den Datenverkehr für FabricPool oder andere Clients.

Weitere Informationen zu diesem Schritt finden Sie unter "[Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool](#)".

Schritte

1. Überprüfen Sie die Richtlinie.
2. Wenn Sie diese Verkehrsklassifizierungsrichtlinie erstellen möchten, wählen Sie **Erstellen und fortfahren**.

Sobald FabricPool mit dem Tiering von Daten in StorageGRID beginnt, können Sie auf der Seite „Richtlinien zur Traffic-Klassifizierung“ die Kennzahlen für den Netzwerk-Traffic für diese Richtlinie

anzeigen. Später können Sie auch Regeln hinzufügen, um andere Workloads einzuschränken und sicherzustellen, dass der FabricPool-Workload den größten Teil der Bandbreite hat.

3. Andernfalls wählen Sie **diesen Schritt überspringen**.

Schritt 9 von 9: Zusammenfassung überprüfen

Die Zusammenfassung enthält Details zu den von Ihnen konfigurierten Elementen, darunter den Namen des Load Balancer, Mandanten und Buckets, die Richtlinie zur Datenklassifizierung und die aktive ILM-Richtlinie.

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Wählen Sie **Fertig**.

Nächste Schritte

Führen Sie nach Abschluss des FabricPool-Assistenten die folgenden zusätzlichen Schritte aus.

Schritte

1. Gehen Sie zu ["Konfigurieren Sie ONTAP System Manager"](#) Um die gespeicherten Werte einzugeben und die ONTAP-Seite der Verbindung abzuschließen. Sie müssen StorageGRID als Cloud-Tier hinzufügen, die Cloud-Tier einer lokalen Tier zuweisen, um eine FabricPool zu erstellen, und Volume-Tiering-Richtlinien festlegen.
2. Gehen Sie zu ["Konfigurieren Sie den DNS-Server"](#) Und stellen Sie sicher, dass der DNS einen Datensatz enthält, um den StorageGRID-Servernamen (vollständig qualifizierter Domänenname) jeder verwendeten StorageGRID-IP-Adresse zuzuordnen.
3. Gehen Sie zu ["Weitere Best Practices für StorageGRID und FabricPool"](#) Um Best Practices für StorageGRID-Prüfprotokolle und andere globale Konfigurationsoptionen zu erfahren.

Konfigurieren Sie StorageGRID manuell

Erstellen einer HA-Gruppe (High Availability, Hochverfügbarkeit) für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, können Sie optional eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) erstellen. Eine HA-Gruppe ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um FabricPool-Datenverbindungen verfügbar zu halten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Service zu ermöglichen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den FabricPool-Betrieb managen.

Weitere Informationen zu dieser Aufgabe finden Sie unter ["Management von Hochverfügbarkeitsgruppen"](#). Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu ["Öffnen und Abschließen des FabricPool Setup-Assistenten"](#).

Bevor Sie beginnen

- Sie haben die geprüft ["Best Practices für Hochverfügbarkeitsgruppen ab"](#).
- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).

- Sie haben die Root-Zugriffsberechtigung.
- Wenn Sie ein VLAN verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)".

Schritte

1. Wählen Sie **CONFIGURATION > Network > High Availability groups**.
2. Wählen Sie **Erstellen**.
3. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

Feld	Beschreibung
Name DER HA-Gruppe	Ein eindeutiger Anzeigename für diese HA-Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

4. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

5. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

Ziehen Sie Zeilen, um die Werte in der Spalte **Priority order** zu ändern.

Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Ausfälle behoben werden, werden die VIP-Adressen wieder auf die Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist.

6. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR Notation—eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: 192.16.0.0/22.

Feld	Beschreibung
Gateway-IP-Adresse (optional)	Optional Wenn sich die ONTAP-IP-Adressen, die für den Zugriff auf StorageGRID verwendet werden, nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die IP-Adresse des lokalen StorageGRID-VIP-Gateways ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

7. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**.

Erstellen eines Load Balancer-Endpunkts für FabricPool

StorageGRID verwendet einen Load Balancer zum Managen des Workloads von Client-Applikationen wie FabricPool. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, müssen Sie einen Load Balancer-Endpunkt konfigurieren und ein Load Balancer-Endpunktzertifikat hochladen oder generieren, das zum Sichern der Verbindung zwischen ONTAP und StorageGRID verwendet wird.

Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu ["Öffnen und Abschließen des FabricPool Setup-Assistenten"](#).

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben den General überprüft ["Überlegungen zum Lastausgleich"](#) sowie dem ["Best Practices für Lastausgleich für FabricPool"](#).

Schritte

1. Wählen Sie **CONFIGURATION > Network > Load Balancer Endpunkte**.
2. Wählen Sie **Erstellen**.
3. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.

Feld	Beschreibung
Port	<p>Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert. Diese Ports sind für Admin-Nodes reserviert.</p> <p>Hinweis: von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe "Referenz für Netzwerk-Ports".</p> <p>Sie geben diese Nummer an ONTAP an, wenn Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen.</p>
Client-Typ	Wählen Sie S3 .
Netzwerkprotokoll	<p>Wählen Sie HTTPS.</p> <p>Hinweis: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.</p>

4. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt zugegriffen wird—Verwendung einer beliebigen IP-Adresse oder Verwendung bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	<p>Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen.</p> <p>Verwenden Sie die Global-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.</p>
Virtuelle IPs von HA-Gruppen	<p>Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen.</p> <p>Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.</p>
Node-Schnittstellen	<p>Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.</p>

Option	Beschreibung
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

5. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	<p>Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.</p> <p>Alle Mandanten zulassen ist fast immer die geeignete Option für den für FabricPool verwendeten Load Balancer Endpunkt.</p> <p>Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben.</p>
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

6. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Siehe " Konfigurieren von Load Balancer-Endpunkten " Für Details, was eingegeben werden soll.
StorageGRID S3 und Swift-Zertifikat verwenden	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Siehe " Konfigurieren von S3- und Swift-API-Zertifikaten " Entsprechende Details.

7. Wählen Sie **Erstellen**.



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Erstellen eines Mandantenkontos für FabricPool

Sie müssen ein Mandantenkonto im Grid Manager for FabricPool Use erstellen.

Mandantenkonten ermöglichen Client-Applikationen, Objekte auf StorageGRID zu speichern und abzurufen. Jedes Mandantenkonto verfügt über eine eigene Account-ID, autorisierte Gruppen und Benutzer, Buckets und Objekte.

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Erstellen eines Mandantenkontos](#)". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "[Öffnen und Abschließen des FabricPool Setup-Assistenten](#)".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen**.
3. Geben Sie für die Schritte zum Eingeben von Details die folgenden Informationen ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten.
Client-Typ	Muss S3 für FabricPool sein.
Storage-Kontingent (optional)	Lassen Sie dieses Feld für FabricPool leer.

4. Für den Schritt Berechtigungen auswählen:

- a. Wählen Sie nicht **Plattformdienste zulassen**.

FabricPool Mandanten benötigen in der Regel keine Plattform-Services, wie z. B. CloudMirror-Replizierung.

- b. Wählen Sie optional **eigene Identitätsquelle verwenden**.

- c. Wählen Sie nicht **S3 Select zulassen**.

FabricPool-Mandanten müssen in der Regel nicht S3 Select verwenden.

- d. Wählen Sie optional **Grid Federation Connection** verwenden, um dem Mandanten die Verwendung eines zu ermöglichen "[Netzverbundverbindung](#)" Für Account-Klonen und Grid-übergreifende Replizierung. Wählen Sie dann die zu verwendende Netzverbundverbindung aus.

5. Geben Sie für den Schritt Root-Zugriff definieren an, welcher Benutzer die anfängliche Root-Zugriffsberechtigung für das Mandantenkonto erhält, je nachdem, ob das StorageGRID-System verwendet

"Identitätsföderation", "Single Sign On (SSO)" Oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

6. Wählen Sie **Create Tenant**.

Erstellen eines S3-Buckets und Abrufen von Zugriffsschlüsseln

Bevor Sie StorageGRID mit einem FabricPool-Workload verwenden, müssen Sie einen S3-Bucket für Ihre FabricPool-Daten erstellen. Außerdem müssen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel für das Mandantenkonto erhalten, das Sie für FabricPool verwenden werden.

Weitere Informationen zu dieser Aufgabe finden Sie unter ["S3-Bucket erstellen"](#) Und ["Erstellen Ihrer eigenen S3-Zugriffsschlüssel"](#). Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu ["Öffnen und Abschließen des FabricPool Setup-Assistenten"](#).

Bevor Sie beginnen

- Sie haben ein Mandantenkonto für die Nutzung von FabricPool erstellt.
- Sie haben Root-Zugriff auf das Mandantenkonto.

Schritte

1. Melden Sie sich beim Tenant Manager an.

Sie können eine der folgenden Aktionen ausführen:

- Wählen Sie auf der Seite Mandantenkonten im Grid Manager den Link **Anmelden** für den Mieter aus, und geben Sie Ihre Anmeldedaten ein.
- Geben Sie die URL für das Mandantenkonto in einem Webbrowser ein, und geben Sie Ihre Anmeldedaten ein.

2. Erstellung eines S3-Buckets für FabricPool-Daten

Sie müssen für jedes zu verwendende ONTAP Cluster einen eindeutigen Bucket erstellen.

- Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
- Wählen Sie **Eimer erstellen**.
- Geben Sie den Namen des StorageGRID-Buckets ein, den Sie mit FabricPool verwenden möchten.

Beispiel: `fabricpool-bucket`.



Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

d. Wählen Sie die Region für diesen Bucket aus.

Standardmäßig werden alle Buckets im erstellt `us-east-1` Werden.

e. Wählen Sie **Weiter**.

f. Wählen Sie **Eimer erstellen**.



Wählen Sie nicht **enable object Versioning** für den FabricPool Bucket aus. Bearbeiten Sie einen FabricPool-Bucket nicht, um **verfügbar** oder einen nicht standardmäßigen Konsistenzlevel zu verwenden. Die empfohlene Bucket-Konsistenzstufe für FabricPool Buckets ist **Read-after-New-write**, was die Standardeinstellung für einen neuen Bucket ist.

3. Erstellen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel.

a. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.

b. Wählen Sie **Schlüssel erstellen**.

c. Wählen Sie **Zugriffsschlüssel erstellen**.

d. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.

Sie geben diese Werte in ONTAP ein, wenn Sie StorageGRID als FabricPool Cloud-Tier konfigurieren.



Wenn Sie in Zukunft in StorageGRID einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls könnte ONTAP vorübergehend seinen Zugriff auf StorageGRID verlieren.

Konfigurieren Sie ILM für FabricPool-Daten

Sie können diese einfache Beispielrichtlinie als Ausgangspunkt für Ihre eigenen ILM-Regeln und -Richtlinien verwenden.

Das Beispiel geht davon aus, dass Sie die ILM-Regeln und eine ILM-Richtlinie für ein StorageGRID System mit vier Storage-Nodes in einem einzelnen Datacenter in Denver, Colorado, entwerfen. Die FabricPool-Daten in diesem Beispiel verwenden einen Bucket mit dem Namen `fabricpool-bucket`.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen. Weitere Informationen finden Sie unter ["Objektmanagement mit ILM"](#).



Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Setzen Sie die Aufbewahrungsfrist auf **Forever**, um sicherzustellen, dass FabricPool-Objekte nicht durch StorageGRID ILM gelöscht werden.

Bevor Sie beginnen

- Sie haben die geprüft "[Best Practices für die Verwendung von ILM mit FabricPool-Daten](#)".
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Berechtigung für den ILM- oder Root-Zugriff.
- Wenn Sie von einer früheren StorageGRID-Version auf StorageGRID 11.7 aktualisiert haben, haben Sie den zu verwendenden Speicherpool konfiguriert. Im Allgemeinen sollten Sie für jeden StorageGRID-Standort einen Speicherpool erstellen.



Diese Voraussetzung gilt nicht für neue StorageGRID 11.7-Installationen. Wenn Sie StorageGRID 11.7 in einem neuen Grid installieren, werden für jeden Standort automatisch Speicherpools erstellt.

Schritte

1. Erstellen einer ILM-Regel, die sich nur auf die Daten in bezieht `fabricpool-bucket`. In dieser Beispielregel werden Kopien mit Verfahren zur Fehlerkorrektur erstellt.

Regeldefinition	Beispielwert
Regelname	2 + 1 Erasure Coding für FabricPool-Daten
Bucket-Name	<code>fabricpool-bucket</code> Sie könnten auch nach dem FabricPool-Mandantenkonto filtern.
Erweiterte Filter	Objektgröße größer als 0.2 MB. Hinweis: FabricPool schreibt nur 4 MB Objekte, aber Sie müssen einen Objektgrößenfilter hinzufügen, da diese Regel Erasure Coding verwendet.
Referenzzeit	Aufnahmezeit
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte durch Erasure Coding mit dem 2+1-EC-Schema in Denver und bewahren Sie diese Objekte für immer in StorageGRID auf.  Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht.
Aufnahmeverhalten	Ausgeglichen

- Erstellen Sie eine standardmäßige ILM-Regel, die zwei replizierte Kopien von Objekten erstellt, die der ersten Regel nicht zugeordnet sind. Wählen Sie keinen einfachen Filter (Mandantenkonto oder Bucket-Name) oder keine erweiterten Filter aus.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Bucket-Name	<i>None</i>
Erweiterte Filter	<i>None</i>
Referenzzeit	Aufnahmezeit
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte, indem Sie 2 Kopien in Denver replizieren.
Aufnahmeverhalten	Ausgeglichen

- Erstellen Sie eine vorgeschlagene ILM-Richtlinie und wählen Sie beide Regeln aus. Da die Replikationsregel keine Filter verwendet, kann es sich um die Standardregel (letzte) für die Richtlinie handeln.
- Aufnahme von Testobjekten in das Raster
- Simulieren Sie die Richtlinie mit den Testobjekten, um das Verhalten zu überprüfen.
- Aktivieren Sie die Richtlinie.

Wenn diese Richtlinie aktiviert ist, speichert StorageGRID Objektdaten wie folgt:

- Die Daten-Tiering von FabricPool in `fabricpool-bucket` Wird mithilfe des 2+1-Schemas zur Einhaltung von Datenkonsistenz (Erasure Coding) codiert. Zwei Datenfragmente und ein Paritätsfragment werden auf drei verschiedenen Storage Nodes platziert.
- Alle Objekte in allen anderen Buckets werden repliziert. Es werden zwei Kopien erstellt und auf zwei verschiedenen Speicherknoten platziert.
- Die Kopien werden für immer in StorageGRID aufbewahrt. StorageGRID ILM wird diese Objekte nicht löschen.

Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool

Optional können Sie eine StorageGRID Traffic-Klassifizierungsrichtlinie entwerfen, um die Servicequalität für den FabricPool-Workload zu optimieren.

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Verwalten von Richtlinien zur Verkehrsklassifizierung](#)". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "[Öffnen und Abschließen des FabricPool Setup-Assistenten](#)".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Die Best Practices für das Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool hängen vom Workload ab:

- Bei der Planung, primäre FabricPool Workload-Daten auf StorageGRID zu verschieben, sollte sichergestellt werden, dass der FabricPool-Workload den größten Teil der Bandbreite hat. Sie können eine Traffic-Klassifizierungsrichtlinie erstellen, um alle anderen Workloads einzuschränken.



Im Allgemeinen sind FabricPool-Lesevorgänge wichtiger als Schreibvorgänge.

Wenn beispielsweise andere S3-Clients dieses StorageGRID-System verwenden, sollten Sie eine Traffic-Klassifizierungsrichtlinie erstellen. Der Netzwerk-Traffic kann für die anderen Buckets, Mandanten, IP-Subnetze oder Load Balancer Endpunkte begrenzt werden.

*Im Allgemeinen sollten Sie keine Quality of Service-Limits für FabricPool-Workloads einführen; Sie sollten nur die anderen Workloads begrenzen.

- Die Einschränkungen, die für andere Workloads gelten, sollten das Verhalten dieser Workloads berücksichtigen. Die auferlegten Einschränkungen hängen auch von der Größe und den Funktionen des Grids und der erwarteten Auslastung ab.

Schritte

1. Wählen Sie **CONFIGURATION > Network > traffic classification**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung (optional) für die Richtlinie ein und wählen Sie **Weiter**.
4. Fügen Sie für den Schritt übereinstimmende Regeln hinzufügen mindestens eine Regel hinzu.
 - a. Wählen Sie **Regel hinzufügen**
 - b. Wählen Sie unter Typ * Load Balancer Endpunkt* aus, und wählen Sie den Load Balancer Endpunkt aus, den Sie für FabricPool erstellt haben.

Sie können auch das FabricPool-Mandantenkonto oder den Bucket auswählen.
 - c. Wenn diese Datenverkehrsrichtlinie den Datenverkehr für die anderen Endpunkte einschränken soll, wählen Sie **inverse Übereinstimmung**.
5. Fügen Sie optional eine oder mehrere Grenzwerte hinzu, um den Netzwerkverkehr zu steuern, der der Regel entspricht.



StorageGRID sammelt Kennzahlen, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends besser verstehen können.

- a. Wählen Sie **Limit hinzufügen**.
 - b. Wählen Sie den zu begrenzenden Verkehrstyp und die anzuwählenden Grenzwerte aus.
6. Wählen Sie **Weiter**.
 7. Lesen und prüfen Sie die Richtlinie zur Verkehrsklassifizierung. Verwenden Sie die Schaltfläche * Zurück*, um zurückzugehen und Änderungen vorzunehmen. Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie **Speichern und fortfahren**.

Nach dem Ende

"[Zeigen Sie Metriken zum Netzwerkverkehr an](#)" Um zu überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Konfigurieren Sie ONTAP System Manager

Nachdem Sie die erforderlichen StorageGRID Informationen erhalten haben, können Sie auf ONTAP StorageGRID als Cloud-Tier hinzufügen.

Bevor Sie beginnen

- Wenn Sie den FabricPool-Setup-Assistenten abgeschlossen haben, steht Ihnen der zur Verfügung `ONTAP_FabricPool_settings_bucketname.txt` Heruntergeladene Datei.
- Wenn Sie StorageGRID manuell konfiguriert haben, verfügen Sie über den vollständig qualifizierten Domännennamen (FQDN), den Sie für StorageGRID verwenden, oder über die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe, die Portnummer für den Endpunkt des Load Balancer, das Load Balancer-Zertifikat, Die Zugriffsschlüssel-ID und der geheime Schlüssel für den Root-Benutzer des Mandantenkontos sowie den Namen des Bucket-ONTAP, die in diesem Mandanten verwendet werden.

Zugriff auf ONTAP System Manager

In diesen Anweisungen wird beschrieben, wie Sie StorageGRID mit ONTAP System Manager als Cloud-Tier hinzufügen. Sie können dieselbe Konfiguration mithilfe der ONTAP CLI abschließen. Weitere Anweisungen finden Sie unter "[ONTAP 9: FabricPool-Tier-Management mit CLI](#)".

Schritte

1. Greifen Sie auf System Manager für den ONTAP-Cluster zu, den Sie auf StorageGRID Tiering möchten.
2. Melden Sie sich als Administrator für das Cluster an.
3. Navigieren Sie zu **STORAGE > Tiers > Add Cloud Tier**.
4. Wählen Sie **StorageGRID** aus der Liste der Objektspeicher-Anbieter aus.

Geben Sie StorageGRID-Werte ein

Siehe "[ONTAP 9: FabricPool Tier-Management-Überblick mit System Manager](#)" Finden Sie weitere Informationen.

Schritte

1. Füllen Sie das Formular „Cloud-Tiering hinzufügen“ mit der aus `ONTAP_FabricPool_settings_bucketname.txt` Datei oder die Werte, die Sie manuell erhalten haben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für diese Cloud-Tier ein. Sie können den Standardwert übernehmen.

Feld	Beschreibung
URL-Stil	<p>Wenn Sie "Domännennamen des S3-Endpunkts wurden konfiguriert" Wählen Sie Virtual Hosted-Style URL.</p> <p>Pfad-Stil-URL ist der Standard für ONTAP, aber die Verwendung von virtuellen Hosted-Stil-Anforderungen wird für StorageGRID empfohlen. Sie müssen Pfad-Stil-URL verwenden, wenn Sie eine IP-Adresse anstelle eines Domännennamens für das Feld Servername (FQDN) angeben.</p>
Servername (FQDN)	<p>Geben Sie den vollständig qualifizierten Domännennamen (FQDN) ein, den Sie für StorageGRID verwenden, oder die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe. Beispiel: <code>s3.storagegrid.company.com</code>.</p> <p>Beachten Sie Folgendes:</p> <ul style="list-style-type: none"> • Die hier angegebene IP-Adresse oder der Domänenname muss mit dem Zertifikat übereinstimmen, das Sie für den StorageGRID-Load-Balancer-Endpunkt hochgeladen oder generiert haben. • Wenn Sie einen Domännennamen angeben, muss der DNS-Eintrag jeder IP-Adresse zugeordnet werden, die Sie zur Verbindung mit StorageGRID verwenden. Siehe "Konfigurieren Sie den DNS-Server".
SSL	Aktiviert (Standard).
Objektspeicherzertifikat	<p>Fügen Sie das Zertifikat-PEM ein, das Sie für den StorageGRID Load Balancer-Endpunkt verwenden, einschließlich: -----BEGIN CERTIFICATE----- Und -----END CERTIFICATE-----.</p> <p>Hinweis: Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zwischenzertifikat vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.</p>
Port	Geben Sie den vom Endpunkt des StorageGRID Load Balancer verwendeten Port ein. ONTAP wird diesen Port verwenden, wenn es eine Verbindung zu StorageGRID herstellt. Beispiel: 10433.
Zugriffsschlüssel und geheimer Schlüssel	<p>Geben Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer des StorageGRID-Mandantenkontos ein.</p> <p>Tipp: Wenn Sie in Zukunft einen neuen Zugriffsschlüssel und geheimen Zugriffsschlüssel in StorageGRID generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls könnte ONTAP vorübergehend seinen Zugriff auf StorageGRID verlieren.</p>
Containername	Geben Sie den Namen des StorageGRID-Buckets ein, den Sie für die Verwendung mit diesem ONTAP-Tier erstellt haben.

2. Schließen Sie die endgültige FabricPool-Konfiguration in ONTAP ab.
 - a. Fügen Sie ein oder mehrere Aggregate zur Cloud-Tier hinzu.
 - b. Optional können Sie eine Tiering Policy für Volumes erstellen.

Konfigurieren Sie den DNS-Server

Nach der Konfiguration von Hochverfügbarkeitsgruppen, Load Balancer-Endpunkten und S3-Endpunkt-Domännennamen müssen Sie sicherstellen, dass der DNS die erforderlichen Einträge für StorageGRID enthält. Sie müssen einen DNS-Eintrag für jeden Namen im Sicherheitszertifikat und für jede IP-Adresse angeben, die Sie verwenden können.

Siehe "[Überlegungen zum Lastausgleich](#)".

DNS-Einträge für den StorageGRID-Servernamen

Fügen Sie DNS-Einträge hinzu, um den Namen des StorageGRID-Servers (vollständig qualifizierter Domänenname) jeder verwendeten StorageGRID-IP-Adresse zuzuordnen. Die im DNS eingegebenen IP-Adressen hängen davon ab, ob Sie eine HA-Gruppe der Load-Balancing-Nodes verwenden:

- Wenn Sie eine HA-Gruppe konfiguriert haben, stellt ONTAP eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, kann sich ONTAP mithilfe der IP-Adresse eines beliebigen Gateway-Node oder Admin-Node mit dem StorageGRID Load Balancer-Service verbinden.
- Wenn der Servername auf mehr als eine IP-Adresse aufgelöst wird, baut ONTAP Client-Verbindungen mit allen IP-Adressen auf (bis zu maximal 16 IP-Adressen). Die IP-Adressen werden bei Verbindungsaufbau in einer Round-Robin-Methode erfasst.

DNS-Einträge für Anforderungen im virtuellen Hosted-Stil

Wenn Sie definiert haben "[Domännennamen des S3-Endpunkts](#)" Außerdem verwenden Sie Anfragen im virtuellen Hosted-Stil und fügen DNS-Einträge für alle erforderlichen S3-Endpunkt-Domännennamen hinzu, einschließlich aller Platzhalternamen.

StorageGRID Best Practices für FabricPool

Best Practices für Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen)

Bevor Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen, erfahren Sie mehr über StorageGRID HA-Gruppen (High Availability, Hochverfügbarkeit) und lesen Sie die Best Practices zur Verwendung von HA-Gruppen mit FabricPool durch.

Was ist eine HA-Gruppe?

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist eine Sammlung von Schnittstellen aus mehreren StorageGRID Gateway-Nodes, Admin-Nodes oder beidem. Eine HA-Gruppe hilft, Client-Datenverbindungen verfügbar zu halten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringer Auswirkung auf die FabricPool-Vorgänge managen.

Jede HA-Gruppe ermöglicht einen hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes. Beispielsweise bietet eine HA-Gruppe, die aus Schnittstellen nur auf Gateway-Nodes oder sowohl Admin-Nodes als auch Gateway-Nodes besteht, einen hochverfügbaren Zugriff auf den Shared Load Balancer

Service.

Weitere Informationen zu Hochverfügbarkeitsgruppen finden Sie unter "[Managen Sie Hochverfügbarkeitsgruppen \(High Availability Groups, HA-Gruppen\)](#)".

Verwenden von HA-Gruppen

Die Best Practices für die Erstellung einer StorageGRID HA-Gruppe für FabricPool hängen von den Workloads ab.

- Wenn Sie FabricPool für primäre Workload-Daten verwenden möchten, müssen Sie eine HA-Gruppe erstellen, die mindestens zwei Nodes für Lastausgleich enthält, um eine Unterbrechung des Datenabrufs zu verhindern.
- Wenn Sie eine FabricPool Richtlinie für das reine Volume-Tiering nur für Snapshots oder nicht für lokale Performance-Tiers (z. B. Disaster Recovery-Standorte oder NetApp SnapMirror Ziele) verwenden möchten, können Sie eine HA-Gruppe mit nur einem Node konfigurieren.

Diese Anweisungen beschreiben die Einrichtung einer HA-Gruppe für Active-Backup HA (ein Node ist aktiv und ein Node ist ein Backup). Möglicherweise verwenden Sie jedoch lieber DNS Round Robin oder Active-Active HA. Informationen zu den Vorteilen dieser anderen HA-Konfigurationen finden Sie unter "[Konfigurationsoptionen für HA-Gruppen](#)".

Best Practices für Lastausgleich für FabricPool

Bevor Sie StorageGRID als FabricPool-Cloud-Tier einbinden, sollten Sie sich die Best Practices für die Verwendung von Load Balancern mit FabricPool ansehen.

Allgemeine Informationen zum StorageGRID Load Balancer und zum Load Balancer-Zertifikat finden Sie unter "[Überlegungen zum Lastausgleich](#)".

Best Practices für den Mandantenzugriff auf den für FabricPool verwendeten Load Balancer-Endpunkt

Sie können steuern, welche Mandanten einen bestimmten Load Balancer-Endpunkt für den Zugriff auf ihre Buckets verwenden können. Sie können alle Mandanten erlauben, einige Mandanten zulassen oder einige Mandanten blockieren. Wenn Sie einen Endpunkt für die Lastverteilung für die FabricPool-Nutzung erstellen, wählen Sie **Alle Mandanten zulassen** aus. ONTAP verschlüsselt die in StorageGRID Buckets gespeicherten Daten, sodass diese zusätzliche Sicherheitsschicht nur wenig zusätzliche Sicherheit bietet.

Best Practices für das Sicherheitszertifikat

Wenn Sie einen StorageGRID Load Balancer-Endpunkt für die Verwendung mit FabricPool erstellen, geben Sie das Sicherheitszertifikat an, mit dem ONTAP sich mit StorageGRID authentifizieren kann.

In den meisten Fällen sollte bei der Verbindung zwischen ONTAP und StorageGRID die TLS-Verschlüsselung (Transport Layer Security) verwendet werden. Die Verwendung von FabricPool ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen. Wenn Sie das Netzwerkprotokoll für den Endpunkt des StorageGRID Load Balancer auswählen, wählen Sie **HTTPS** aus. Stellen Sie dann das Sicherheitszertifikat bereit, mit dem ONTAP sich mit StorageGRID authentifizieren kann.

Weitere Informationen zum Serverzertifikat für einen Lastausgleichsendpunkt:

- "[Verwalten von Sicherheitszertifikaten](#)"
- "[Überlegungen zum Lastausgleich](#)"

- ["Härtungsrichtlinien für Serverzertifikate"](#)

Zertifikat zu ONTAP hinzufügen

Wenn Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen, müssen Sie dasselbe Zertifikat auf dem ONTAP-Cluster installieren, einschließlich des Stammzertifikats und aller untergeordneten Zertifizierungsstellenzertifikate.

Managen Sie den Ablauf des Zertifikats



Wenn das Zertifikat zur Sicherung der Verbindung zwischen ONTAP und StorageGRID ausläuft, funktioniert FabricPool vorübergehend nicht mehr, und ONTAP verliert vorübergehend den Zugriff auf Daten, die auf StorageGRID-Daten verteilt sind.

Befolgen Sie die folgenden Best Practices, um Probleme mit dem Ablauf von Zertifikaten zu vermeiden:

- Überwachen Sie sorgfältig alle Warnungen, die darauf hinweisen, dass sich das Ablaufdatum des Zertifikats nähert, z. B. das Endpunktzertifikat **Ablauf des Load Balancer** und **Ablauf des globalen Serverzertifikats für S3- und Swift-API**-Warnungen.
- Halten Sie die StorageGRID- und ONTAP-Versionen des Zertifikats immer synchron. Wenn Sie das für einen Load Balancer-Endpoint verwendete Zertifikat ersetzen oder erneuern, müssen Sie das von ONTAP für die Cloud-Tier verwendete Zertifikat ersetzen oder erneuern.
- Ein öffentlich signiertes CA-Zertifikat verwenden. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie die Grid-Management-API verwenden, um die Zertifikatrotation zu automatisieren. So können Sie bald abgelaufene Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat generiert haben und dieses Zertifikat kurz vor dem Ablauf steht, müssen Sie das Zertifikat sowohl in StorageGRID als auch in ONTAP manuell ersetzen, bevor das vorhandene Zertifikat abläuft. Wenn ein selbstsigniertes Zertifikat bereits abgelaufen ist, deaktivieren Sie die Zertifikatvalidierung in ONTAP, um einen Zugriffsverlust zu verhindern.

Siehe ["NetApp Knowledge Base: So konfigurieren Sie ein neues selbstsigniertes StorageGRID Serverzertifikat für eine vorhandene ONTAP FabricPool Implementierung"](#) Weitere Anweisungen.

Best Practices für die Verwendung von ILM mit FabricPool-Daten

Wenn Sie FabricPool für das Tiering von Daten für StorageGRID verwenden, müssen Sie die Anforderungen für die Verwendung von StorageGRID Information Lifecycle Management (ILM) mit FabricPool-Daten kennen.



FabricPool ist nicht mit den StorageGRID ILM-Regeln oder -Richtlinien bekannt. Wenn die StorageGRID ILM-Richtlinie falsch konfiguriert ist, kann es zu Datenverlusten kommen. Ausführliche Informationen finden Sie unter ["Erstellen Sie eine ILM-Regel: Überblick"](#) Und ["Erstellen Sie eine ILM-Richtlinie: Überblick"](#).

Richtlinien für die Verwendung von ILM mit FabricPool

Bei Verwendung des FabricPool-Einrichtungsassistenten erstellt der Assistent automatisch eine neue ILM-Regel für jeden von Ihnen erstellten S3-Bucket, fügt diese Regel einer vorgeschlagenen Richtlinie hinzu und fordert Sie zur Aktivierung der neuen Richtlinie im Rahmen des Assistenten auf. Die automatisch erstellte Regel folgt den empfohlenen Best Practices: Sie verwendet 2+1 Erasure Coding an einem einzigen Standort.

Wenn Sie StorageGRID manuell konfigurieren und nicht den FabricPool Setup-Assistenten verwenden, lesen Sie diese Richtlinien, um sicherzustellen, dass Ihre ILM-Regeln und ILM-Richtlinien für FabricPool-Daten und Ihre Geschäftsanforderungen geeignet sind. Möglicherweise müssen Sie neue Regeln erstellen und Ihre aktive ILM-Richtlinie aktualisieren, um diese Richtlinien zu erfüllen.

- Sie können jede beliebige Kombination aus Replizierung und Verfahren zur Einhaltung von Datenkonsistenz zum Schutz von Cloud-Tiering-Daten verwenden.

Die empfohlene Best Practice besteht darin, ein 2+1-Verfahren zur Einhaltung von Datenkonsistenz an einem Standort zu verwenden, um eine kosteneffiziente Datensicherung zu gewährleisten. Das Verfahren zur Einhaltung von Datenkonsistenz benötigt zwar mehr CPU, bietet aber wesentlich weniger Storage-Kapazität als Replizierung. Die Schemata 4+1 und 6+1 benötigen weniger Kapazität als das Schema 2+1. Die Schemata 4+1 und 6+1 sind jedoch weniger flexibel, wenn Sie während der Grid-Erweiterung Storage-Nodes hinzufügen müssen. Weitere Informationen finden Sie unter ["Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden"](#).

- Jede auf FabricPool-Daten angewandte Regel muss entweder Erasure Coding verwenden oder mindestens zwei replizierte Kopien erstellen.



Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

- Wenn es nötig ist ["FabricPool-Daten aus StorageGRID entfernen"](#), Verwenden Sie ONTAP, um alle Daten für das FabricPool-Volumen abzurufen und auf die Performance-Tier zu übertragen.



Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Legen Sie den Aufbewahrungszeitraum in jeder ILM-Regel auf **Forever** fest, um sicherzustellen, dass FabricPool Objekte nicht durch StorageGRID ILM gelöscht werden.

- Erstellen Sie keine Regeln, um Daten aus FabricPool Cloud-Tiers an einen anderen Speicherort zu verschieben. Sie können keinen Cloud-Speicherpool verwenden, um FabricPool-Daten in einen anderen Objektspeicher zu verschieben. Ebenso können Sie FabricPool-Daten nicht mit einem Archivknoten auf Band archivieren.



Die Verwendung von Cloud Storage Pools mit FabricPool wird nicht unterstützt, weil die zusätzliche Latenz zum Abrufen eines Objekts aus dem Cloud-Storage-Pool-Ziel hinzugefügt wird.

- Ab ONTAP 9.8 können Sie optional Objekt-Tags erstellen, um Daten in Tiers zu klassifizieren und zu sortieren und das Management zu erleichtern. Beispielsweise können Sie Tags nur auf FabricPool Volumes festlegen, die an StorageGRID angebunden sind. Wenn Sie dann ILM-Regeln in StorageGRID erstellen, können Sie diese Daten mithilfe des erweiterten Filter Object Tag auswählen und platzieren.

Weitere Best Practices für StorageGRID und FabricPool

Wenn Sie ein StorageGRID-System für die Verwendung mit FabricPool konfigurieren, müssen Sie möglicherweise andere StorageGRID-Optionen ändern. Bevor Sie eine globale Einstellung ändern, überlegen Sie, wie sich die Änderung auf andere S3-

Anwendungen auswirkt.

Überwachungsmeldung und Protokollziele

FabricPool-Workloads verfügen oft über eine hohe Rate an Lesevorgängen, die ein hohes Volumen an Audit-Nachrichten erzeugen können.

- Wenn Sie keine Aufzeichnung von Client-Leseoperationen für FabricPool oder eine andere S3-Anwendung benötigen, gehen Sie optional zu **CONFIGURATION > Monitoring > Audit und Syslog-Server**. Ändern Sie die Einstellung **Client reads** auf **Error**, um die Anzahl der im Auditprotokoll aufgezeichneten Überwachungsmeldungen zu verringern. Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)" Entsprechende Details.
- Wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Applikationen verwenden oder alle Audit-Daten behalten möchten, konfigurieren Sie einen externen Syslog-Server und speichern Sie Audit-Informationen Remote. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Audit-Nachrichten auf die Performance minimiert, ohne dass die Vollständigkeit der Audit-Daten reduziert wird. Siehe "[Überlegungen für externen Syslog-Server](#)" Entsprechende Details.

Objektverschlüsselung

Beim Konfigurieren von StorageGRID können Sie optional den aktivieren "[Globale Option für Verschlüsselung gespeicherter Objekte](#)" Falls Datenverschlüsselung für andere StorageGRID Clients erforderlich ist. Die Daten, die von FabricPool zu StorageGRID verschoben werden, sind bereits verschlüsselt, d. h. die Aktivierung der StorageGRID-Einstellung ist nicht erforderlich. Die Client-seitige Verschlüsselung ist Eigentum von ONTAP.

Objektkomprimierung

Aktivieren Sie beim Konfigurieren von StorageGRID nicht das "[Globale Option zum Komprimieren gespeicherter Objekte](#)". Die Daten, die von FabricPool zu StorageGRID verschoben werden, werden bereits komprimiert. Durch Verwendung der Option StorageGRID wird die Größe eines Objekts nicht weiter reduziert.

Bucket-Konsistenzstufe

Für FabricPool Buckets ist die empfohlene Bucket-Konsistenzstufe **Read-after-New-write**, was die Standardeinstellung für einen neuen Bucket ist. Bearbeiten Sie FabricPool Buckets nicht, um **verfügbar** oder eine andere Konsistenzstufe zu verwenden.

FabricPool Tiering

Wenn ein StorageGRID Node Storage verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Wenn beispielsweise ein StorageGRID Node auf einem VMware Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datastore für den StorageGRID Node unterstützt, keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

FabricPool-Daten aus StorageGRID entfernen

Falls Sie die aktuell in StorageGRID gespeicherten FabricPool-Daten entfernen müssen, müssen Sie mithilfe von ONTAP alle Daten des FabricPool Volumes abrufen und in die Performance-Tier verschieben.

Bevor Sie beginnen

- Sie haben die Anweisungen und Überlegungen in geprüft ["Daten auf die Performance-Tier übertragen"](#).
- Sie verwenden ONTAP 9.8 oder höher.
- Sie verwenden ein ["Unterstützter Webbrowser"](#).
- Sie gehören einer StorageGRID-Benutzergruppe für das FabricPool-Mandantenkonto an, das über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#).

Über diese Aufgabe

Im Folgenden wird erläutert, wie Daten von StorageGRID zurück zu FabricPool verschoben werden. Sie führen dieses Verfahren mit ONTAP und StorageGRID Tenant Manager durch.

Schritte

1. Von ONTAP, geben Sie die `volume modify` Befehl.

Einstellen `tiering-policy` Bis `none` Um das neue Tiering zu beenden und festzulegen `cloud-retrieval-policy` Bis `promote` Um alle Daten zurückzugeben, die zuvor auf StorageGRID verschoben wurden.

Siehe ["Sämtliche Daten von einem FabricPool Volume auf die Performance-Tier übertragen"](#).

2. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie können das verwenden `volume object-store` Befehl mit dem `tiering` Option auf ["Überprüfen Sie den Status der Performance-Tier-Promotion"](#).

3. Wenn der Hochstufen-Vorgang abgeschlossen ist, melden Sie sich beim StorageGRID-Mandanten-Manager für das FabricPool-Mandanten-Konto an.
4. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
5. Vergewissern Sie sich, dass der FabricPool-Bucket jetzt leer ist.
6. Wenn der Eimer leer ist, ["Löschen Sie den Bucket"](#).

Nachdem Sie fertig sind

Wenn Sie den Bucket löschen, kann das Tiering von FabricPool zu StorageGRID nicht mehr fortgesetzt werden. Da die lokale Tier jedoch nach wie vor mit dem StorageGRID-Cloud-Tier verbunden ist, gibt ONTAP System Manager Fehlermeldungen aus, die darauf hinweisen, dass der Bucket nicht verfügbar ist.

Um diese Fehlermeldungen zu vermeiden, führen Sie einen der folgenden Schritte aus:

- Verwenden Sie FabricPool Mirror, um ein anderes Cloud-Tier zum Aggregat zu verbinden.
- Verschieben Sie die Daten aus dem FabricPool-Aggregat in ein nicht-FabricPool-Aggregat und löschen Sie dann das ungenutzte Aggregat.

Siehe ["ONTAP-Dokumentation für FabricPool"](#) Weitere Anweisungen.

Verwenden Sie StorageGRID

Verwenden Sie ein Mandantenkonto

Verwenden Sie ein Mandantenkonto: Überblick

Ein Mandantenkonto ermöglicht Ihnen, entweder die Simple Storage Service (S3) REST-API oder die Swift REST-API zu verwenden, um Objekte in einem StorageGRID System zu speichern und abzurufen.

Was ist ein Mandantenkonto?

Jedes Mandantenkonto verfügt über eigene föderierte bzw. lokale Gruppen, Benutzer, S3 Buckets oder Swift Container und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte durch verschiedene Einheiten zu trennen. Beispielsweise können für einen der folgenden Anwendungsfälle mehrere Mandantenkonten verwendet werden:

- **Anwendungsbeispiel für Unternehmen:** Wenn das StorageGRID-System innerhalb eines Unternehmens verwendet wird, kann der Objekt-Storage des Grid von den verschiedenen Abteilungen des Unternehmens getrennt werden. Beispielsweise können Mandantenkonten für die Marketingabteilung, die Kundenbetreuung, die Personalabteilung usw. vorhanden sein.



Wenn Sie das S3-Client-Protokoll verwenden, können Sie auch S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen eines Unternehmens zu trennen. Sie müssen keine separaten Mandantenkonten erstellen. Siehe Anweisungen zur Implementierung "[S3-Buckets und Bucket-Richtlinien](#)" Finden Sie weitere Informationen.

- **Anwendungsfall des Service-Providers:** Wenn das StorageGRID-System von einem Service-Provider verwendet wird, kann der Objekt-Storage des Grid von den verschiedenen Einheiten getrennt werden, die den Storage leasen. Beispielsweise können Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. vorhanden sein.

Erstellen eines Mandantenkontos

Mandantenkonten werden von einem erstellt "[StorageGRID Grid-Administrator, der den Grid Manager verwendet](#)". Beim Erstellen eines Mandantenkontos gibt der Grid-Administrator Folgendes an:

- Grundlegende Informationen, einschließlich Mandantename, Client-Typ (S3 oder Swift) und optionalem Storage-Kontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Platformservices verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Verbundverbindung verwenden kann.
- Der erste Root-Zugriff für den Mandanten basiert darauf, ob das StorageGRID System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign On (SSO) verwendet.

Grid-Administratoren können zudem die S3-Objektsperreinstellung für das StorageGRID System aktivieren, wenn S3-Mandantenkonten die gesetzlichen Anforderungen erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und managen.

S3-Mandanten konfigurieren

Nach einem ["S3-Mandantenkonto wird erstellt"](#), Sie können auf den Tenant Manager zugreifen, um Aufgaben wie die folgenden durchzuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Grid-Verbund für Account-Klone und Grid-übergreifende Replizierung verwenden
- Managen von S3-Zugriffsschlüsseln
- S3 Buckets erstellen und managen
- Verwenden Sie S3-Platfformservices
- Verwenden Sie S3 Select
- Monitoring der Storage-Auslastung



S3-Buckets können mit dem Tenant Manager erstellt und gemanagt werden, doch müssen Sie zum Einspielen und Managen von Objekten einen S3-Client verwenden. Siehe ["S3-REST-API VERWENDEN"](#) Entsprechende Details.

Konfigurieren Sie Swift Mandanten

Nach A ["Swift-Mandantenkonto wird erstellt"](#), Sie können auf den Tenant Manager zugreifen, um Aufgaben wie die folgenden durchzuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Monitoring der Storage-Auslastung



Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung erlaubt Benutzern jedoch nicht, sich beim zu authentifizieren ["Swift REST API"](#) Um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

So melden Sie sich an und melden sich ab

Melden Sie sich bei Tenant Manager an

Sie greifen auf den Mandanten-Manager zu, indem Sie die URL für den Mandanten in die Adresszeile von A eingeben ["Unterstützter Webbrowser"](#).

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verfügen über eine URL für den Zugriff auf den Mandanten-Manager, die vom Grid-Administrator bereitgestellt wird. Die URL sieht wie ein Beispiel 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 vollständig qualifizierten Domänennamen (FQDN), die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Knoten. Sie kann auch eine Portnummer, die 20-stellige Mandanten-Account-ID oder beides enthalten.

- Wenn die URL nicht die 20-stellige Konto-ID des Mandanten enthält, haben Sie diese Konto-ID.
- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie gehören einer Benutzergruppe an, die über verfügt "[Bestimmte Zugriffsberechtigungen](#)".

Schritte

1. Starten Sie A "[Unterstützter Webbrowser](#)".
2. Geben Sie in der Adressleiste des Browsers die URL für den Zugriff auf Tenant Manager ein.
3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten.
4. Melden Sie sich beim Tenant Manager an.

Der angezeigte Anmeldebildschirm hängt von der eingegebenen URL und davon ab, ob Single Sign-On (SSO) für StorageGRID konfiguriert wurde.

SSO wird nicht verwendet

Wenn StorageGRID SSO nicht verwendet, wird einer der folgenden Bildschirme angezeigt:

- Die Anmeldeseite des Grid Manager. Wählen Sie den Link **Tenant Sign-in**.



NetApp StorageGRID®

Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- Die Anmeldeseite von Tenant Manager. Das Feld **Account** ist möglicherweise bereits ausgefüllt, wie unten gezeigt.

NetApp StorageGRID®

Tenant Manager

Recent

-- Optional --

Account

64600207336181242061

Username

|

Password

Sign in

[NetApp support](#) | [NetApp.com](#)

- i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn er in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.
- ii. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
- iii. Wählen Sie **Anmelden**.

Das Dashboard von Tenant Manager wird angezeigt.

- iv. Wenn Sie ein erstes Passwort von einer anderen Person erhalten haben, wählen Sie **username > Passwort ändern**, um Ihr Konto zu sichern.

SSO wird verwendet

Wenn StorageGRID SSO verwendet, wird einer der folgenden Bildschirme angezeigt:

- Die SSO-Seite Ihres Unternehmens. Beispiel:

Sign in with your organizational account

someone@example.com

Password

Sign in

Geben Sie Ihre Standard-SSO-Anmeldeinformationen ein, und wählen Sie **Anmelden**.

- Die SSO-Anmeldeseite für den Tenant Manager.
 - i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn er in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.
 - ii. Wählen Sie **Anmelden**.
 - iii. Melden Sie sich mit Ihren Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihres Unternehmens an.

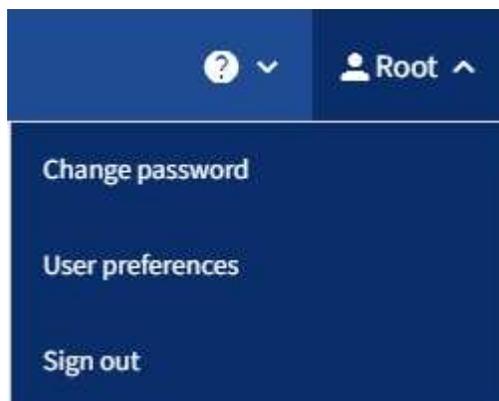
Das Dashboard von Tenant Manager wird angezeigt.

Melden Sie sich von Tenant Manager ab

Wenn Sie die Arbeit mit dem Mandantenmanager abgeschlossen haben, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer nicht auf das StorageGRID-System zugreifen können. Wenn Sie Ihren Browser schließen, werden Sie möglicherweise aufgrund der Cookie-Einstellungen des Browsers nicht aus dem System abgesendet.

Schritte

1. Suchen Sie das Dropdown-Menü Benutzername 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 für den Mandanten-Manager wird angezeigt.



Wenn Sie sich bei mehr als einem Admin-Node angemeldet haben, müssen Sie sich von jedem Knoten abmelden.

- Wenn SSO aktiviert ist:

Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugreifen konnten. Die Seite StorageGRID-Anmeldung wird angezeigt. Der Name des Mietkontos, auf das Sie gerade zugegriffen haben, wird als Standard im Dropdown-Menü **Letzte Konten** angegeben, und die **Konto-ID** des Mieters wird angezeigt.



Wenn SSO aktiviert ist und Sie sich auch beim Grid Manager angemeldet haben, müssen Sie sich auch vom Grid Manager abmelden, um sich von SSO abzumelden.

Mandantenmanager-Dashboard verstehen

Das Tenant Manager-Dashboard bietet einen Überblick über die Konfiguration eines Mandantenkontos und die Menge an Speicherplatz, die von Objekten in den Buckets (S3) oder Containern (Swift) verwendet wird. Wenn der Mandant über ein Kontingent verfügt, wird im Dashboard angezeigt, wie viel des Kontingents verwendet wird und wie viel übrig bleibt. Wenn Fehler im Zusammenhang mit dem Mandantenkonto auftreten, werden die Fehler auf dem Dashboard angezeigt.



Die Werte für den genutzten Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.

Wenn Objekte hochgeladen wurden, sieht das Dashboard wie das folgende Beispiel aus:

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups

1 User
View users

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

Tenant details [?](#)

Name: Tenant02
ID: 3341 1240 0546 8283 2208
 Platform services enabled
 Can use own identity source
 S3 Select enabled

Zusammenfassung des Mandantenkontos

Oben im Dashboard sind die folgenden Informationen enthalten:

- Die Anzahl der konfigurierten Buckets oder Container, Gruppen und Benutzer
- Die Anzahl der Endpunkte von Plattformservices, falls vorhanden

Sie können die Links auswählen, um die Details anzuzeigen.

Auf der rechten Seite des Dashboards sind folgende Informationen enthalten:

- Die Gesamtzahl der Objekte für den Mandanten.

Wenn für ein S3-Konto keine Objekte aufgenommen wurden und Sie über die Root-Zugriffsberechtigung verfügen, werden anstelle der Gesamtanzahl der Objekte die Richtlinien „erste Schritte“ angezeigt.

- Mandantendetails, einschließlich des Mandantenkontonamens und der ID und der Frage, ob der Mandant verwendet werden kann "Plattform-Services", "Seine eigene Identitätsquelle", "Grid-Verbund", Oder "S3 Select" (Es werden nur die aktivierten Berechtigungen aufgelistet.)

Storage- und Kontingentnutzung

Das Fenster Speichernutzung enthält die folgenden Informationen:

- Die Menge der Objektdaten für den Mandanten.



Dieser Wert gibt die Gesamtanzahl der hochgeladenen Objektdaten an und stellt nicht den Speicherplatz dar, der zum Speichern der Kopien dieser Objekte und ihrer Metadaten verwendet wird.

- Wenn ein Kontingent festgelegt ist, ist die Gesamtmenge an Speicherplatz, der für Objektdaten verfügbar ist, sowie die Menge und der Prozentsatz des verbleibenden Speicherplatzes. Der Kontingentnutzer beschränkt die Menge der Objektdaten, die aufgenommen werden können.



Die Quotennutzung basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. StorageGRID überprüft beispielsweise das Kontingent, wenn ein Mandant beginnt, Objekte hochzuladen und neue Einlässe zurückweist, wenn der Mieter die Quote überschritten hat. StorageGRID berücksichtigt jedoch bei der Bestimmung, ob das Kontingent überschritten wurde, nicht die Größe des aktuellen Uploads. Wenn Objekte gelöscht werden, kann ein Mandant vorübergehend daran gehindert werden, neue Objekte hochzuladen, bis die Kontingentnutzung neu berechnet wird. Berechnungen der Kontingentnutzung können 10 Minuten oder länger dauern.

- Ein Balkendiagramm, das die relative Größe der größten Buckets oder Container darstellt.

Sie können den Mauszeiger über eines der Diagrammsegmente platzieren, um den gesamten Speicherplatz anzuzeigen, der von diesem Bucket oder Container verbraucht wird.



- Zur Übereinstimmung mit dem Balkendiagramm, eine Liste der größten Buckets oder Container, einschließlich der Gesamtzahl 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 ein Mandant mehr als neun Buckets oder Container enthält, werden alle anderen Buckets oder Container zu einem Eintrag im unteren Teil der Liste zusammengefasst.



Um die Einheiten für die im Tenant Manager angezeigten Speicherwerte zu ändern, wählen Sie oben rechts im Tenant Manager das Benutzer-Dropdown aus, und wählen Sie dann **Benutzereinstellungen** aus.

Warnmeldungen zur Kontingentnutzung

Wenn im Grid Manager Warnmeldungen zur Kontingentnutzung aktiviert wurden, werden diese im Mandanten-Manager angezeigt, wenn das Kontingent niedrig oder überschritten ist, wie folgt:

Wenn 90% oder mehr der Quote eines Mandanten verwendet wurden, wird die Meldung **Tenant Quotenverbrauch hoch** ausgelöst. Führen Sie die empfohlenen Aktionen für die Warnmeldung aus.

 Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

Wenn Sie Ihre Quote überschreiten, können Sie keine neuen Objekte hochladen.

 The quota has been met. You cannot upload new objects.

Endpunktfehler

Wenn Sie mit Grid Manager einen oder mehrere Endpunkte für die Verwendung mit Plattformdiensten konfiguriert haben, zeigt das Tenant Manager-Dashboard eine Warnmeldung an, wenn in den letzten sieben Tagen Endpunktfehler aufgetreten sind.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Um Details über anzuzeigen "[Fehler am Endpunkt der Plattformdienste](#)" Wählen Sie **Endpoints**, um die Seite Endpoints anzuzeigen.

Mandantenmanagement-API

Mandantenmanagement-API verstehen

Sie können Systemmanagementaufgaben mit der REST-API für das Mandantenmanagement anstelle der Mandantenmanager-Benutzeroberfläche ausführen. Möglicherweise möchten Sie beispielsweise die API zur Automatisierung von Vorgängen verwenden oder mehrere Einheiten, wie beispielsweise Benutzer, schneller erstellen.

Die Mandantenmanagement-API:

- Verwendet die Open Source API-Plattform von Swagger. Swagger bietet eine intuitive Benutzeroberfläche, über die Entwickler und nicht-Entwickler mit der API interagieren können. Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.
- Verwendet "[Versionierung zur Unterstützung unterbrechungsfreier Upgrades](#)".

So greifen Sie auf die Swagger-Dokumentation für die Mandantenmanagement-API zu:

1. Melden Sie sich beim Tenant Manager an.
2. Wählen Sie oben im Tenant Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.

API-Betrieb

Die Mandantenmanagement-API organisiert die verfügbaren API-Vorgänge in die folgenden Abschnitte:

- **Account:** Operationen auf dem aktuellen Mandantenkonto, einschließlich der Speichernutzung Informationen.
- **Auth:** Operationen zur Authentifizierung der Benutzersitzung.

Die Mandantenmanagement-API unterstützt das Authentifizierungsschema für das Inhabertoken. Für eine Mandantenanmeldung geben Sie einen Benutzernamen, ein Passwort und eine Buchhaltungs-ID im JSON-Körper der Authentifizierungsanforderung (d. h. `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header der nachfolgenden API-Anforderungen ("Authorization: Bearer Token") bereitgestellt werden.

Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter "[Schützen Sie sich vor Cross-Site Request Forgery](#)".



Wenn Single Sign-On (SSO) für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Siehe "[Anweisungen zur Verwendung der Grid Management API](#)".

- **Config:** Operationen im Zusammenhang mit der Produktversion und den Versionen der Mandantenmanagement-API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container:** Operationen auf S3 Buckets oder Swift Containern.
- **Deactivated-Features:** Operationen zum Anzeigen von Features, die möglicherweise deaktiviert wurden.
- **Endpunkte:** Operationen zur Verwaltung eines Endpunkts. Endpunkte ermöglichen es einem S3-Bucket, einen externen Service für die Replizierung, Benachrichtigungen oder Suchintegration von StorageGRID CloudMirror zu verwenden.
- **Grid-Federation-connections:** Operationen auf Grid Federation-Verbindungen und Cross-Grid-Replikation.
- **Groups:** Operationen zur Verwaltung lokaler Mandantengruppen und zum Abrufen verbundener Mandantengruppen aus einer externen Identitätsquelle.
- **Identity-source:** Operationen zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **Regionen:** Operationen, um zu bestimmen, welche Regionen für das StorageGRID-System konfiguriert wurden.
- **s3:** Operationen zur Verwaltung von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-Object-Lock:** Operationen auf globalen S3 Object Lock-Einstellungen, die zur Unterstützung der Einhaltung gesetzlicher Vorschriften verwendet werden.
- **Benutzer:** Operationen zum Anzeigen und Verwalten von Mandantenbenutzern.

Betriebsdetails

Wenn Sie die einzelnen API-Operationen erweitern, können Sie die HTTP-Aktion, die Endpunkt-URL, eine Liste aller erforderlichen oder optionalen Parameter, ein Beispiel des Anforderungskörpers (falls erforderlich)

und die möglichen Antworten sehen.

groups Operations on groups

GET /org/groups Lists Tenant User Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses Response content type: application/json

Code	Description
200	

Example Value | Model

```
{
  "responseTime": "2018-02-01T16:22:31.066Z",
  "status": "success",
  "apiVersion": "2.1"
}
```

API-Anforderungen ausgeben



Alle API-Operationen, die Sie mit der API Docs Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Schritte

1. Wählen Sie die HTTP-Aktion aus, um die Anfragedetails anzuzeigen.
2. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, z. B. eine Gruppe oder eine Benutzer-ID. Dann erhalten Sie diese Werte. Sie müssen möglicherweise zuerst eine andere API-Anfrage stellen, um die Informationen zu erhalten, die Sie benötigen.

3. Bestimmen Sie, ob Sie den Text für die Beispielanforderung ändern müssen. In diesem Fall können Sie **Modell** wählen, um die Anforderungen für jedes Feld zu erfahren.
4. Wählen Sie **Probieren Sie es aus**.
5. Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
6. Wählen Sie **Ausführen**.
7. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Mandantenmanagement-API-Versionierung

Die Mandanten-Management-API verwendet Versionierung zur Unterstützung unterbrechungsfreier Upgrades.

Diese Anforderungs-URL gibt beispielsweise Version 3 der API an.

```
https://hostname_or_ip_address/api/v3/authorize
```

Die Hauptversion der Tenant Management API wird bei Änderungen, die *nicht kompatibel* mit älteren Versionen durchgeführt werden, angestoßen. Die Nebenversion der Tenant Management API wird angestoßen, wenn Änderungen vorgenommen werden, die *kompatibel* mit älteren Versionen sind. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften. Das folgende Beispiel zeigt, wie die API-Version basierend auf dem Typ der vorgenommenen Änderungen angestoßen wird.

Typ der Änderung in API	Alte Version	Neue Version
Kompatibel mit älteren Versionen	2.1	2.2
Nicht kompatibel mit älteren Versionen	2.1	3.0

Wenn die StorageGRID-Software zum ersten Mal installiert wird, ist nur die neueste Version der Mandantenmanagement-API aktiviert. Wenn StorageGRID jedoch auf eine neue Funktionsversion aktualisiert wird, haben Sie weiterhin Zugriff auf die ältere API-Version für mindestens eine StorageGRID-Funktionsversion.

Veraltete Anfragen werden wie folgt als veraltet markiert:

- Der Antwortkopf ist "Deprecated: True"
- Der JSON-Antwortkörper enthält „veraltet“: Wahr

Legen Sie fest, welche API-Versionen in der aktuellen Version unterstützt werden

Verwenden Sie die folgende API-Anforderung, um eine Liste der unterstützten API-Hauptversionen anzuzeigen:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Geben Sie die API-Version für die Anforderung an

Sie können die API-Version mithilfe eines Pfadparameters angeben (`/api/v3`) Oder eine Kopfzeile (`Api-Version: 3`). Wenn Sie beide Werte angeben, überschreibt der Kopfzeilenwert den Pfadwert.

```
curl https://<IP-Address>/api/v3/grid/accounts
```

```
curl -H "Api-Version: 3" https://<IP-Address>/api/grid/accounts
```

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

Sie können mithilfe von CSRF-Tokens die Authentifizierung verbessern, die Cookies verwendet, um Angriffe auf Cross-Site Request Forgery (CSRF) gegen StorageGRID zu schützen. Grid Manager und Tenant Manager aktivieren diese Sicherheitsfunktion automatisch; andere API-Clients können wählen, ob sie aktiviert werden sollen, wenn sie sich anmelden.

Ein Angreifer, der eine Anfrage an eine andere Website auslösen kann (z. B. mit einem HTTP-FORMULARPOST), kann dazu führen, dass bestimmte Anfragen mithilfe der Cookies des angemeldeten Benutzers erstellt werden.

StorageGRID schützt mit CSRF-Tokens vor CSRF-Angriffen. Wenn diese Option aktiviert ist, muss der Inhalt eines bestimmten Cookies mit dem Inhalt eines bestimmten Kopfes oder eines bestimmten POST-Body-Parameters übereinstimmen.

Um die Funktion zu aktivieren, stellen Sie die ein `csrfToken` Parameter an `true` Während der Authentifizierung. Die Standardeinstellung lautet `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Wenn wahr, A `GridCsrfToken` Cookies werden mit einem zufälligen Wert für die Anmeldung bei Grid Manager und dem gesetzt `AccountCsrfToken` Cookie wird mit einem zufälligen Wert für die Anmeldung bei Tenant Manager gesetzt.

Wenn das Cookie vorhanden ist, müssen alle Anforderungen, die den Status des Systems (POST, PUT, PATCH, DELETE) ändern können, eine der folgenden Optionen enthalten:

- Der `X-Csrf-Token` Kopfzeile, wobei der Wert der Kopfzeile auf den Wert des CSRF-Token-Cookies gesetzt ist.
- Für Endpunkte, die einen formcodierten Körper annehmen: A `csrfToken` Formularkodierung für den Anforderungskörperparameter.

Verwenden Sie zum Konfigurieren des CSRF-Schutzes die "[Grid Management API](#)" Oder "[Mandantenmanagement-API](#)".



Anforderungen, die über ein CSRF-Token-Cookie-Set verfügen, werden auch die durchsetzen "`Content-Type: application/json`" Kopfzeile für jede Anfrage, die einen JSON-Anforderungskörper als zusätzlichen Schutz gegen CSRF-Angriffe erwartet.

Netzverbundverbindungen verwenden

Klonen von Mandantengruppen und Benutzern

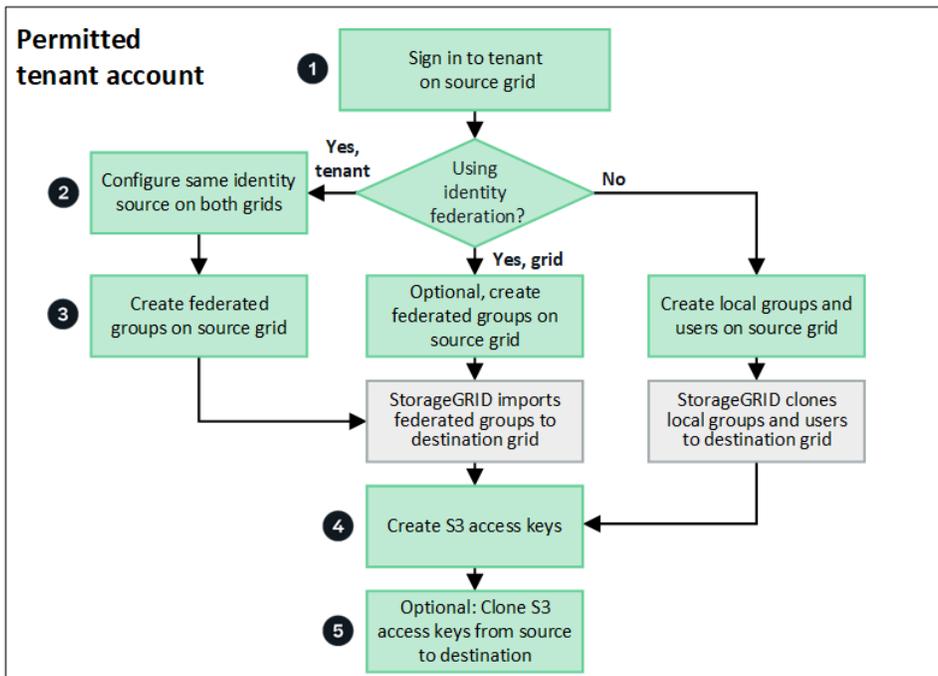
Wenn ein neuer Mandant über die Berechtigung zur Verwendung einer Grid-Verbundverbindung verfügt, wird dieser Mandant bei seiner Erstellung von einem StorageGRID System auf ein anderes StorageGRID System repliziert. Nach der Replizierung des Mandanten werden alle Gruppen und Benutzer, die dem Quellmandanten hinzugefügt wurden, dem Zielmandanten geklont.

Das StorageGRID-System, auf dem der Tenant ursprünglich erstellt wurde, ist das *source Grid* des Tenants. Das StorageGRID-System, auf dem der Mandant repliziert wird, ist das *Destination Grid* des Mandanten. Beide Mandantenkonten haben die gleiche Konto-ID, den gleichen Namen, eine Beschreibung, das gleiche Storage-Kontingent und die gleichen Berechtigungen, Der Zielmandant verfügt jedoch zunächst nicht über ein Root-Benutzerpasswort. Weitere Informationen finden Sie unter "[Was ist Account-Klon](#)" Und "[Management zulässiger Mandanten](#)".

Das Klonen von Mandantenkontoinformationen ist für erforderlich "[Grid-übergreifende Replizierung](#)" Von Bucket-Objekten. Durch die Verwendung derselben Mandantengruppen und Benutzer in beiden Grids können Sie auf die entsprechenden Buckets und Objekte in beiden Grids zugreifen.

Mandanten-Workflow für Account-Klon

Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, sehen Sie sich im Workflow-Diagramm die Schritte an, die Sie zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln durchführen werden.



Das sind die primären Schritte im Workflow:

1

Melden Sie sich beim Mandanten an

Melden Sie sich beim Mandantenkonto im Quellraster an (dem Raster, in dem der Mandant ursprünglich erstellt wurde).

2

Optional können Sie die Identity Federation konfigurieren

Wenn Ihr Mandantenkonto über die Berechtigung **eigene Identitätsquelle verwenden** verfügt, um verbundene Gruppen und Benutzer zu verwenden, konfigurieren Sie die gleiche Identitätsquelle (mit den gleichen Einstellungen) für die Quell- und Zielmandanten-Konten. Föderierte Gruppen und Benutzer können nur geklont werden, wenn beide Grids dieselbe Identitätsquelle verwenden. Anweisungen hierzu finden Sie unter "[Verwenden Sie den Identitätsverbund](#)".

3

Erstellen Sie Gruppen und Benutzer

Wenn Sie Gruppen und Benutzer erstellen, beginnen Sie immer vom Quellraster des Mandanten. Wenn Sie eine neue Gruppe hinzufügen, klonst StorageGRID sie automatisch in das Zielraster.

- Wenn die Identity Federation für das gesamte StorageGRID System oder Ihr Mandantenkonto konfiguriert wurde, "[Erstellen neuer Mandantengruppen](#)" Durch Importieren föderierter Gruppen aus der Identitätsquelle.
- Wenn Sie keine Identitätsföderation verwenden, "[Erstellen Sie neue lokale Gruppen](#)" Und dann "[Erstellen Sie lokale Benutzer](#)".

4

Erstellen von S3 Zugriffsschlüsseln

Das können Sie "[Erstellen Sie Ihre eigenen Zugriffsschlüssel](#)" Oder an "[Erstellen Sie die Zugriffsschlüssel](#)

eines anderen Benutzers" Entweder im Quell- oder im Zielraster, um auf Buckets in diesem Grid zuzugreifen.

5

Optionales Klonen von S3-Zugriffsschlüsseln

Wenn Sie auf Buckets mit denselben Zugriffsschlüsseln in beiden Grids zugreifen müssen, erstellen Sie die Zugriffsschlüssel im Quellraster und klonen Sie sie dann manuell mit der Tenant Manager-API in das Zielraster. Anweisungen hierzu finden Sie unter ["Klonen von S3-Zugriffsschlüsseln mithilfe der API"](#).

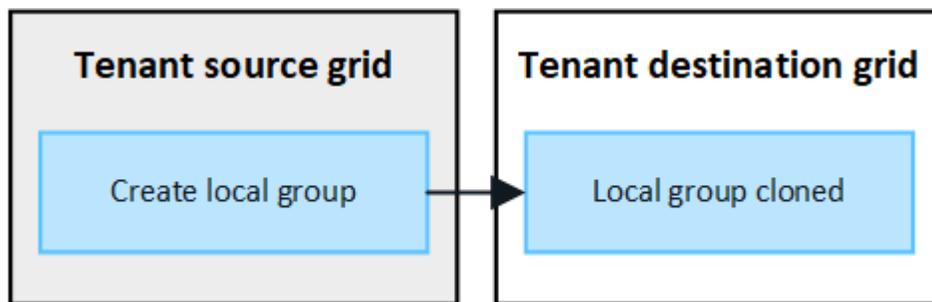
Wie werden Gruppen, Benutzer und S3-Zugriffsschlüssel geklont?

Lesen Sie diesen Abschnitt, um zu erfahren, wie Gruppen, Benutzer und S3-Zugriffsschlüssel zwischen dem Mandanten-Quellraster und dem Mandanten-Zielraster geklont werden.

Lokale Gruppen, die im Quellraster erstellt wurden, werden geklont

Nachdem ein Mandantenkonto erstellt und in das Zielraster repliziert wurde, klonst StorageGRID automatisch alle lokalen Gruppen, die Sie dem Quell-Grid des Mandanten zum Zielraster des Mandanten hinzufügen.

Sowohl die ursprüngliche Gruppe als auch der zugehörige Klon weisen den gleichen Zugriffsmodus, die gleichen Gruppenberechtigungen und die S3-Gruppenrichtlinie auf. Anweisungen hierzu finden Sie unter ["Gruppen für S3 Mandanten erstellen"](#).

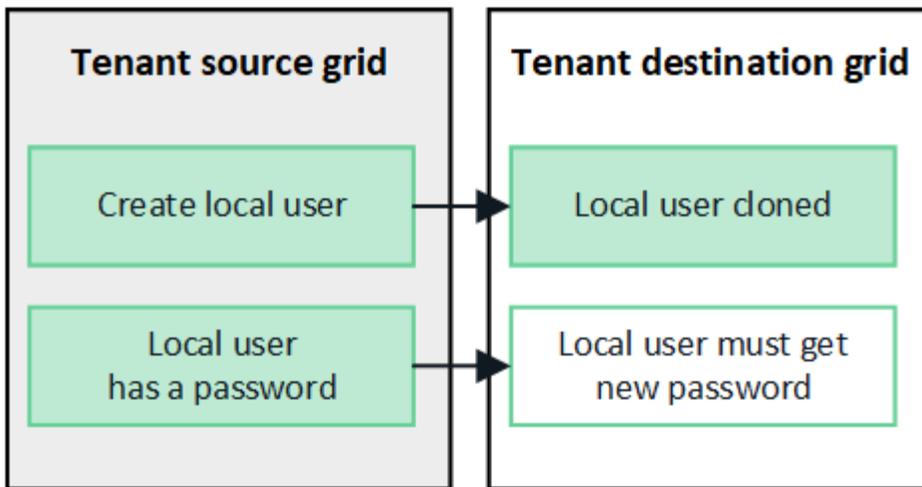


Alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quellraster auswählen, werden nicht berücksichtigt, wenn die Gruppe im Zielraster geklont wird. Wählen Sie aus diesem Grund keine Benutzer aus, wenn Sie die Gruppe erstellen. Wählen Sie stattdessen die Gruppe aus, wenn Sie die Benutzer erstellen.

Lokale Benutzer, die im Quellraster erstellt wurden, werden geklont

Wenn Sie einen neuen lokalen Benutzer im Quellraster erstellen, klonst StorageGRID diesen Benutzer automatisch in das Zielraster. Sowohl der ursprüngliche Benutzer als auch sein Klon haben den gleichen vollständigen Namen, Benutzernamen und die gleiche Einstellung für **Zugriff verweigern**. Beide Benutzer gehören ebenfalls zu den gleichen Gruppen. Anweisungen hierzu finden Sie unter ["Managen Sie lokale Benutzer"](#).

Aus Sicherheitsgründen werden lokale Benutzerpasswörter nicht im Zielraster geklont. Wenn ein lokaler Benutzer im Zielraster auf Tenant Manager zugreifen muss, muss der Root-Benutzer des Mandantenkontos ein Kennwort für diesen Benutzer im Zielraster hinzufügen. Anweisungen hierzu finden Sie unter ["Managen Sie lokale Benutzer"](#).

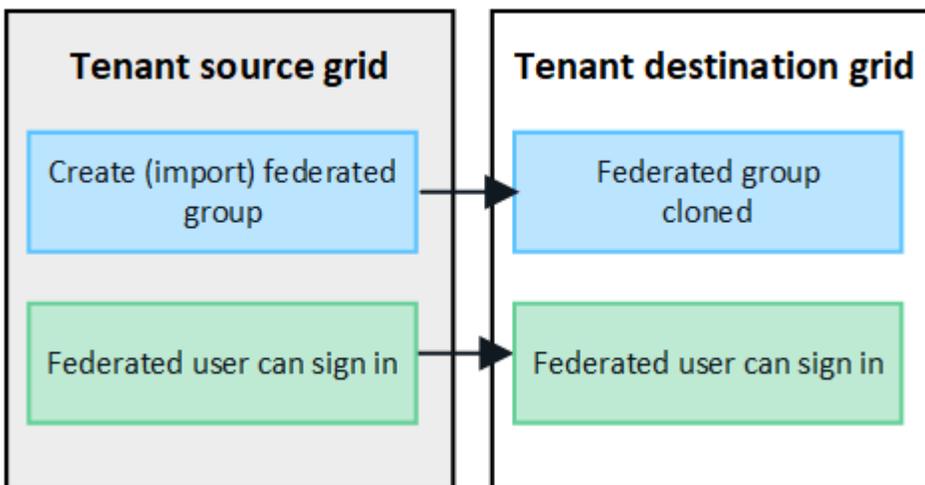


Im Quellraster erstellte Verbundgruppen werden geklont

Angenommen, die Anforderungen für die Verwendung von Account Clone mit werden angenommen ["Single Sign On"](#) Und ["Identitätsföderation"](#) Zusammengetragen wurden, werden gebündelte Gruppen, die Sie für den Mandanten im Quellraster erstellen (importieren), automatisch auf den Mandanten im Zielraster geklont.

Beide Gruppen verfügen über denselben Zugriffsmodus, dieselben Gruppenberechtigungen und dieselbe S3-Gruppenrichtlinie.

Nachdem für den Quellmandanten gebündelte Gruppen erstellt und für den Zielmandanten geklont wurden, können sich föderierte Benutzer in beiden Grids beim Mandanten anmelden.



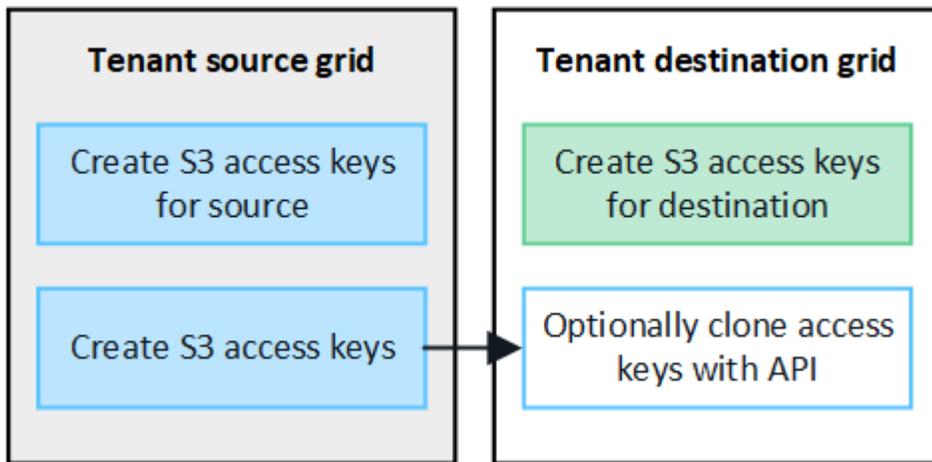
S3-Zugriffsschlüssel können manuell geklont werden

StorageGRID klonet S3-Zugriffsschlüssel nicht automatisch, da die Sicherheit durch unterschiedliche Schlüssel auf jedem Grid verbessert wird.

Zum Verwalten der Zugriffsschlüssel in den beiden Grids haben Sie folgende Möglichkeiten:

- Wenn Sie nicht die gleichen Tasten für jedes Raster verwenden müssen, können Sie ["Erstellen Sie Ihre eigenen Zugriffsschlüssel"](#) Oder ["Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers"](#) Auf jedem Raster.
- Wenn Sie dieselben Schlüssel auf beiden Rastern verwenden müssen, können Sie Schlüssel im Quellraster erstellen und dann die Tenant Manager-API manuell verwenden ["Schlüssel klonen"](#) Zum

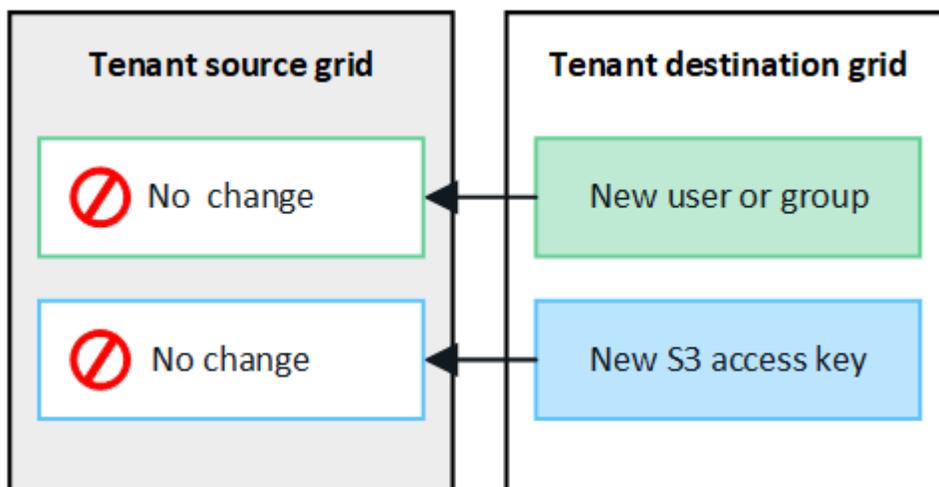
Zielraster.



Wenn Sie S3-Zugriffsschlüssel für einen föderierten Benutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel zum Zielmandanten geklont.

Gruppen und Benutzer, die dem Zielraster hinzugefügt wurden, sind nicht geklont

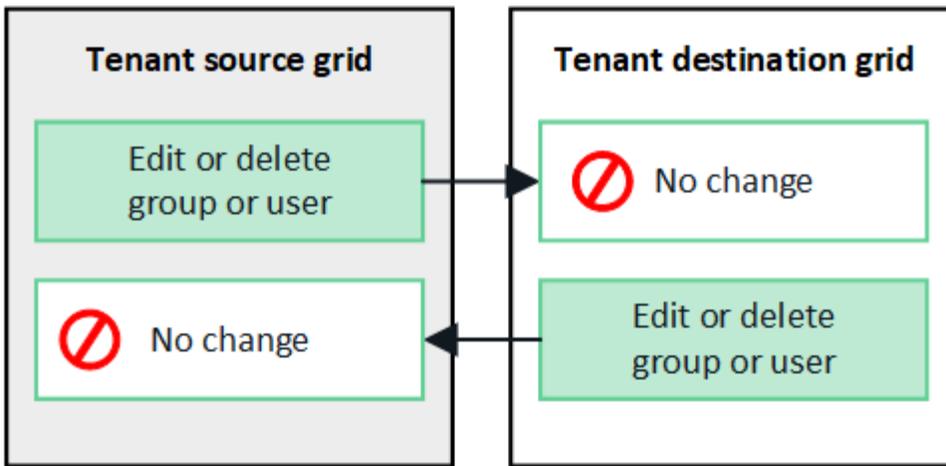
Das Klonen erfolgt nur vom Quell-Grid des Mandanten zum Ziel-Grid des Mandanten. Wenn Sie Gruppen und Benutzer im Zielraster des Mandanten erstellen oder importieren, werden diese Elemente von StorageGRID nicht im Quellraster des Mandanten geklont.



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 einer der beiden Raster bearbeiten oder löschen, werden die Änderungen nicht in der anderen Tabelle geklont.



Klonen von S3-Zugriffsschlüsseln mithilfe der API

Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen.

Bevor Sie beginnen

- Das Mandantenkonto hat die Berechtigung **Grid Federation connection** verwenden.
- Die Netzwerkverbindung hat einen **Verbindungsstatus** von **Verbunden**.
- Sie sind mit einem beim Tenant Manager im Quellraster des Mandanten angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen Sie Ihre eigenen S3-Anmeldedaten 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 föderierten Benutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel zum Zielmandanten hinzugefügt.

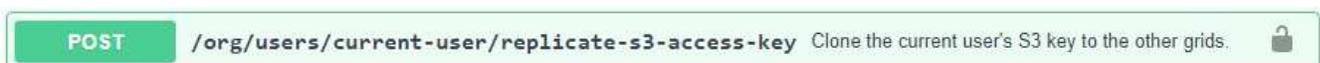
Eigene Zugriffsschlüssel klonen

Sie können Ihre eigenen Zugriffsschlüssel klonen, wenn Sie auf dieselben Buckets in beiden Rastern zugreifen müssen.

Schritte

1. Mithilfe des Tenant Manager im Quellraster "[Erstellen Sie Ihre eigenen Zugriffsschlüssel](#)" Und laden Sie die herunter .csv Datei:
2. Wählen Sie oben im Tenant Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
3. Wählen Sie im Abschnitt **s3** den folgenden Endpunkt aus:

POST /org/users/current-user/replicate-s3-access-key



4. Wählen Sie **Probieren Sie es aus**.
5. Ersetzen Sie im Textfeld **body** die Beispieleinträge für **accesskey** und **secretAccessKey** durch die Werte aus der heruntergeladenen **.csv**-Datei.

Achten Sie darauf, dass die doppelten Anführungszeichen um jede Zeichenfolge herum beibehalten werden.



6. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Zeit als String im ISO 8601-Datenzeitformat (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 vorangegangene Komma).
7. Wählen Sie **Ausführen**.
8. Bestätigen Sie, dass der Server-Antwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

Die Zugriffsschlüssel eines anderen Benutzers klonen

Sie können die Zugriffsschlüssel eines anderen Benutzers klonen, wenn er auf dieselben Buckets in beiden Rastern zugreifen muss.

Schritte

1. Mithilfe des Tenant Manager im Quellraster "[Erstellen Sie die S3-Zugriffsschlüssel des anderen Benutzers](#)" Und laden Sie die herunter **.csv** Datei:
2. Wählen Sie oben im Tenant Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
3. Die Benutzer-ID abrufen. Sie benötigen diesen Wert, um die Zugriffsschlüssel des anderen Benutzers zu klonen.
 - a. Wählen Sie im Abschnitt **Users** den folgenden Endpunkt aus:

```
GET /org/users
```
 - b. Wählen Sie **Probieren Sie es aus**.
 - c. Geben Sie alle Parameter an, die beim Suchen von Benutzern verwendet werden sollen.
 - 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
```

POST

/org/users/{userId}/replicate-s3-access-key Clone an S3 key to the other grids.



5. Wählen Sie **Probieren Sie es aus**.
6. Fügen Sie im Textfeld **userid** die von Ihnen kopierte Benutzer-ID ein.
7. Ersetzen Sie im Textfeld **body** die Beispieleinträge für **example Access key** und **secret Access key** durch die Werte aus der **.csv**-Datei für diesen Benutzer.

Achten Sie darauf, dass die doppelten Anführungszeichen um die Zeichenfolge herum beibehalten werden.

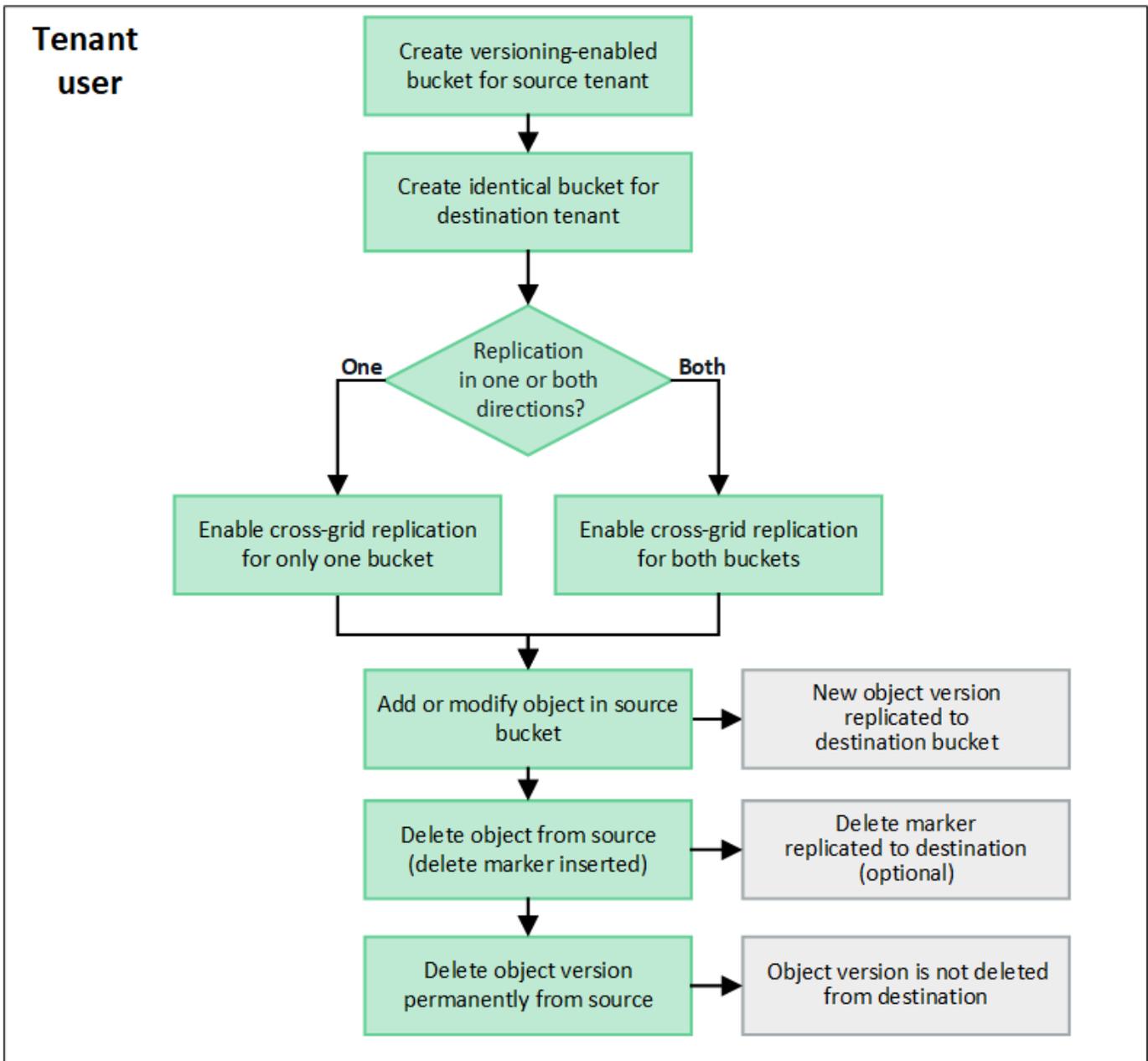
8. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Zeit als String im ISO 8601-Datenzeitformat (z. B. `2023-02-28T22:46:33-08:00`). Wenn der Schlüssel nicht abläuft, geben Sie **null** als Wert für den Eintrag **expires** ein (oder entfernen Sie die Zeile **expires** und das vorangegangene Komma).
9. Wählen Sie **Ausführen**.
10. Bestätigen Sie, dass der Server-Antwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

Grid-übergreifende Replizierung managen

Wenn Ihrem Mandantenkonto bei der Erstellung die Berechtigung **Grid Federation connection** zugewiesen wurde, können Sie mittels Grid-Replizierung automatisch Objekte zwischen Buckets im Quell-Grid des Mandanten und Buckets im Zielraster des Mandanten replizieren. Die Grid-übergreifende Replizierung kann in eine oder beide Richtungen erfolgen.

Workflow für Grid-übergreifende Replizierung

Das Workflow-Diagramm fasst die Schritte zusammen, die Sie zur Konfiguration der Grid-übergreifenden Replikation zwischen Buckets in zwei Grids durchführen. Diese Schritte werden im Folgenden genauer beschrieben.



Konfiguration der Grid-übergreifenden Replizierung

Bevor Sie die Grid-übergreifende Replizierung verwenden können, müssen Sie sich bei den entsprechenden Mandantenkonten in jedem Grid anmelden und identische Buckets erstellen. Anschließend können Sie die Grid-übergreifende Replizierung für einen oder beide Buckets aktivieren.

Bevor Sie beginnen

- Sie haben die Anforderungen für die Grid-übergreifende Replizierung überprüft. Siehe "[Was ist Grid-übergreifende Replizierung](#)".
- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Das Mandantenkonto hat die Berechtigung **use Grid Federation connection**, und identische Mandantenkonten existieren auf beiden Grids. Siehe "[Verwalten Sie die zulässigen Mandanten für die Grid Federation-Verbindung](#)".
- Der Mandantenbenutzer, den Sie sich anmelden, da er bereits in beiden Rastern vorhanden ist, gehört zu einer Benutzergruppe, die über den verfügt "[Root-Zugriffsberechtigung](#)".

- Wenn Sie sich als lokaler Benutzer im Zielraster des Mandanten anmelden, hat der Root-Benutzer für das Mandantenkonto ein Kennwort für Ihr Benutzerkonto in diesem Raster festgelegt.

Erstellen Sie zwei identische Buckets

Melden Sie sich als ersten Schritt bei den entsprechenden Mandantenkonten in jedem Grid an und erstellen Sie identische Buckets.

Schritte

1. Erstellen Sie ausgehend von einem der beiden Raster in der Grid Federation-Verbindung einen neuen Bucket:
 - a. Melden Sie sich mit den Anmeldeinformationen eines Mandantenbenutzers an, der in beiden Grids vorhanden ist.



Wenn Sie sich nicht als lokaler Benutzer am Zielraster des Mandanten anmelden können, bestätigen Sie, dass der Root-Benutzer für das Mandantenkonto ein Kennwort für Ihr Benutzerkonto festgelegt hat.

- b. Befolgen Sie die Anweisungen unter "[Erstellen eines S3-Buckets](#)".
 - c. Wählen Sie auf der Registerkarte **Objekteinstellungen verwalten** **Objektversionierung aktivieren**.
 - d. Wenn die S3-Objektsperre für Ihr StorageGRID-System aktiviert ist, aktivieren Sie nicht die S3-Objektsperre für den Bucket.
 - e. Wählen Sie **Eimer erstellen**.
 - f. Wählen Sie **Fertig**.
2. Wiederholen Sie diese Schritte, um einen identischen Bucket für dasselbe Mandantenkonto auf dem anderen Grid in der Grid-Federation-Verbindung zu erstellen.

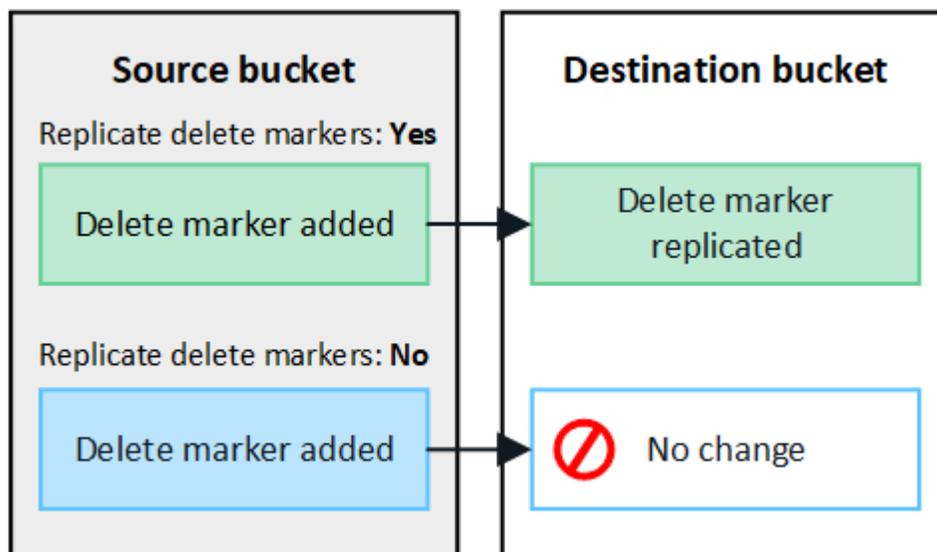
Grid-übergreifende Replizierung

Sie müssen diese Schritte ausführen, bevor Sie Objekte zu einem Bucket hinzufügen.

Schritte

1. Aktivieren Sie, beginnend mit einem Raster, dessen Objekte Sie replizieren möchten "[Grid-übergreifende Replizierung in eine Richtung](#)":
 - a. Melden Sie sich beim Mandantenkonto für den Bucket an.
 - b. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
 - c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Seite mit den Bucket-Details zuzugreifen.
 - d. Wählen Sie die Registerkarte **Grid-Replikation** aus.
 - e. Wählen Sie **enable**, und überprüfen Sie die Liste der Anforderungen.
 - f. Wenn alle Anforderungen erfüllt sind, wählen Sie die zu verwendende Netzverbundverbindung aus.
 - g. Optional können Sie die Einstellung **Replicate delete Markers** ändern, um festzustellen, was im Zielraster passiert, wenn ein S3-Client eine Löschanforderung an das Quellraster ausgibt, das keine Versions-ID enthält:
 - Wenn **Yes** (Standard), wird dem Quell-Bucket eine Löschmarkierung hinzugefügt und in den Ziel-Bucket repliziert.

- Wenn **Nein**, wird dem Quell-Bucket eine Löschmarkierung hinzugefügt, aber nicht in den Ziel-Bucket repliziert.



Wenn die Löschanforderung eine Versions-ID enthält, wird diese Objektversion dauerhaft aus dem Quell-Bucket entfernt. StorageGRID repliziert Löschanforderungen, die eine Versions-ID enthalten, nicht, sodass dieselbe Objektversion nicht vom Ziel gelöscht wird.

Siehe "[Was ist Grid-übergreifende Replizierung](#)" Entsprechende Details.

- Überprüfen Sie Ihre Auswahl. Sie können diese Einstellungen nur ändern, wenn beide Buckets leer sind.
- Wählen Sie **Enable und Test**.

Nach einigen Augenblicken wird eine Erfolgsmeldung angezeigt. Objekte, die diesem Bucket hinzugefügt wurden, werden nun automatisch in das andere Grid repliziert. **Grid-übergreifende Replikation** wird als aktivierte Funktion auf der Bucket-Detailseite angezeigt.

- Gehen Sie optional zum entsprechenden Bucket auf dem anderen Raster und "[Aktivieren Sie die Grid-übergreifende Replizierung in beide Richtungen](#)".

Testen Sie die Replikation zwischen Grids

Wenn die Grid-übergreifende Replizierung für einen Bucket aktiviert ist, müssen Sie möglicherweise überprüfen, ob die Verbindung und die Grid-übergreifende Replizierung ordnungsgemäß funktionieren und dass die Quell- und Ziel-Buckets nach wie vor alle Anforderungen erfüllen (beispielsweise ist die Versionierung weiterhin aktiviert).

Bevor Sie beginnen

- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Schritte

- Melden Sie sich beim Mandantenkonto für den Bucket an.
- Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

3. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Seite mit den Bucket-Details zuzugreifen.
4. Wählen Sie die Registerkarte **Grid-Replikation** aus.
5. Wählen Sie **Verbindung testen**.

Wenn die Verbindung in einem ordnungsgemäßen Zustand ist, wird ein Erfolgsbanner angezeigt. Andernfalls wird eine Fehlermeldung angezeigt, die Sie und der Grid-Administrator zur Behebung des Problems verwenden können. Weitere Informationen finden Sie unter "[Fehler beim Grid-Verbund beheben](#)".

6. Wenn die Grid-übergreifende Replikation in beide Richtungen konfiguriert ist, gehen Sie zum entsprechenden Bucket auf dem anderen Grid und wählen Sie **Verbindung testen** aus, um zu überprüfen, ob die Grid-übergreifende Replikation in die andere Richtung funktioniert.

Deaktivieren Sie die Grid-übergreifende Replizierung

Sie können die Grid-übergreifende Replikation dauerhaft beenden, wenn Sie keine Objekte mehr in das andere Raster kopieren möchten.

Beachten Sie vor dem Deaktivieren der Grid-übergreifenden Replikation Folgendes:

- Durch die Deaktivierung der Grid-übergreifenden Replikation werden keine Objekte entfernt, die bereits zwischen den Rastern kopiert wurden. Beispiel: Objekte in `my-bucket` In Raster 1, die in `my-bucket` In Grid 2 kopiert wurden werden nicht entfernt, wenn Sie die Grid-übergreifende Replizierung für diesen Bucket deaktivieren. Wenn Sie diese Objekte löschen möchten, müssen Sie sie manuell entfernen.
- Wenn die Grid-übergreifende Replizierung für jeden Buckets aktiviert wurde (d. h. wenn die Replikation in beide Richtungen erfolgt), können Sie die Grid-übergreifende Replizierung für einen oder beide Buckets deaktivieren. Sie können beispielsweise die Replikation von `my-bucket` Auf Raster 1 bis `my-bucket` In Tabelle 2, während Sie weiterhin Objekte aus `my-bucket` Auf Raster 2 bis `my-bucket` In Raster 1.
- Sie müssen die Grid-übergreifende Replizierung deaktivieren, bevor Sie die Berechtigung eines Mandanten zur Verwendung der Grid-Federation-Verbindung entfernen können. Siehe "[Management zulässiger Mandanten](#)".
- Wenn Sie die Grid-übergreifende Replizierung für einen Bucket deaktivieren, der Objekte enthält, können Sie die Grid-übergreifende Replizierung nur wieder aktivieren, wenn Sie alle Objekte sowohl aus den Quell- als auch aus den Ziel-Buckets löschen.



Die Replikation kann nur dann wieder aktiviert werden, wenn beide Buckets leer sind.

Bevor Sie beginnen

- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Schritte

1. Beenden Sie die Grid-Replizierung für den Bucket, beginnend mit dem Grid, dessen Objekte Sie nicht mehr replizieren möchten:
 - a. Melden Sie sich beim Mandantenkonto für den Bucket an.
 - b. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
 - c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Seite mit den Bucket-Details zuzugreifen.

- d. Wählen Sie die Registerkarte **Grid-Replikation** aus.
- e. Wählen Sie **Replikation deaktivieren**.
- f. Wenn Sie sicher sind, dass Sie die Grid-übergreifende Replikation für diesen Bucket deaktivieren möchten, geben Sie **Yes** in das Textfeld ein und wählen Sie **Disable** aus.

Nach einigen Augenblicken wird eine Erfolgsmeldung angezeigt. Neue Objekte, die diesem Bucket hinzugefügt wurden, können nicht mehr automatisch in das andere Grid repliziert werden. **Grid-übergreifende Replikation** wird nicht mehr als aktivierte Funktion auf der Buckets-Seite angezeigt.

2. Wenn die Grid-übergreifende Replizierung für beide Richtungen konfiguriert wurde, wechseln Sie zum entsprechenden Bucket auf dem anderen Grid und beenden Sie die Grid-übergreifende Replizierung in die andere Richtung.

Anzeigen von Verbindungen mit Grid Federation

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, können Sie die zulässigen Verbindungen anzeigen.

Bevor Sie beginnen

- Das Mandantenkonto hat die Berechtigung **Grid Federation connection** verwenden.
- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Grid Federation Connections**.

Die Seite Grid Federation Connection wird angezeigt und enthält eine Tabelle, in der die folgenden Informationen zusammengefasst werden:

Spalte	Beschreibung
Verbindungsname	Der Grid-Verbund stellt Verbindungen her, zu denen dieser Mandant berechtigt ist.
Buckets mit Grid-übergreifender Replizierung	Für jede Grid-Verbundverbindung die Mandanten-Buckets, für die die Grid-übergreifende Replizierung aktiviert ist Objekte, die diesen Buckets hinzugefügt werden, werden in das andere Raster der Verbindung repliziert.
Letzter Fehler	Bei jeder Grid-Federation-Verbindung tritt ggf. der letzte Fehler auf, wenn die Daten in das andere Grid repliziert wurden. Siehe Löschen Sie den letzten Fehler .

2. Wählen Sie optional einen Bucket-Namen aus "[Bucket-Details anzeigen](#)".

Leeren Sie den letzten Fehler

In der Spalte **Last error** kann aus einem der folgenden Gründe ein Fehler auftreten:

- Die Version des Quellobjekts wurde nicht gefunden.

- Der Quell-Bucket wurde nicht gefunden.
- Der Ziel-Bucket wurde gelöscht.
- Der Ziel-Bucket wurde von einem anderen Konto neu erstellt.
- Im Ziel-Bucket ist die Versionierung angehalten.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist aber jetzt nicht mehr versioniert.



In dieser Spalte wird nur der letzte gitterübergreifende Replikationsfehler angezeigt. Frühere Fehler, die möglicherweise aufgetreten sind, werden nicht angezeigt.

Schritte

1. Wenn in der Spalte **Last error** eine Meldung angezeigt wird, sehen Sie sich den Nachrichtentext an.

Dieser Fehler zeigt beispielsweise an, dass der Ziel-Bucket für die Grid-übergreifende Replizierung in einem ungültigen Status war, möglicherweise weil die Versionierung ausgesetzt oder S3 Object Lock aktiviert wurde.

2. Führen Sie alle empfohlenen Aktionen aus. Wenn beispielsweise die Versionierung auf dem Ziel-Bucket für die Grid-übergreifende Replizierung angehalten wurde, aktivieren Sie die Versionierung für diesen Bucket neu.
3. Wählen Sie die Verbindung aus der Tabelle aus.
4. Wählen Sie **Fehler löschen**.
5. Wählen Sie **Ja**, um die Meldung zu löschen und den Systemstatus zu aktualisieren.
6. Warten Sie 5-6 Minuten, und nehmen Sie dann ein neues Objekt in den Bucket auf. Bestätigen Sie, dass die Fehlermeldung nicht erneut angezeigt wird.



Um sicherzustellen, dass die Fehlermeldung gelöscht wird, warten Sie mindestens 5 Minuten nach dem Zeitstempel in der Nachricht, bevor Sie ein neues Objekt aufnehmen.

7. Informationen zum Bestimmen, ob Objekte aufgrund des Bucket-Fehlers nicht repliziert werden konnten, finden Sie unter "[Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut](#)".

Verwalten von Gruppen und Benutzern

Verwenden Sie den Identitätsverbund

Durch die Verwendung eines Identitätsverbunds können Mandantengruppen und Benutzer schneller eingerichtet werden, und Mandantenbenutzer können sich dann mithilfe der vertrauten Anmeldedaten beim Mandantenkonto anmelden.

Konfigurieren Sie die Identitätsföderation für Mandanten-Manager

Sie können eine Identitätsföderation für den Mandanten-Manager konfigurieren, wenn Mandantengruppen und Benutzer in einem anderen System, z. B. Active Directory, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server, gemanagt werden sollen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Root-Zugriffsberechtigung"](#).
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitäts-Provider.



Wenn Sie einen nicht aufgeführten LDAP v3-Dienst verwenden möchten, wenden Sie sich an den technischen Support.

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Siehe [Richtlinien für die Konfiguration von OpenLDAP-Server](#).
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, muss der Identitäts-Provider TLS 1.2 oder 1.3 verwenden. Siehe ["Unterstützte Chiffren für ausgehende TLS-Verbindungen"](#).

Über diese Aufgabe

Ob Sie einen Identitätsföderationsdienst für Ihren Mandanten konfigurieren können, hängt davon ab, wie Ihr Mandantenkonto eingerichtet wurde. Der Mandant kann sich möglicherweise den für den Grid Manager konfigurierten Identitätsföderationsdienst teilen. Wenn diese Meldung angezeigt wird, wenn Sie auf die Seite Identity Federation zugreifen, können Sie keine separate föderierte Identitätsquelle für diesen Mandanten 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 Identifizieren Verbund konfigurieren, geben Sie die Werte an, die StorageGRID für die Verbindung mit einem LDAP-Dienst benötigt.

Schritte

1. Wählen Sie *** ACCESS MANAGEMENT* > Identity Federation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
------------------	-------	----------	-------

Wählen Sie **Other** aus, um Werte für einen LDAP-Server zu konfigurieren, der Oracle Directory Server verwendet.

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt LDAP-Attribute aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
 - **Eindeutiger Benutzername:** Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `uid` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `uid`.
 - **Benutzer-UUID:** Der Name des Attributs, das den permanenten eindeutigen Identifier eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
 - **Group Unique Name:** Der Name des Attributs, das den eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `cn` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn`.
 - **Group UUID:** Der Name des Attributs, das den permanenten eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
5. Geben Sie für alle LDAP-Servicetypen die Informationen zum erforderlichen LDAP-Server und zur Netzwerkverbindung im Abschnitt LDAP-Server konfigurieren ein.
 - **Hostname:** Der vollständig qualifizierte Domainname (FQDN) oder die IP-Adresse des LDAP-Servers.
 - **Port:** Der Port, über den eine Verbindung zum LDAP-Server hergestellt wird.



Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden beliebigen Port verwenden, solange Ihre Firewall korrekt konfiguriert ist.

- **Benutzername:** Der vollständige Pfad des Distinguished Name (DN) für den Benutzer, der eine Verbindung zum LDAP-Server herstellt.

Für Active Directory können Sie auch den unten angegebenen Anmeldenamen oder den Benutzerprinzipalnamen festlegen.

Der angegebene Benutzer muss über die Berechtigung zum Auflisten von Gruppen und Benutzern sowie zum Zugriff auf die folgenden Attribute verfügen:

- `sAMAccountName` Oder `uid`

- objectGUID, entryUUID, Oder nsuniqueid
 - cn
 - memberOf Oder isMemberOf
 - **Active Directory:** objectSid, primaryGroupID, userAccountControl, und userPrincipalName
 - **Azure:** accountEnabled Und userPrincipalName
- **Passwort:** Das mit dem Benutzernamen verknüpfte Passwort.
 - **Group Base DN:** Der vollständige Pfad des Distinguished Name (DN) für einen LDAP-Unterbaum, nach dem Sie nach Gruppen suchen möchten. Im Active Directory-Beispiel (unten) können alle Gruppen, deren Distinguished Name relativ zum Basis-DN (DC=storagegrid,DC=example,DC=com) ist, als föderierte Gruppen verwendet werden.



Die **Group Unique Name**-Werte müssen innerhalb des **Group Base DN**, zu dem sie gehören, eindeutig sein.

- **User Base DN:** Der vollständige Pfad des Distinguished Name (DN) eines LDAP-Unterbaums, nach dem Sie nach Benutzern suchen möchten.



Die **Benutzer-eindeutigen Namen**-Werte müssen innerhalb des **User Base DN**, zu dem sie gehören, eindeutig sein.

- **Bind username Format** (optional): Das Standard-Username Muster StorageGRID sollte verwendet werden, wenn das Muster nicht automatisch ermittelt werden kann.

Es wird empfohlen, **Bind username Format** bereitzustellen, da Benutzer sich anmelden können, wenn StorageGRID nicht mit dem Servicekonto verknüpft werden kann.

Geben Sie eines der folgenden Muster ein:

- **UserPrincipalName pattern (Active Directory und Azure):** [USERNAME]@example.com
- **Namensmuster für Anmeldung auf der Ebene nach unten (Active Directory und Azure):** example\[USERNAME]
- *** Distinguished Name pattern*:** CN=[USERNAME],CN=Users,DC=example,DC=com

Fügen Sie **[USERNAME]** genau wie geschrieben ein.

6. Wählen Sie im Abschnitt Transport Layer Security (TLS) eine Sicherheitseinstellung aus.

- **Verwenden Sie STARTTLS:** Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder andere, diese Option wird jedoch für Azure nicht unterstützt.
- **LDAPS verwenden:** Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für Azure auswählen.
- **Verwenden Sie keine TLS:** Der Netzwerkverkehr zwischen dem StorageGRID-System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.



Die Verwendung der Option **keine TLS** verwenden wird nicht unterstützt, wenn Ihr Active Directory-Server die LDAP-Signatur erzwingt. Sie müssen STARTTLS oder LDAPS verwenden.

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, mit dem die Verbindung gesichert werden soll.
 - **Verwenden Sie das Betriebssystem CA-Zertifikat:** Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
 - **Benutzerdefiniertes CA-Zertifikat verwenden:** Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat.

Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat in das Textfeld CA-Zertifikat und fügen Sie es ein.

Testen Sie die Verbindung und speichern Sie die Konfiguration

Nachdem Sie alle Werte eingegeben haben, müssen Sie die Verbindung testen, bevor Sie die Konfiguration speichern können. StorageGRID überprüft die Verbindungseinstellungen für den LDAP-Server und das BIND-Username-Format, wenn Sie es angegeben haben.

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein bind username Format angegeben haben:
 - Wenn die Verbindungseinstellungen gültig sind, wird eine Meldung „Verbindung erfolgreich testen“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
 - Wenn die Verbindungseinstellungen ungültig sind, wird eine „Testverbindung konnte nicht hergestellt werden“-Meldung angezeigt. Wählen Sie **Schließen**. Beheben Sie anschließend alle Probleme, und testen Sie die Verbindung erneut.
3. Wenn Sie ein bind username Format angegeben haben, geben Sie den Benutzernamen und das Kennwort eines gültigen föderierten Benutzers ein.

Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr Kennwort ein. Geben Sie keine Sonderzeichen in den Benutzernamen ein, z. B. @ oder /.

Test Connection ✕

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel
Test Connection

- Wenn die Verbindungseinstellungen gültig sind, wird eine Meldung „Verbindung erfolgreich testen“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
- Es wird eine Fehlermeldung angezeigt, wenn die Verbindungseinstellungen, das Bind-Username-Format oder der Test-Benutzername und das Kennwort ungültig sind. Beheben Sie alle Probleme, und testen Sie die Verbindung erneut.

Synchronisierung mit Identitätsquelle erzwingen

Das StorageGRID-System synchronisiert regelmäßig föderierte Gruppen und Benutzer von der Identitätsquelle aus. Sie können die Synchronisierung erzwingen, wenn Sie Benutzerberechtigungen so schnell wie möglich aktivieren oder einschränken möchten.

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Wählen Sie oben auf der Seite **Sync Server** aus.

Der Synchronisierungsprozess kann je nach Umgebung einige Zeit in Anspruch nehmen.



Die Warnmeldung * Identity Federation Failure* wird ausgelöst, wenn es ein Problem gibt, das die Synchronisierung von föderierten Gruppen und Benutzern aus der Identitätsquelle verursacht.

Deaktivieren Sie den Identitätsverbund

Sie können den Identitätsverbund für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, besteht keine Kommunikation zwischen StorageGRID und der Identitätsquelle. Allerdings bleiben alle von Ihnen konfigurierten Einstellungen erhalten, sodass Sie die Identitätsföderation zukünftig einfach wieder aktivieren können.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.
- Föderierte Benutzer, die sich derzeit anmelden, erhalten bis zu ihrem Ablauf Zugriff auf das StorageGRID-

System, können sich jedoch nach Ablauf der Sitzung nicht anmelden.

- Die Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle erfolgt nicht, und Warnmeldungen oder Alarme werden nicht für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Enable Identity Federation** ist deaktiviert, wenn Single Sign-On (SSO) auf **enabled** oder **Sandbox Mode** eingestellt ist. Der SSO-Status auf der Seite Single Sign-On muss **deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Siehe "[Deaktivieren Sie Single Sign-On](#)".

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Deaktivieren Sie das Kontrollkästchen **Enable Identity Federation**.

Richtlinien für die Konfiguration von OpenLDAP-Server

Wenn Sie einen OpenLDAP-Server für die Identitätsföderation verwenden möchten, müssen Sie bestimmte Einstellungen auf dem OpenLDAP-Server konfigurieren.



Bei Identitätsquellen, die nicht ActiveDirectory oder Azure sind, blockiert StorageGRID den S3-Zugriff nicht automatisch für Benutzer, die extern deaktiviert sind. Löschen Sie zum Blockieren des S3-Zugriffs alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie in den Anweisungen zur Wartung der Umkehrgruppenmitgliedschaft [imhttp://www.openldap.org/doc/admin24/index.html](http://www.openldap.org/doc/admin24/index.html)["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"].

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Stichwörtern für den Index konfigurieren:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Stellen Sie außerdem sicher, dass die in der Hilfe für den Benutzernamen genannten Felder für eine optimale Leistung indiziert sind.

Weitere Informationen zur Wartung von Gruppenmitgliedschaften finden Sie [imhttp://www.openldap.org/doc/admin24/index.html](http://www.openldap.org/doc/admin24/index.html)["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"].

Managen von Mandantengruppen

Erstellen von Gruppen für einen S3-Mandanten

Sie können Berechtigungen für S3-Benutzergruppen managen, indem Sie föderierte

Gruppen importieren oder lokale Gruppen erstellen.

Bevor Sie beginnen

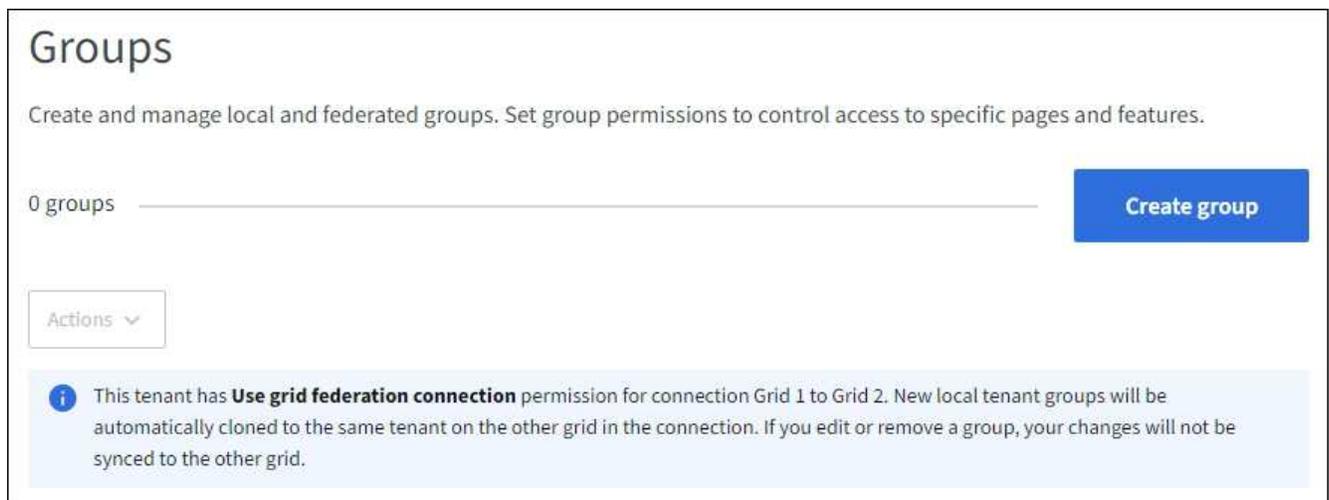
- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".
- Wenn Sie planen, eine föderierte Gruppe zu importieren, haben Sie "[Konfigurierte Identitätsföderation](#)", Und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, haben Sie den Workflow und die Überlegungen für überprüft "[Klonen von Mandantengruppen und Benutzern](#)", Und Sie sind im Quellraster des Mandanten angemeldet.

Rufen Sie den Assistenten zum Erstellen von Gruppen auf

Rufen Sie als ersten Schritt den Assistenten zum Erstellen von Gruppen auf.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verfügt, bestätigen Sie, dass ein blaues Banner erscheint, das anzeigt, dass neue Gruppen, die in diesem Raster erstellt werden, auf demselben Mandanten auf dem anderen Raster der Verbindung geklont werden. Wenn dieses Banner nicht angezeigt wird, werden Sie möglicherweise im Zielraster des Mandanten angemeldet.



3. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

Sie können eine lokale Gruppe erstellen oder eine föderierte Gruppe importieren.

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, 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 Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

2. Geben Sie den Namen der Gruppe ein.

- **Lokale Gruppe:** Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, tritt ein Klonfehler auf, wenn der gleiche **eindeutige Name** bereits für den Mandanten im Zielraster vorhanden ist.

- **Federated Group:** Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.

3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer in Tenant Manager und Tenant Management API durchführen können.

Schritte

1. Wählen Sie für **Access Mode** eine der folgenden Optionen aus:

- **Lesen-Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Konfiguration des Mandanten verwalten.
- **Schreibgeschützt:** Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder keine Vorgänge in der Tenant Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Wählen Sie eine oder mehrere Berechtigungen für diese Gruppe aus.

Siehe "[Mandantenmanagement-Berechtigungen](#)".

3. Wählen Sie **Weiter**.

Legen Sie die S3-Gruppenrichtlinie fest

Die Gruppenrichtlinie legt fest, über welche S3-Zugriffsberechtigungen Benutzer verfügen.

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 über eine Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.

Gruppenrichtlinie	Beschreibung
Schreibgeschützter Zugriff	Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine schreibgeschützte Gruppenrichtlinie angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
Voller Zugriff	Benutzer in dieser Gruppe haben vollständigen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
Ransomware-Minimierung	<p>Diese Beispielrichtlinie gilt für alle Buckets für diesen Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber Objekte aus Buckets, für die die Objektversionierung aktiviert ist, nicht dauerhaft löschen.</p> <p>Tenant Manager-Benutzer mit der Berechtigung Alle Buckets verwalten können diese Gruppenrichtlinie überschreiben. Beschränken Sie die Berechtigung zum Verwalten aller Buckets auf vertrauenswürdige Benutzer und verwenden Sie die Multi-Faktor-Authentifizierung (MFA), sofern verfügbar.</p>
Individuell	Benutzer in der Gruppe erhalten die Berechtigungen, 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 einen gültigen JSON-formatierten String eingeben.

Ausführliche Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispiele, finden Sie unter "[Beispiel für Gruppenrichtlinien](#)".

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine Verbundgruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional alle bereits vorhandenen lokalen Benutzer hinzufügen.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verfügt, werden alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quellraster auswählen, nicht berücksichtigt, wenn die Gruppe im Zielraster geklont wird. Wählen Sie aus diesem Grund keine Benutzer aus, wenn Sie die Gruppe erstellen. 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 stellen**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie sich im Quellraster des Mandanten befinden, wird die neue Gruppe im Zielraster des Mandanten geklont. **Success** erscheint als **Klonstatus** im Abschnitt Übersicht der Detailseite der Gruppe.

Erstellen von 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 Swift-Administratorberechtigung verfügen, die zur Verwaltung der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".
- Wenn Sie planen, eine föderierte Gruppe zu importieren, haben Sie "[Konfigurierte Identitätsföderation](#)", Und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Rufen Sie den Assistenten zum Erstellen von Gruppen auf

Schritte

Rufen Sie als ersten Schritt den Assistenten zum Erstellen von Gruppen auf.

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

Sie können eine lokale Gruppe erstellen oder eine föderierte Gruppe importieren.

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, 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 Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

2. Geben Sie den Namen der Gruppe ein.
 - **Lokale Gruppe:** Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.

- **Federated Group:** Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.

3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer in Tenant Manager und Tenant Management API durchführen können.

Schritte

1. Wählen Sie für **Access Mode** eine der folgenden Optionen aus:

- **Lesen-Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Konfiguration des Mandanten verwalten.
- **Schreibgeschützt:** Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder keine Vorgänge in der Tenant Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Aktivieren Sie das Kontrollkästchen **Root Access**, wenn Gruppenbenutzer sich 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, um 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 Verbundgruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional alle bereits vorhandenen lokalen 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 dem Benutzer auf der Seite Benutzer hinzufügen. Siehe "[Managen Sie lokale Benutzer](#)".

2. Wählen Sie **Gruppe erstellen** und **Fertig stellen**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Mandantenmanagement-Berechtigungen

Bevor Sie eine Mandantengruppe erstellen, überlegen Sie, welche Berechtigungen Sie dieser Gruppe zuweisen möchten. Über die Mandantenmanagement-Berechtigungen wird festgelegt, welche Aufgaben Benutzer mit dem Tenant Manager oder der Mandantenmanagement-API durchführen können. Ein Benutzer kann einer oder mehreren Gruppen angehören. Berechtigungen werden kumulativ, wenn ein Benutzer zu mehreren Gruppen gehört.

Um sich beim Tenant Manager anzumelden oder die Mandantenmanagement-API zu verwenden, müssen Benutzer einer Gruppe mit mindestens einer Berechtigung angehören. Alle Benutzer, die sich anmelden können, können die folgenden Aufgaben ausführen:

- Dashboard anzeigen
- Eigenes Kennwort ändern (für lokale Benutzer)

Für alle Berechtigungen legt die Einstellung Zugriffsmodus der Gruppe fest, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie nur die zugehörigen Einstellungen und Funktionen anzeigen können.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff 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.

Berechtigung	Beschreibung
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API. Hinweis: Swift-Benutzer müssen über Root-Zugriffsberechtigung verfügen, um sich beim Mandantenkonto anzumelden.
Verwalter	Nur Swift Mandanten. Bietet vollständigen Zugriff auf die Swift Container und Objekte für dieses Mandantenkonto Hinweis: Swift-Benutzer müssen über die Swift-Administrator-Berechtigung verfügen, um alle Operationen mit der Swift REST-API auszuführen.
Management Ihrer eigenen S3 Zugangsdaten	Benutzer können ihre eigenen S3-Zugriffsschlüssel erstellen und entfernen. Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption STORAGE (S3) > Meine S3-Zugriffstasten nicht.

Berechtigung	Beschreibung
Managen aller Buckets	<ul style="list-style-type: none"> • S3-Mandanten: Ermöglicht Benutzern die Nutzung des Mandanten-Manager und der Mandanten-Management-API, um S3-Buckets zu erstellen und zu löschen sowie die Einstellungen für alle S3-Buckets im Mandantenkonto zu managen, unabhängig von S3-Bucket- oder Gruppenrichtlinien. <p>Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption Buckets nicht.</p> <ul style="list-style-type: none"> • Swift Mandanten: Ermöglicht Swift Benutzern die Kontrolle der Konsistenzstufe für Swift Container mithilfe der Mandanten-Management-API. <p>Hinweis: Sie können Swift-Gruppen nur die Berechtigung Alle Buckets verwalten über die Tenant Management API zuweisen. Diese Berechtigung können Swift-Gruppen nicht mit dem Tenant Manager zugewiesen werden.</p>
Verwalten von Endpunkten	<p>Ermöglicht Benutzern die Verwendung des Tenant Managers oder der Mandanten-Management-API zum Erstellen oder Bearbeiten von Plattformdienstendpunkten, die als Ziel für StorageGRID-Plattformdienste verwendet werden.</p> <p>Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption Plattform-Dienste-Endpunkte nicht.</p>
Managen von Objekten über die S3-Konsole	<p>In Kombination mit der Berechtigung Alle Buckets verwalten können Benutzer über die Seite Buckets auf die Experimental S3-Konsole zugreifen. Benutzer, die über diese Berechtigung verfügen, aber nicht über die Berechtigung zum Verwalten aller Buckets verfügen, können dennoch direkt zur Experimental S3 Console navigieren.</p>

Gruppen managen

Sie können eine Gruppe anzeigen, den Namen, die Berechtigungen, die Richtlinien und die Benutzer einer Gruppe bearbeiten und eine Gruppe duplizieren. Oder eine Gruppe löschen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[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 für alle lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

Wenn das Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie

Gruppen im Quellraster des Mandanten anzeigen, zeigt ein blaues Banner an, dass Ihre Änderungen beim Bearbeiten oder Entfernen einer Gruppe nicht mit dem anderen Raster synchronisiert werden. Siehe ["Klonen von Mandantengruppen und Benutzern"](#).

3. Wenn Sie den Namen der Gruppe ändern möchten:
 - a. Aktivieren Sie das Kontrollkästchen für die Gruppe.
 - b. Wählen Sie **Aktionen > Gruppenname bearbeiten**.
 - c. Geben Sie den neuen Namen ein.
 - d. Wählen Sie **Änderungen speichern**.
4. Wenn Sie weitere Details anzeigen oder weitere 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 **actions > View Group Details**.
5. Lesen Sie den Abschnitt „Übersicht“, in dem die folgenden Informationen für jede Gruppe angezeigt werden:
 - Anzeigename
 - Eindeutiger Name
 - Typ
 - Zugriffsmodus
 - Berechtigungen
 - S3-Richtlinie
 - Anzahl der Benutzer in dieser Gruppe
 - Zusätzliche Felder, wenn das Mandantenkonto die Berechtigung **Grid Federation connection** verwendet hat und Sie die Gruppe im Quellraster des Mandanten anzeigen:
 - Klonstatus, entweder **success** oder **failure**
 - Ein blaues Banner, das darauf hinweist, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diese Gruppe bearbeiten oder löschen.
6. Bearbeiten Sie die Gruppeneinstellungen nach Bedarf. Siehe ["Erstellen von Gruppen für einen S3-Mandanten"](#) und ["Erstellen von Gruppen für einen Swift Mandanten"](#) Für Details, was eingegeben werden soll.
 - 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** 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 den JSON-String 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.

Manage users

You can add users to this group or remove users from this group.

Add users
Remove Users

🔍

Displaying 1 results

Username ⌵	Full Name ⌵	Denied ⌵
User_02	User_02_Managers	

b. Wählen Sie **Benutzer hinzufügen**.

c. Wählen Sie die vorhandenen Benutzer aus, die Sie hinzufügen möchten, und wählen Sie **Benutzer hinzufügen**.

Oben rechts wird eine Erfolgsmeldung angezeigt.

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 wird eine Erfolgsmeldung angezeigt.

9. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

Gruppe duplizieren

Sie können eine vorhandene Gruppe duplizieren, um neue Gruppen schneller zu erstellen.



Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie eine Gruppe aus dem Quellraster des Mandanten duplizieren, wird die duplizierte Gruppe im Zielraster 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. Siehe "[Erstellen von Gruppen für einen S3-Mandanten](#)" Oder "[Erstellen von Gruppen für einen Swift Mandanten](#)" Für Details, was eingegeben werden soll.

5. Wählen Sie **Gruppe erstellen**.

Löschen Sie eine oder mehrere Gruppen

Sie können eine oder mehrere Gruppen löschen. Alle Benutzer, die nur zu einer Gruppe gehören, die gelöscht wurde, können sich nicht mehr beim Tenant Manager anmelden oder das Mandantenkonto verwenden.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie eine Gruppe löschen, wird StorageGRID die entsprechende Gruppe im anderen Raster nicht löschen. 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**.

Managen Sie lokale Benutzer

Sie können lokale Benutzer erstellen und lokalen Gruppen zuweisen, um zu bestimmen, auf welche Funktionen diese Benutzer zugreifen können. Der Tenant Manager enthält einen vordefinierten lokalen Benutzer mit dem Namen „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 Mandanten-Management-API anmelden, obwohl sie Clientanwendungen verwenden können, um basierend auf Gruppenberechtigungen auf die Ressourcen des Mandanten zuzugreifen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, haben Sie den Workflow und die Überlegungen für überprüft "[Klonen von Mandantengruppen und Benutzern](#)", Und Sie sind im Quellraster des Mandanten angemeldet.

Erstellen Sie einen lokalen Benutzer

Sie können einen lokalen Benutzer erstellen und diesen einer oder mehreren lokalen Gruppen zuweisen, um ihre Zugriffsberechtigungen zu steuern.

S3-Benutzer, die keiner Gruppe angehören, haben keine Managementberechtigungen oder S3-Gruppenrichtlinien, die auf sie angewendet werden. Diese Benutzer haben möglicherweise S3-Bucket-Zugriff, der über eine Bucket-Richtlinie gewährt wird.

Swift-Benutzer, die keiner Gruppe angehören, haben keine Managementberechtigungen oder Swift-Container-Zugriff.

Rufen Sie den Assistenten zum Erstellen von Benutzern auf

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, zeigt ein blaues Banner an, dass dies das Quellraster des Mandanten ist. Alle lokalen Benutzer, die Sie in diesem Raster erstellen, werden in das andere Raster der Verbindung geklont.

2. Wählen Sie **Benutzer erstellen**.

Geben Sie die Anmeldedaten ein

Schritte

1. Füllen Sie für den Schritt **Enter user credentials** die folgenden Felder aus.

Feld	Beschreibung
Vollständiger Name	Der vollständige Name für diesen Benutzer, z. B. der vor- und Nachname einer Person oder der Name einer Anwendung.
Benutzername	Der Name, den dieser Benutzer zur Anmeldung verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden. Hinweis: Wenn Ihr Mieterkonto die Berechtigung Grid Federation connection verwenden hat, tritt ein Klonfehler auf, wenn der gleiche Benutzername bereits für den Mieter im Zielraster vorhanden ist.
Passwort und Passwort bestätigen	Das Passwort, das der Benutzer beim Anmelden verwendet.
Zugriff verweigern	Wählen Sie Ja , um zu verhindern, dass sich dieser Benutzer beim Mandantenkonto anmeldet, obwohl er noch zu einer oder mehreren Gruppen gehört. Wählen Sie zum Beispiel Ja , um die Anmelde-Fähigkeit eines Benutzers vorübergehend zu unterbrechen.

2. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

Schritte

1. Weisen Sie den Benutzer einer oder mehreren lokalen Gruppen zu, um zu bestimmen, welche Aufgaben er ausführen kann.

Das Zuweisen eines Benutzers zu Gruppen ist optional. Wenn Sie möchten, können Sie Benutzer auswählen, wenn Sie Gruppen erstellen oder bearbeiten.

Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören. Siehe "[Mandantenmanagement-Berechtigungen](#)".

2. Wählen Sie **Benutzer erstellen**.

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie sich im

Quellraster des Mandanten befinden, wird der neue lokale Benutzer im Zielraster des Mandanten geklont. **Success** erscheint als **Klonstatus** im Abschnitt Übersicht der Detailseite des Benutzers.

3. Wählen Sie **Fertig**, um zur Benutzerseite 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 für alle lokalen und föderierten Benutzer dieses Mandantenkontos aufgeführt sind.

Wenn das Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie den Benutzer im Quellraster des Mandanten anzeigen, zeigt ein blaues Banner an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie den Benutzer bearbeiten oder entfernen.

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 weitere 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. Lesen Sie den Abschnitt Übersicht, in dem die folgenden Informationen für jeden Benutzer angezeigt werden:
 - Vollständiger Name
 - Benutzername
 - Benutzertyp
 - Zugriff verweigert
 - Zugriffsmodus
 - Gruppenmitgliedschaft
 - Zusätzliche Felder, wenn das Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie den Benutzer im Quellraster des Mandanten anzeigen:
 - Klonstatus, entweder **success** oder **failure**
 - Ein blaues Banner, das darauf hinweist, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diesen Benutzer bearbeiten.
6. Bearbeiten Sie die Benutzereinstellungen nach Bedarf. Siehe [Erstellen Sie einen lokalen Benutzer](#) Für Details, was eingegeben werden soll.
 - a. Ändern Sie im Abschnitt Übersicht den vollständigen Namen, indem Sie den Namen oder das Bearbeiten-Symbol 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 **Access No** aus, damit sich der Benutzer anmelden kann, oder wählen Sie **Yes**, um die Anmeldung des Benutzers zu verhindern. Wählen Sie dann **Änderungen speichern**.
 - d. Wählen Sie auf der Registerkarte **Zugriffstasten** die Option **Schlüssel erstellen** aus, und befolgen Sie die Anweisungen für "[Erstellen der S3-Zugriffsschlüssel eines anderen Benutzers](#)".
 - e. Wählen Sie auf der Registerkarte **Gruppen** die Option **Gruppen bearbeiten**, um den Benutzer zu Gruppen hinzuzufügen oder ihn aus Gruppen zu entfernen. Wählen Sie dann **Änderungen speichern**.
7. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

Doppelter lokaler Benutzer

Sie können einen lokalen Benutzer duplizieren, um einen neuen Benutzer schneller zu erstellen.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie einen Benutzer aus dem Quellraster des Mandanten duplizieren, wird der duplizierte Benutzer im Zielraster 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. Siehe [Erstellen Sie einen lokalen Benutzer](#) Für Details, was eingegeben werden soll.
5. Wählen Sie **Benutzer erstellen**.

Löschen Sie einen oder mehrere lokale Benutzer

Sie können einen oder mehrere lokale Benutzer, die nicht mehr auf das StorageGRID-Mandantenkonto zugreifen müssen, dauerhaft löschen.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie einen lokalen Benutzer löschen, wird StorageGRID den entsprechenden Benutzer im anderen Raster nicht löschen. Wenn Sie diese Informationen synchron halten müssen, müssen Sie denselben Benutzer aus beiden Rastern löschen.



Sie müssen die föderierte Identitätsquelle verwenden, um verbundene Benutzer 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 Bestätigungsdiaologfeld wird angezeigt.

4. Wählen Sie **Benutzer löschen** oder **Benutzer löschen**.

Managen von S3-Zugriffsschlüsseln

Managen Sie S3 Zugriffsschlüssel: Übersicht

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 gemanagt werden:

- Benutzer, die die Berechtigung **Manage your own S3 credentials** besitzen, 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 vollständigen Zugriff auf alle Buckets und Objekte für Mandanten, sofern nicht ausdrücklich von einer Bucket-Richtlinie deaktiviert wurde.

StorageGRID unterstützt die Authentifizierung nach Signature Version 2 und Signature Version 4. Der Zugriff auf übergreifende Konten ist nur zulässig, wenn diese durch eine Bucket-Richtlinie ausdrücklich aktiviert wurde.

Erstellen Ihrer eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel erstellen. Sie benötigen einen Zugriffsschlüssel für den Zugriff auf Ihre Buckets und Objekte.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen Sie Ihre eigenen S3-Anmeldedaten oder Root-Zugriffsberechtigungen"](#).

Über diese Aufgabe

Sie können einen oder mehrere S3-Zugriffsschlüssel erstellen und managen, 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 dem geheimen Zugriffsschlüssel. Aus Sicherheitsgründen sollten Sie nicht mehr Schlüssel erstellen, als Sie benötigen, und die Schlüssel löschen, die Sie nicht verwenden. Wenn Sie nur einen Schlüssel haben und demnächst abläuft, erstellen Sie einen neuen Schlüssel, bevor der alte Schlüssel abläuft, und löschen Sie dann den alten Schlüssel.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder keinen Ablauf haben. Beachten Sie die folgenden Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für Ihre Schlüssel fest, um den Zugriff auf einen bestimmten Zeitraum zu beschränken. Durch die Einrichtung einer kurzen Ablaufzeit kann Ihr Risiko verringert werden, wenn Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel versehentlich ausgesetzt sind. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie keine Ablaufzeit für Ihre Schlüssel festlegen. Wenn Sie sich zu einem späteren Zeitpunkt für die Erstellung neuer Schlüssel entscheiden, löschen Sie die alten Schlüssel manuell.



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.

Die Seite Meine Zugriffsschlüssel wird angezeigt und enthält alle vorhandenen Zugriffsschlüssel.

2. Wählen Sie **Schlüssel erstellen**.
3. Führen Sie einen der folgenden Schritte aus:
 - Wählen Sie **Verfallszeit nicht festlegen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
 - Wählen Sie **Verfallszeit festlegen**, und legen Sie das Ablaufdatum und die Uhrzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Verfallszeit kann mindestens eine Minute von der aktuellen Zeit entfernt sein.

4. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld Zugriffsschlüssel herunterladen wird angezeigt, in dem Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel aufgeführt sind.

5. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.



Schließen Sie dieses Dialogfeld erst, wenn Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

6. Wählen Sie **Fertig**.

Die neue Taste wird auf der Seite eigene Zugriffsschlüssel angezeigt.

7. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie optional die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen. Siehe "[Klonen von S3-Zugriffsschlüsseln mithilfe der API](#)".

Die S3-Zugriffsschlüssel anzeigen

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie eine Liste Ihrer S3-Zugriffsschlüssel anzeigen. Sie können die Liste nach Ablauf der Zeit sortieren, sodass Sie feststellen können, welche Schlüssel bald ablaufen. Nach Bedarf können Sie "[Erstellen Sie neue Schlüssel](#)" Oder "[Schlüssel löschen](#)" Die Sie nicht mehr verwenden.



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die eigenen S3-Anmeldeinformationen verwalten verfügt "[Berechtigung](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.
2. Sortieren Sie auf der Seite Meine Zugriffsschlüssel alle vorhandenen Zugriffsschlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie nach 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 mit der Verwendung der neuen Schlüssel beginnen, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Löschen Ihrer eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten. Siehe "[Mandantenmanagement-Berechtigungen](#)".



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.
2. Aktivieren Sie auf der Seite Meine Zugriffsschlüssel das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie entfernen möchten.
3. Wählen Sie * Taste löschen*.
4. Wählen Sie im Bestätigungsdialogfeld **Delete key**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.

Erstellen Sie die S3-Zugriffstasten eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie S3-Zugriffsschlüssel für andere Benutzer erstellen, beispielsweise Applikationen, die Zugriff auf Buckets und Objekte benötigen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Über diese Aufgabe

Sie können einen oder mehrere S3-Zugriffsschlüssel für andere Benutzer erstellen und managen, damit sie 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 demnächst ablaufen, erstellen Sie einen neuen Schlüssel, bevor der alte Schlüssel abläuft, und löschen Sie dann den alten Schlüssel.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder keinen Ablauf haben. Beachten Sie die folgenden Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für die Schlüssel fest, um den Zugriff des Benutzers auf einen bestimmten Zeitraum zu beschränken. Durch das Festlegen einer kurzen Ablaufzeit kann das Risiko verringert werden, wenn die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel versehentlich ausgesetzt sind. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie keine periodischen neuen Schlüssel erstellen müssen, müssen Sie keine Ablaufzeit für die Schlüssel festlegen. Wenn Sie sich zu einem späteren Zeitpunkt für die Erstellung neuer Schlüssel entscheiden, löschen Sie die alten Schlüssel manuell.



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Wählen Sie den Benutzer aus, dessen S3-Zugriffsschlüssel Sie managen möchten.

Die Seite mit den Benutzerdetails wird angezeigt.

3. Wählen Sie **Zugriffstasten**, und wählen Sie dann **Schlüssel erstellen**.
4. Führen Sie einen der folgenden Schritte aus:
 - Wählen Sie **Keine Ablaufzeit einstellen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)

- Wählen Sie **Verfallszeit festlegen**, und legen Sie das Ablaufdatum und die Uhrzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Verfallszeit kann mindestens eine Minute von der aktuellen Zeit entfernt sein.

5. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld Zugriffsschlüssel herunterladen wird angezeigt, in dem die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel aufgeführt sind.

6. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.



Schließen Sie dieses Dialogfeld erst, wenn 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 Seite mit den Benutzerdetails angezeigt.

8. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie optional die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen. Siehe "[Klonen von S3-Zugriffsschlüsseln mithilfe der API](#)".

Zeigen Sie die S3-Zugriffstasten eines anderen Benutzers an

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 Ablauf der Zeit sortieren, sodass Sie feststellen können, welche Schlüssel bald ablaufen. Nach Bedarf können Sie neue Schlüssel erstellen und Schlüssel löschen, die nicht mehr verwendet werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

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 mit den Benutzerdetails **Zugriffstasten** aus.
4. Sortieren Sie die Tasten nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
5. Erstellen Sie bei Bedarf neue Schlüssel und löschen Sie manuell die nicht mehr verwendeten Schlüssel.

Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, kann der Benutzer mit der Verwendung der neuen Schlüssel beginnen, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Verwandte Informationen

["Erstellen von S3-Zugriffsschlüsseln eines anderen Benutzers"](#)

["Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers"](#)

Löschen Sie die S3-Zugriffstasten eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung. Siehe ["Mandantenmanagement-Berechtigungen"](#).



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

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 mit den Benutzerdetails **Zugriffsschlüssel** aus, und aktivieren Sie dann das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie löschen möchten.
4. Wählen Sie **Aktionen > Ausgewählte Taste löschen**.
5. Wählen Sie im Bestätigungsdialogfeld **Delete key**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.

Management von S3-Buckets

Erstellen eines S3-Buckets

Sie können im Mandanten-Manager S3-Buckets für Objektdaten erstellen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den Root-Zugriff oder Alle Buckets verwalten verfügt "[Berechtigung](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.



Berechtigungen zum Festlegen oder Ändern der S3-Objektsperrereigenschaften von Buckets oder Objekten können von erteilt werden "[Bucket-Richtlinie oder Gruppenrichtlinie](#)".

- Wenn Sie die S3-Objektsperrung für einen Bucket aktivieren möchten, hat ein Grid-Administrator die globale S3-Objektsperrung für das StorageGRID-System aktiviert, und Sie haben die Anforderungen für S3-Objektsperrbuckets und -Objekte geprüft. Siehe "[Verwenden Sie S3 Objektsperrung, um Objekte beizubehalten](#)".

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie **Eimer erstellen**.

Geben Sie Details ein

Schritte

1. Geben Sie Details für den Bucket ein.

Feld	Beschreibung
Bucket-Name	<p>Ein Name für den Bucket, der die folgenden Regeln erfüllt:</p> <ul style="list-style-type: none">• Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos).• Muss DNS-konform sein.• Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten.• Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden.• Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. <p>Weitere Informationen finden Sie im "Dokumentation der Amazon Web Services (AWS) zu den Bucket-Benennungsregeln".</p> <p>Hinweis: Sie können den Bucket-Namen nicht ändern, nachdem Sie den Bucket erstellt haben.</p>

Feld	Beschreibung
Region	<p>Der Bereich des Eimers.</p> <p>Der StorageGRID-Administrator managt die verfügbaren Regionen. Die Regionen eines Buckets können die Datensicherungsrichtlinie, die auf Objekte angewendet wird, beeinflussen. Standardmäßig werden alle Buckets im erstellt <code>us-east-1</code> Werden.</p> <p>Hinweis: Sie können die Region nicht ändern, nachdem Sie den Bucket erstellt haben.</p>

2. Wählen Sie **Weiter**.

Verwalten von Objekteinstellungen

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 nach Bedarf frühere Versionen eines Objekts abrufen. Sie müssen die Objektversionierung aktivieren, wenn der Bucket für die Grid-übergreifende Replizierung verwendet wird.

2. Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können Sie optional S3 Object Lock für den Bucket aktivieren, um Objekte mithilfe eines WORM-Modells (Write-Once-Read-Many) zu speichern.

Aktivieren Sie die S3-Objektsperre für einen Bucket nur, wenn Objekte z. B. für eine bestimmte Zeit aufbewahrt werden müssen, um bestimmte gesetzliche Vorgaben zu erfüllen. S3 Object Lock ist eine permanente Einstellung, mit der Sie verhindern können, dass Objekte für einen festgelegten Zeitraum oder für einen unbegrenzten Zeitraum gelöscht oder überschrieben werden.



Nachdem die S3-Objektsperre für einen Bucket aktiviert ist, kann sie nicht deaktiviert werden. Jeder mit den richtigen Berechtigungen kann diesem Bucket Objekte hinzufügen, die nicht geändert werden können. Sie können diese Objekte oder den Bucket selbst möglicherweise nicht löschen.

Wenn Sie S3 Object Lock für einen Bucket aktivieren, wird die Bucket-Versionierung automatisch aktiviert.

3. Wenn Sie **S3 Object Lock aktivieren** ausgewählt haben, aktivieren Sie optional **Default Retention** für diesen Bucket.

Wenn **Default Retention** aktiviert ist, werden neue Objekte, die dem Bucket hinzugefügt werden, automatisch vor dem Löschen oder Überschreiben geschützt. Die Einstellung **Default Retention** gilt nicht für Objekte mit eigenen Aufbewahrungsfristen.

a. Wenn **Default Retention** aktiviert ist, geben Sie einen **Default Retention Mode** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Compliance	<ul style="list-style-type: none"> • Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
Governance	<ul style="list-style-type: none"> • Benutzer mit <code>s3:BypassGovernanceRetention</code> Berechtigung kann den verwenden <code>x-amz-bypass-governance-retention: true</code> Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

b. Wenn **Default Retention** aktiviert ist, geben Sie die **Default Retention Period** für den Bucket an.

Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert zwischen 1 und 36,500 Tagen oder zwischen 1 und 100 Jahren an, einschließlich.

4. Wählen Sie **Eimer erstellen**.

Der Bucket wird erstellt und der Tabelle auf der Seite Buckets hinzugefügt.

5. Wählen Sie optional **Gehe zur Seite mit den Bucket-Details** zu "[Bucket-Details anzeigen](#)" Und zusätzliche Konfiguration durchführen.

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto anzeigen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite „Buckets“ wird angezeigt.

2. Überprüfen Sie die Zusammenfassungsinformationen für jeden Bucket.

Bei Bedarf können Sie die Informationen nach einer beliebigen Spalte sortieren oder Sie können die Seite vorwärts und zurück durch die Liste blättern.



Die angezeigten Werte für Objektanzahl und verwendeter Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen. Wenn Buckets die Versionierung aktiviert ist, sind gelöschte Objektversionen in der Objektanzahl enthalten.

Spalte	Beschreibung
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	Gibt an, ob S3 Object Lock für den Bucket aktiviert ist. Diese Spalte wird nur angezeigt, wenn die S3-Objektsperre für das Raster aktiviert ist. In dieser Spalte werden außerdem Informationen für alle Buckets angezeigt, die für die Konformität mit älteren Daten verwendet wurden.
Region	Der Bereich des Eimers, der nicht geändert werden kann.
Objektanzahl	Die Anzahl der Objekte in diesem Bucket. Wenn Objekte hinzugefügt oder gelöscht werden, wird dieser Wert möglicherweise nicht sofort aktualisiert. Wenn für Buckets die Versionierung aktiviert ist, sind nicht aktuelle Objektversionen in diesem Wert enthalten.
Belegten Speicherplatz	Die logische Größe aller Objekte im Bucket Die logische Größe umfasst nicht den tatsächlich benötigten Speicherplatz für replizierte oder Erasure Coding-Kopien oder für Objekt-Metadaten.
Erstellungsdatum	Datum und Uhrzeit der Erstellung des Buckets.

3. Um Details für einen bestimmten Bucket anzuzeigen, wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt. Auf dieser Seite können Sie die folgenden Aufgaben ausführen:

- Konfigurieren und Managen von Bucket-Optionen wie z. B. "[Konsistenzstufe](#)", "[Aktualisierung der Uhrzeit des letzten Zugriffs](#)", "[Objektversionierung](#)", "[S3-Objektsperre](#)" Und "[Standardmäßige Bucket-Aufbewahrung](#)"
- Konfigurieren Sie den Bucket-Zugriff, z. B. "[Cross-Origin Resource Sharing \(CORS\)](#)"
- Managen "[Plattform-Services](#)" (Falls für den Mandanten erlaubt), einschließlich Replikation, Ereignisbenachrichtigungen und Suchintegration
- Aktivieren Sie und "[Grid-übergreifende Replizierung managen](#)" (Falls dies für den Mandanten zulässig ist) zum Replizieren von Objekten, die in diesen Bucket aufgenommen wurden, auf ein anderes StorageGRID-System
- Auf das zugreifen "[Experimentelle S3-Konsole](#)" Zum Verwalten der Objekte im Bucket
- "[Löschen aller Objekte in einem Bucket](#)"
- "[Löschen eines Buckets](#)" Das ist bereits leer

Ändern der Konsistenzstufe eines Buckets

Wenn Sie einen S3-Mandanten verwenden, können Sie die Konsistenzstufe für Vorgänge ändern, die für die Objekte in S3-Buckets ausgeführt werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Konsistenzkontrollen bieten ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg. Im Allgemeinen sollten Sie für Ihre Buckets die Konsistenzstufe **Read-after-New-write** verwenden.

Wenn die Konsistenzstufe **Read-after-New-write** nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenzstufe ändern, indem Sie die Bucket-Konsistenzstufe oder die verwenden `Consistency-Control` Kopfzeile. Der `Consistency-Control` Kopfzeile setzt die Bucket-Konsistenzstufe außer Kraft.



Wenn Sie die Konsistenzstufe eines Buckets ändern, werden nur die Objekte, die nach der Änderung aufgenommen werden, garantiert, um die überarbeitete Ebene zu erfüllen.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Consistency Level** aus.
4. Wählen Sie eine Konsistenzstufe für Operationen aus, die an den Objekten in diesem Bucket durchgeführt werden.
 - **All**: Bietet die höchste Konsistenz. Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
 - **Strong-global**: Garantiert Lese-nach-Schreiben-Konsistenz für alle Client-Anfragen über alle Standorte hinweg.
 - **Strong-site**: Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.
 - **Read-after-New-write** (default): Bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
 - **Verfügbar**: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.
5. Wählen Sie **Änderungen speichern**.

Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit

Wenn Grid-Administratoren die Regeln für das Information Lifecycle Management (ILM)

für ein StorageGRID-System erstellen, können sie optional angeben, dass die letzte Zugriffszeit eines Objekts verwendet wird, um zu bestimmen, ob das Objekt auf einen anderen Storage-Standort verschoben werden soll. Wenn Sie einen S3-Mandanten verwenden, können Sie diese Regeln nutzen, indem Sie Updates 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 **Letzte Zugriffszeit** als erweiterten Filter oder als Referenzzeit verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System eine solche Regel nicht enthält. Siehe "[Verwenden Sie die letzte Zugriffszeit in ILM-Regeln](#)" Entsprechende Details.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Letzte Zugriffszeit ist eine der Optionen für die **Referenzzeit**-Platzierungsanweisung für eine ILM-Regel. Durch Festlegen der Referenzzeit für eine Regel auf Letzte Zugriffszeit können Grid-Administratoren festlegen, dass Objekte an bestimmten Speicherorten platziert werden, basierend auf dem Zeitpunkt, zu dem diese Objekte zuletzt abgerufen (gelesen oder angezeigt) wurden.

Um z. B. sicherzustellen, dass kürzlich angezeigte Objekte im schnelleren Storage verbleiben, kann ein Grid-Administrator eine ILM-Regel erstellen, die Folgendes angibt:

- Objekte, die im letzten Monat abgerufen wurden, sollten auf lokalen Speicherknotten verbleiben.
- Objekte, die im letzten Monat nicht abgerufen wurden, sollten an einen externen Standort verschoben werden.

Standardmäßig werden Updates zur letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option **Uhrzeit des letzten Zugriffs** verwendet, und Sie möchten, dass diese Option auf Objekte in diesem Bucket angewendet wird, müssen Sie für die in dieser Regel angegebenen S3-Buckets Updates für den letzten Zugriff aktivieren.



Durch das Aktualisieren der letzten Zugriffszeit, zu der ein Objekt abgerufen wird, kann sich die StorageGRID-Performance insbesondere für kleine Objekte reduzieren.

Eine Performance-Beeinträchtigung wird durch die letzten Updates der Zugriffszeit beeinflusst, da StorageGRID jedes Mal, wenn Objekte abgerufen werden, die folgenden zusätzlichen Schritte durchführen muss:

- Aktualisieren Sie die Objekte mit neuen Zeitstempel
- Fügen Sie die Objekte zur ILM-Warteschlange hinzu, damit sie anhand aktueller 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, wenn die letzte Zugriffszeit aktiviert ist	
	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?
Anforderung zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Nein	Ja.	Ja.
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	<ul style="list-style-type: none"> • Nein, für die Quellkopie • Ja, für die Zielkopie 	<ul style="list-style-type: none"> • Nein, für die Quellkopie • Ja, für die Zielkopie 	<ul style="list-style-type: none"> • Ja, für die Quellkopie • Ja, für die Zielkopie 	<ul style="list-style-type: none"> • Ja, für die Quellkopie • Ja, für die Zielkopie
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Letzte Zugriffszeit-Updates** aus.
4. Aktivieren oder deaktivieren Sie die Zeitaktualisierungen für den letzten Zugriff.
5. Wählen Sie **Änderungen speichern**.

Ändern Sie die Objektversionierung für einen Bucket

Wenn Sie einen S3-Mandanten verwenden, können Sie den Versionsstatus für S3-Buckets ändern.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".

- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Sie können die Objektversionierung für einen Bucket aktivieren oder aussetzen. Nachdem Sie die Versionierung für einen Bucket aktiviert haben, kann dieser nicht in den Status „unversioniert“ zurückkehren. Sie können die Versionierung für den Bucket jedoch unterbrechen.

- Deaktiviert: Versionierung wurde noch nie aktiviert
- Aktiviert: Versionierung ist aktiviert
- Suspendiert: Die Versionierung war zuvor aktiviert und wird ausgesetzt

Weitere Informationen finden Sie im Folgenden:

- "[Objektversionierung](#)"
- "[ILM-Regeln und Richtlinien für versionierte S3-Objekte \(Beispiel 4\)](#)"
- "[So werden Objekte gelöscht](#)"

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Object Versioning** aus.
4. Wählen Sie einen Versionierungsstatus für die Objekte in diesem Bucket aus.

Die Objektversionierung muss für einen Bucket aktiviert bleiben, der für die Grid-übergreifende Replizierung verwendet wurde. Wenn die S3-Objektsperre oder die ältere Compliance aktiviert ist, sind die Optionen **Objektversionierung** deaktiviert.

Option	Beschreibung
Aktivieren Sie die Versionierung	Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann nach Bedarf frühere Versionen eines Objekts abrufen. Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.
Die Versionierung unterbrechen	Unterbrechen Sie die Objektversionierung, wenn Sie keine neuen Objektversionen mehr erstellen möchten. Sie können weiterhin alle vorhandenen Objektversionen abrufen.

5. Wählen Sie **Änderungen speichern**.

Verwenden Sie S3 Objektsperre, um Objekte beizubehalten

Sie können S3 Object Lock verwenden, wenn Buckets und Objekte die gesetzlichen

Aufbewahrungsanforderungen erfüllen müssen.

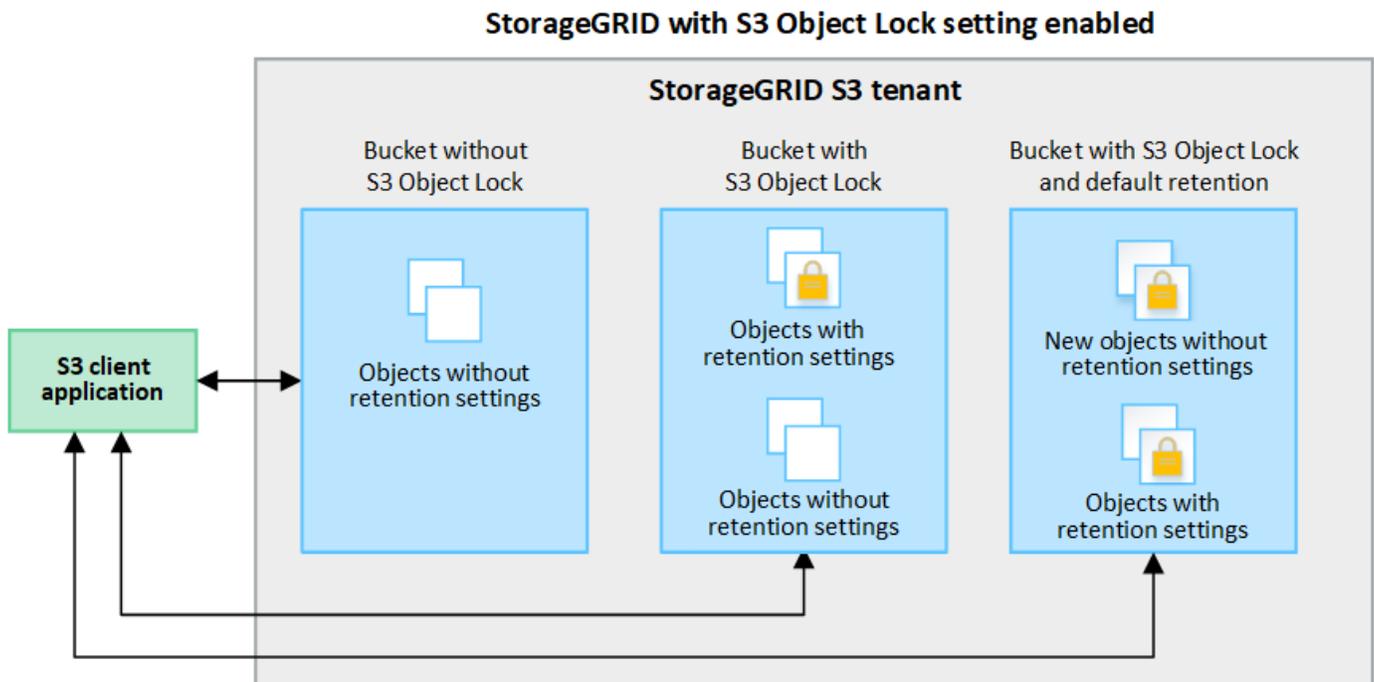
Was ist S3 Object Lock?

Die Funktion StorageGRID S3 Object Lock ist eine Objektschutzlösung, die der S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

Wenn die globale S3-Objektsperre für ein StorageGRID-System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn für einen Bucket die S3 Object Lock aktiviert ist, ist die Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Wenn für einen Bucket die S3 Object Lock aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion angeben, die in diesem Bucket gespeichert ist.

Darüber hinaus kann für einen Bucket, auf dem die S3 Object Lock aktiviert ist, optional ein Standardaufbewahrungsmodus und ein Aufbewahrungszeitraum verwendet werden. Die Standardeinstellungen gelten nur für Objekte, die ohne eigene Aufbewahrungseinstellungen zum Bucket hinzugefügt werden.



Aufbewahrungsmodi

Die Objektsperrefunktion StorageGRID S3 unterstützt zwei Aufbewahrungsmodi, um verschiedene Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Amazon S3 Aufbewahrungsmodi.

- Im Compliance-Modus:
 - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
 - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
 - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
 - Benutzer mit besonderer Berechtigung können in Anfragen einen Überbrückungskopf verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.

- Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
- Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mithilfe der S3-Client-Applikation optional die folgenden Aufbewahrungseinstellungen für jedes Objekt angeben, das dem Bucket hinzugefügt wird:

- **Retention Mode:** Entweder Compliance oder Governance.
- **Rebeat-until-date:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Legal Hold:** Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflicht hat kein Ablaufdatum, bleibt aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.



Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Weitere Informationen zu den Objekteinstellungen finden Sie unter ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

Standardeinstellung für die Aufbewahrung von Buckets

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wurde, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Default Retention Mode:** Entweder Compliance oder Governance.
- **Default Retention Period:** Wie lange neue Objektversionen, die zu diesem Bucket hinzugefügt wurden, beibehalten werden sollen, beginnend mit dem Tag, an dem sie hinzugefügt werden.

Die Standard-Bucket-Einstellungen gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Vorhandene Bucket-Objekte werden nicht beeinflusst, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

Siehe ["Erstellen eines S3-Buckets"](#) und ["Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung"](#).

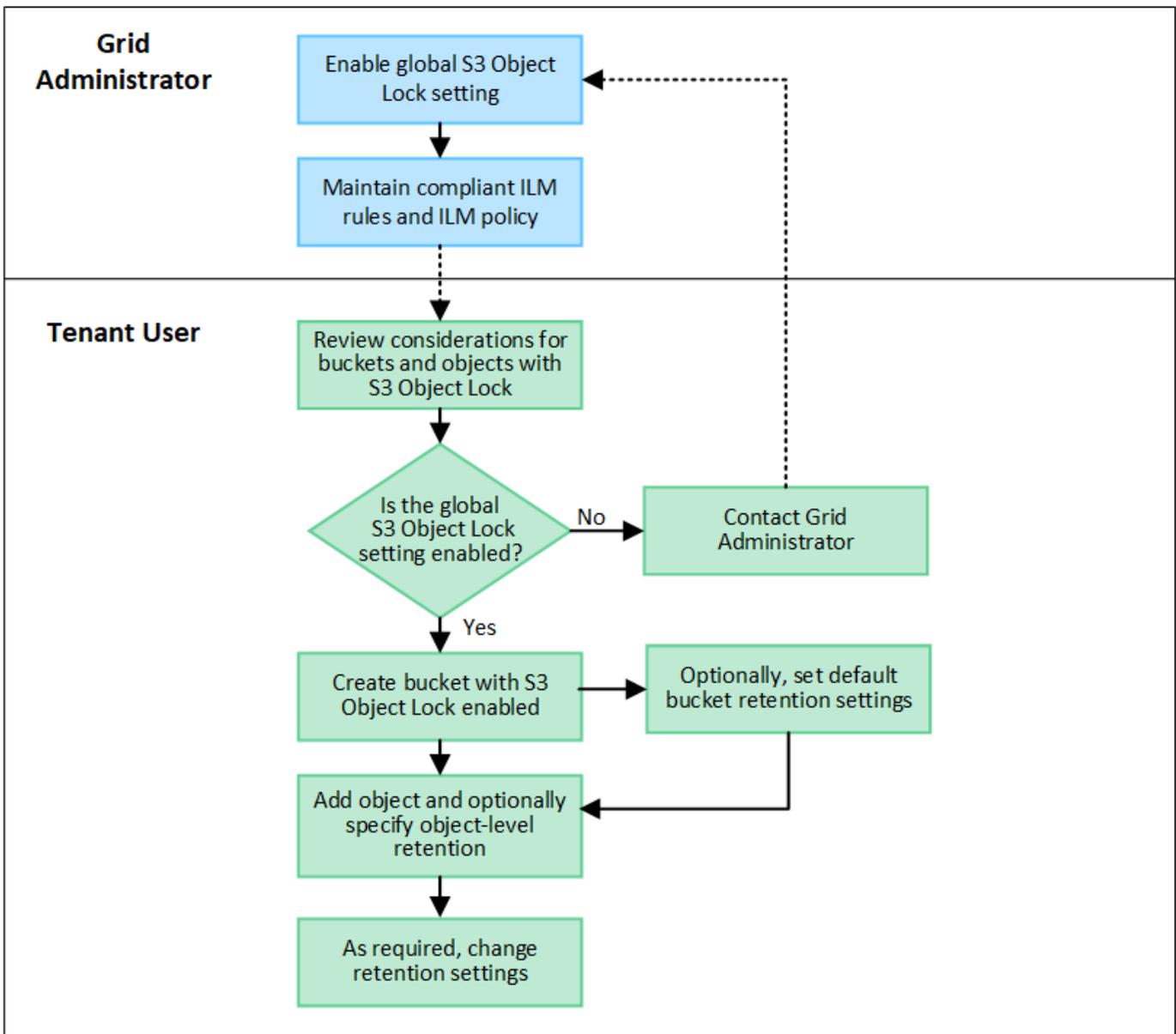
S3-Objektsperre-Workflow

Das Workflow-Diagramm zeigt die grundlegenden Schritte zur Verwendung der S3-Objektsperre in StorageGRID.

Bevor Sie Buckets mit aktivierter S3-Objektsperre erstellen können, muss der Grid-Administrator die globale S3-Objektsperreinstellung für das gesamte StorageGRID-System aktivieren. Der Grid-Administrator muss außerdem sicherstellen, dass die Richtlinie für das Information Lifecycle Management (ILM) „konform“ ist; sie muss die Anforderungen von Buckets erfüllen, wenn S3 Object Lock aktiviert ist. Weitere Informationen erhalten Sie von Ihrem Grid-Administrator oder in den Anweisungen für ["Managen von Objekten mit S3 Object Lock"](#).

Nachdem die globale S3 Object Lock-Einstellung aktiviert wurde, können Sie Buckets erstellen, für die S3

Object Lock aktiviert ist, und optional für jeden Bucket Standardaufbewahrungseinstellungen festlegen. Darüber hinaus können Sie mit der S3-Client-Anwendung optional Aufbewahrungseinstellungen für jede Objektversion angeben.



Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktivierter S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.
- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket. Sie können S3 Object Lock nicht deaktivieren oder die Versionierung für den Bucket nicht unterbrechen.
- Optional können Sie mithilfe von Tenant Manager, der Mandanten-Management-API oder der S3-REST-API für jeden Bucket einen Standardaufbewahrungsmodus und einen Aufbewahrungszeitraum angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket

hinzugefügt wurden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen außer Kraft setzen, indem Sie einen Aufbewahrungsmodus und das Aufbewahrungsdatum für jede Objektversion festlegen, wenn sie hochgeladen wird.

- Die Konfiguration des Bucket-Lebenszyklus wird für Buckets unterstützt, für die S3 Object Lock aktiviert ist.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

Anforderungen für Objekte in Buckets, bei denen die S3-Objektsperre aktiviert ist

- Zum Schutz einer Objektversion können Sie Standardaufbewahrungseinstellungen für den Bucket angeben oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mit der S3-Client-Applikation oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

Jedes in einem Bucket gespeicherte Objekt mit aktivierter S3 Object Lock durchlaufen die folgenden Phasen:

1. Objektaufnahme

Wenn einem Bucket eine Objektversion hinzugefügt wird, für die S3 Object Lock aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

- Wenn für das Objekt Aufbewahrungseinstellungen angegeben werden, werden die Einstellungen auf Objektebene angewendet. Alle standardmäßigen Bucket-Einstellungen werden ignoriert.
- Wenn für das Objekt keine Aufbewahrungseinstellungen angegeben sind, werden die Standard-Bucket-Einstellungen angewendet, sofern diese vorhanden sind.
- Wenn für das Objekt oder den Bucket keine Aufbewahrungseinstellungen angegeben wurden, ist das Objekt nicht durch S3 Object Lock geschützt.

Wenn Aufbewahrungseinstellungen angewendet werden, sind sowohl das Objekt als auch alle benutzerdefinierten S3-Metadaten geschützt.

2. Objektaufbewahrung und -Löschung

Von jedem geschützten Objekt werden innerhalb StorageGRID des angegebenen Aufbewahrungszeitraums mehrere Kopien gespeichert. Die genaue Anzahl und Art der Objektkopien sowie der Speicherort werden durch die konformen Regeln der aktiven ILM-Richtlinie bestimmt. Ob ein geschütztes Objekt gelöscht werden kann, bevor das Aufbewahrungsdatum erreicht ist, hängt vom Aufbewahrungsmodus ab.

- Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Kann ich auch ältere konforme Buckets verwalten?

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Wenn Sie mithilfe einer früheren Version von StorageGRID konforme Buckets 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: Management älterer, konformer Buckets für StorageGRID 11.5"].

Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung

Wenn Sie beim Erstellen des Buckets die S3-Objektsperre aktiviert haben, können Sie den Bucket bearbeiten, um die Standardeinstellungen für die Aufbewahrung zu ändern. Sie können die Standardaufbewahrung aktivieren (oder deaktivieren) und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer festlegen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Objektsperre ist global für Ihr StorageGRID-System aktiviert; Sie haben S3 Objektsperre bei Erstellung des Buckets aktiviert. Siehe "[Verwenden Sie S3 Objektsperre, um Objekte beizubehalten](#)".

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **S3 Object Lock** aus.
4. Aktivieren oder deaktivieren Sie optional **Default Retention** für diesen Bucket.

Änderungen an dieser Einstellung gelten nicht für Objekte, die bereits im Bucket vorhanden sind, oder für Objekte, die möglicherweise eigene Aufbewahrungsfristen haben.

5. Wenn **Default Retention** aktiviert ist, geben Sie einen **Default Retention Mode** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Compliance	<ul style="list-style-type: none">• Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.• Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.• Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.

Standardaufbewahrungsmodus	Beschreibung
Governance	<ul style="list-style-type: none"> • Benutzer mit <code>s3:BypassGovernanceRetention</code> Berechtigung kann den verwenden <code>x-amz-bypass-governance-retention: true</code> Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

6. Wenn **Default Retention** aktiviert ist, geben Sie die **Default Retention Period** für den Bucket an.

Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert zwischen 1 und 36,500 Tagen oder zwischen 1 und 100 Jahren an, einschließlich.

7. Wählen Sie **Änderungen speichern**.

Konfiguration der Cross-Origin Resource Sharing (CORS)

Sie können CORS (Cross-Origin Resource Sharing) für einen S3-Bucket konfigurieren, wenn Webapplikationen in anderen Domänen auf diesen Bucket und die Objekte in diesem Bucket zugreifen sollen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

CORS (Cross-Origin Resource Sharing) ist ein Sicherheitsmechanismus, mit dem Client-Webanwendungen in einer Domäne auf Ressourcen in einer anderen Domäne zugreifen können. Angenommen, Sie verwenden einen S3-Bucket mit dem Namen `Images` Zum Speichern von Grafiken. Durch Konfigurieren von CORS für das `Images` Bucket: Sie können zulassen, dass die Bilder in diesem Bucket auf der Website angezeigt werden `http://www.example.com`.

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um die erforderliche XML zu erstellen.

Dieses Beispiel zeigt die XML, die zur Aktivierung von CORS für einen S3-Bucket verwendet wird. Mit dieser XML-Datei kann jede Domäne GET-Anforderungen an den Bucket senden, es erlaubt jedoch nur das `http://www.example.com` Domain zum Senden VON POST- und LÖSCHEN von Anfragen. Alle Anfragezeilen 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 Developer Guide"](#).

2. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
3. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie auf der Registerkarte **Bucket Access** 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 **Clear**, um von vorne zu beginnen.
2. Wählen Sie **Änderungen speichern**.

Deaktivieren Sie die CORS-Einstellung

Schritte

1. Deaktivieren Sie das Kontrollkästchen **CORS aktivieren**.
2. Wählen Sie **Änderungen speichern**.

Löschen von Objekten in Bucket

Sie können den Tenant Manager verwenden, um die Objekte in einem oder mehreren Buckets zu löschen.

Überlegungen und Anforderungen

Bevor Sie diese Schritte durchführen, beachten Sie Folgendes:

- Wenn Sie die Objekte in einem Bucket löschen, entfernt StorageGRID endgültig alle Objekte und alle Objektversionen in jedem ausgewählten Bucket von allen Nodes und Standorten im StorageGRID System. StorageGRID entfernt auch alle zugehörigen Objekt-Metadaten. 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 hat "[S3-Objektsperre aktiviert](#)", Kann es im Zustand **delete objects: Read-only** für *years* bleiben.



Ein Bucket, der S3 Object Lock verwendet, bleibt im Zustand **delete Objects: Read-only**, bis das Aufbewahrungsdatum für alle Objekte erreicht ist und alle Legal Holds entfernt werden.

- Während Objekte gelöscht werden, ist der Zustand des Buckets **delete objects: Read-only**. In diesem Status können Sie dem Bucket keine neuen Objekte hinzufügen.
- Nachdem alle Objekte gelöscht wurden, verbleibt der Bucket im schreibgeschützten Status. Sie haben folgende Möglichkeiten:
 - Versetzen Sie den Bucket in den Schreibmodus und verwenden Sie ihn für neue Objekte wieder
 - Löschen Sie den Bucket
 - Belassen Sie den Bucket im schreibgeschützten Modus, um seinen Namen für eine zukünftige Verwendung zu reservieren
- Wenn für einen Bucket die Objektversionierung aktiviert ist, werden alle Löschmarkierungen, die sich beim Starten dieser Schritte im Bucket befinden, nicht durch den Vorgang „Objekte löschen“ entfernt. Wenn Sie einen versionierten Bucket löschen möchten, nachdem alle Objekte gelöscht wurden, müssen Sie alle bereits vorhandenen Löschmarkierungen entfernen.
- Wenn Sie verwenden "[Grid-übergreifende Replizierung](#)", Beachten Sie Folgendes:
 - Mit dieser Option werden keine Objekte aus dem Bucket auf dem anderen Raster gelöscht.
 - Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **gitterübergreifender Replikationsfehler** ausgelöst, wenn Sie dem Ziel-Bucket auf dem anderen Grid Objekte hinzufügen. Wenn Sie nicht garantieren können, dass niemand dem Bucket auf dem anderen Raster Objekte hinzufügen wird, "[Deaktivieren Sie die Grid-übergreifende Replizierung](#)" Für diesen Bucket, bevor alle Bucket-Objekte gelöscht werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)". Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.

2. Verwenden Sie das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket.

Menü „Aktionen“

- Aktivieren Sie das Kontrollkästchen für jeden Bucket, aus dem Sie Objekte löschen möchten.
- Wählen Sie **actions > Delete objects in bucket**.

Detailseite

- Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.
- Wählen Sie **Objekte im Bucket löschen**.

- Wenn das Bestätigungdialogfeld angezeigt wird, überprüfen Sie die Details, geben Sie **Ja** ein und wählen Sie **OK**.
- Warten Sie, bis der Löschvorgang beginnt.

Nach ein paar Minuten:

- Auf der Seite mit den Bucket-Details wird ein gelbes Statusbanner angezeigt. Der Fortschrittsbalken gibt an, wie viel Prozent der Objekte gelöscht wurden.
- (read-only)** erscheint nach dem Namen des Buckets auf der Seite mit den Bucket-Details.
- (Objekte löschen: Schreibgeschützt)** erscheint neben dem Namen des Buckets auf der Buckets-Seite.

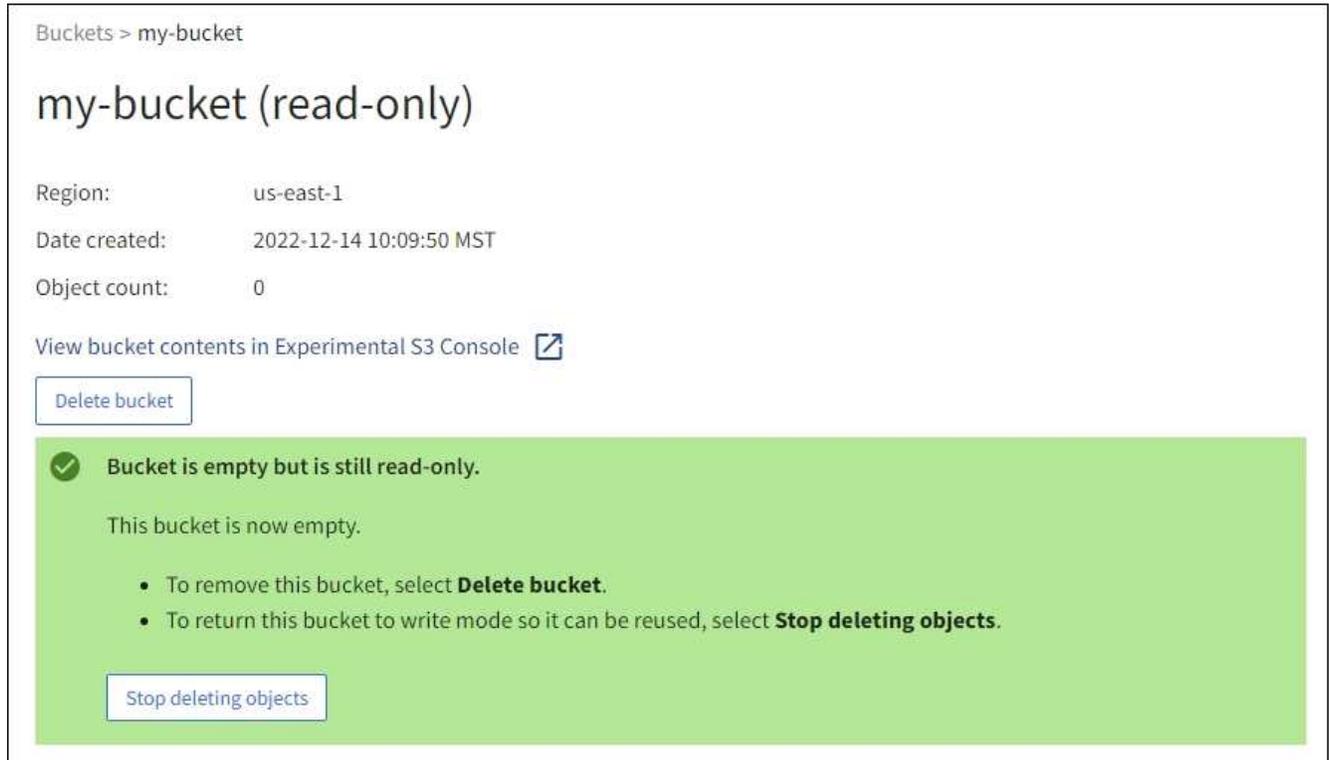
The screenshot shows the AWS S3 console interface for a bucket named 'my-bucket'. The breadcrumb navigation is 'Buckets > my-bucket'. A green success banner at the top right reads 'Success Starting to delete objects from one bucket.' The bucket name 'my-bucket' is followed by '(read-only)' in yellow text. Below this, the bucket details are listed: Region: us-east-1, Date created: 2022-12-14 10:09:50 MST, and Object count: 3. There is a link to 'View bucket contents in Experimental S3 Console' with an external link icon. A 'Delete bucket' button is visible. A large yellow warning banner with a triangle icon contains the text: 'All bucket objects are being deleted. StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select Stop deleting objects. You cannot restore objects that have already been deleted.' Below this banner is a progress bar showing '0% (0 of 3 objects deleted)' and a 'Stop deleting objects' button.

- Wählen Sie, wie erforderlich, während der Vorgang ausgeführt wird, **Löschen von Objekten stoppen**, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Prozess fortzusetzen.

Wenn Sie **Löschen von Objekten stoppen** auswählen, wird der Bucket in den Schreibmodus zurückversetzt. Sie können jedoch nicht auf 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 weiterhin schreibgeschützt.



Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1
Date created: 2022-12-14 10:09:50 MST
Object count: 0

[View bucket contents in Experimental S3 Console](#)

Delete bucket

✓ **Bucket is empty but is still read-only.**

This bucket is now empty.

- To remove this bucket, select **Delete bucket**.
- To return this bucket to write mode so it can be reused, select **Stop deleting objects**.

Stop deleting objects

7. Führen Sie einen der folgenden Schritte aus:

- Schließen Sie die Seite, um den Bucket im schreibgeschützten Modus zu belassen. Beispielsweise können Sie einen leeren Bucket im schreibgeschützten Modus belassen, um den Bucket-Namen für die zukünftige Verwendung zu reservieren.
- Löschen Sie den Bucket. Sie können **Eimer löschen** auswählen, um einen einzelnen Eimer zu löschen, oder die Buckets-Seite zurücksenden und **Aktionen** > *Eimer löschen auswählen, um mehr als einen Eimer zu entfernen.



Wenn Sie einen versionierten Bucket nicht löschen können, nachdem alle Objekte gelöscht wurden, bleiben möglicherweise Löschmarkierungen erhalten. Um den Bucket zu löschen, müssen Sie alle verbleibenden Löschmarkierungen entfernen.

- Versetzen Sie den Bucket in den Schreibmodus und verwenden Sie ihn optional für neue Objekte wieder. Sie können für einen einzelnen Bucket **Stop delete objects** auswählen oder zur Buckets-Seite zurückkehren und für mehr als einen Bucket **Action** > **Stop delete objects** auswählen.

S3-Bucket löschen

Mit dem Tenant Manager können Sie eine oder mehrere leere S3-Buckets löschen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet **"Unterstützter Webbrowser"**.
- Sie gehören einer Benutzergruppe an, die über den verfügt **"Managen aller Buckets oder Root-Zugriffsberechtigungen"**. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen-

oder Bucket-Richtlinien.

- Die Buckets, die Sie löschen möchten, sind leer.

Über diese Aufgabe

Diese Anweisungen beschreiben das Löschen eines S3-Buckets mithilfe von Tenant Manager. Sie können auch S3-Buckets über löschen "[Mandantenmanagement-API](#)" Oder im "[S3-REST-API](#)".

Sie können einen S3-Bucket nicht löschen, wenn er Objekte, nicht aktuelle Objektversionen enthält oder Markierungen löscht. Informationen zum Löschen von S3-versionierten Objekten finden Sie unter "[So werden Objekte gelöscht](#)".

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.

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 **Actions > Eimer löschen**.

Detailseite

- a. Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.
- b. Wählen Sie **Eimer löschen**.

3. Wenn das Bestätigungsdialoefeld 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, wird eine Fehlermeldung angezeigt. Bevor Sie den Bucket löschen können, müssen Sie alle Objekte und alle Löschkennzeichnungen im Bucket löschen.

Verwenden Sie die Experimental S3-Konsole

Sie können die Objekte über die S3-Konsole in einem S3-Bucket anzeigen.

Sie können auch S3 Console verwenden, um folgende Aufgaben zu erledigen:

- Hinzufügen und Löschen von Objekten, Objektversionen und Ordnern
- Benennen Sie Objekte um
- Verschieben und Kopieren von Objekten zwischen Buckets und Ordnern
- Verwalten von Objekt-Tags
- Zeigen Sie Objektmetadaten an
- Objekte herunterladen



Die S3-Konsole ist als „experimentell“ gekennzeichnet, da sie noch nicht vollständig oder für die Verwendung in einer Produktionsumgebung freigegeben ist. Mandanten sollten die S3-Konsole nur verwenden, wenn sie Funktionen für eine kleine Anzahl von Objekten ausführen, z. B. beim Hochladen von Objekten zur Simulation einer neuen ILM-Richtlinie, bei der Fehlerbehebung von Ingest-Problemen oder bei der Verwendung von Proof-of-Concept- oder nicht-Production-Grids.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die Root-Zugriffsberechtigung verfügt oder die sowohl die Verwaltung aller Buckets als auch die Verwaltung von Objekten mit der S3-Konsole verfügt "[Berechtigungen](#)".



Benutzer, die über die Berechtigung zum Verwalten von Objekten mit S3-Konsole verfügen, aber nicht über die Berechtigung zum Verwalten aller Buckets verfügen, können dennoch direkt zur Experimental S3-Konsole navigieren.

- Sie haben einen Bucket erstellt.
- Für den Benutzer wurde eine S3-Gruppen- oder Bucket-Richtlinie konfiguriert.
- Sie kennen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers. Optional haben Sie eine `.csv` Datei mit diesen Informationen. Siehe "[Anweisungen zum Erstellen von Zugriffsschlüsseln](#)".

Schritte

1. Wählen Sie **Buckets**.
2. Wählen Sie [Experimental S3 Console](#) . Sie können auch über die Seite mit den Bucket-Details auf diesen Link zugreifen.
3. Fügen Sie auf der Anmeldeseite Experimental S3 Console die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Felder ein. Wählen Sie andernfalls * Zugriffsschlüssel hochladen* aus, und wählen Sie Ihr aus `.csv` Datei:
4. Wählen Sie **Anmelden**.
5. Objektmanagement nach Bedarf



Buckets > bucket-01

↑ bucket-01

<input type="checkbox"/>	Name	Logical space used	Last modified on
<input type="checkbox"/>	03_Grid_Primer_11.5.pdf	2.73 MB	2021-12-03 09:43:26 MST
<input type="checkbox"/>	04_Tenant_Users_Guide_11.5.pdf	1.07 MB	2021-12-03 09:44:24 MST
<input type="checkbox"/>	06_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
<input type="checkbox"/>	08_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
<input type="checkbox"/>	09_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:26 MST
<input type="checkbox"/>	10_Grid_Primer_11.5.pdf	2.8 MB	2021-12-03 09:43:27 MST

Select an object or folder to view its details.

Displaying 16 objects
Selected 0 objects

Management von S3-Plattform-Services

Was sind Plattform-Services?

Die StorageGRID Plattform-Services unterstützen Sie bei der Implementierung einer Hybrid-Cloud-Strategie, da Sie Ereignisbenachrichtigungen und Kopien von S3 Objekten und Objekt-Metadaten an externe Ziele senden können.

Falls die Verwendung von Plattform-Services für Ihr Mandantenkonto zulässig ist, können Sie die folgenden Services für jeden S3-Bucket konfigurieren:

- **CloudMirror-Replikation:** Verwenden "[StorageGRID CloudMirror Replikationsservice](#)" So spiegeln Sie bestimmte Objekte aus einem StorageGRID Bucket an ein angegebenes externes Ziel:

So können Sie beispielsweise CloudMirror Replizierung verwenden, um spezifische Kundendaten in Amazon S3 zu spiegeln und anschließend AWS Services für Analysen Ihrer Daten nutzen.



Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

- **Benachrichtigungen:** Verwenden "[Bucket-spezifische Ereignisbenachrichtigungen](#)" So senden Sie

Benachrichtigungen über bestimmte Aktionen, die an Objekten ausgeführt werden, an einen bestimmten externen Amazon Simple Notification Service™ (SNS).

Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.



Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

- **Suchintegrationservice:** Verwenden Sie die "[suchintegrations-Service](#)" Senden von S3-Objektmetadaten an einen angegebenen Elasticsearch-Index, bei dem die Metadaten über den externen Service durchsucht oder analysiert werden können.

Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.



Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperre metadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

Da der Zielspeicherort für Plattformservices normalerweise außerhalb Ihrer StorageGRID-Implementierung liegt, erhalten Sie bei Plattform-Services die Leistung und Flexibilität, die sich aus der Nutzung externer Storage-Ressourcen, Benachrichtigungsservices und Such- oder Analyseservices für Ihre Daten ergibt.

Jede Kombination von Plattform-Services kann für einen einzelnen S3-Bucket konfiguriert werden. Beispielsweise könnten Sie sowohl den CloudMirror-Service als auch Benachrichtigungen über einen StorageGRID S3-Bucket konfigurieren, damit Sie bestimmte Objekte auf den Amazon Simple Storage Service spiegeln können, während Sie gleichzeitig eine Benachrichtigung über jedes einzelne Objekt an eine Monitoring-Applikation eines Drittanbieters senden können, um Ihre AWS-Ausgaben zu verfolgen.



Die Nutzung von Plattfordiensten muss für jedes Mandantenkonto durch einen StorageGRID-Administrator aktiviert werden, der den Grid Manager oder die Grid Management API verwendet.

Die Konfiguration von Plattform-Services

Plattform-Services kommunizieren mit externen Endpunkten, die Sie über das konfigurieren "[Mandanten-Manager](#)" Oder im "[Mandantenmanagement-API](#)". Jeder Endpunkt stellt ein externes Ziel dar, beispielsweise einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein SNS-Thema (Simple Notification Service) oder ein lokal gehostetes Elasticsearch-Cluster, in AWS oder an anderer Stelle.

Nachdem Sie einen externen Endpunkt erstellt haben, können Sie einen Plattfordienst für einen Bucket aktivieren, indem Sie dem Bucket eine XML-Konfiguration hinzufügen. Die XML-Konfiguration identifiziert die Objekte, auf denen der Bucket handeln soll, die Aktion, die der Bucket durchführen sollte, und den Endpunkt, den der Bucket für den Service verwenden sollte.

Sie müssen für jeden Plattfordienst, den Sie konfigurieren möchten, separate XML-Konfigurationen hinzufügen. Beispiel:

- Wenn Sie alle Objekte wünschen, mit denen die Tasten beginnen /images Um in einen Amazon S3-Bucket repliziert werden zu können, müssen Sie dem Quell-Bucket eine Replizierungskonfiguration hinzufügen.
- Wenn Sie auch Benachrichtigungen senden möchten, wenn diese Objekte im Bucket gespeichert sind, müssen Sie eine Benachrichtigungskonfiguration hinzufügen.
- Wenn Sie die Metadaten für diese Objekte indizieren möchten, müssen Sie die Konfiguration für die Metadatenbenachrichtigung hinzufügen, die zur Implementierung der Suchintegration verwendet wird.

Das Format für die Konfigurations-XML wird durch die S3-REST-APIs geregelt, die zur Implementierung von StorageGRID Plattform-Services verwendet werden:

Plattform-Service	S3-REST-API
"Replizierung von CloudMirror"	<ul style="list-style-type: none"> • GET Bucket-Replizierung • PUT Bucket-Replizierung
"Benachrichtigungen"	<ul style="list-style-type: none"> • Bucket-Benachrichtigung ABRUFEN • PUT Bucket-Benachrichtigung
"Integration von Suchen"	<ul style="list-style-type: none"> • Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN • PUT Bucket-Metadaten-Benachrichtigungskonfiguration <p>Diese Vorgänge sind individuell für StorageGRID.</p>

Verwandte Informationen

["Überlegungen zu Plattformservices"](#)

["S3-REST-API VERWENDEN"](#)

CloudMirror Replikationsservice

Sie können die CloudMirror-Replizierung für einen S3-Bucket aktivieren, wenn StorageGRID bestimmte Objekte replizieren soll, die dem Bucket zu einem oder mehreren Ziel-Buckets hinzugefügt wurden.

Die CloudMirror Replizierung arbeitet unabhängig von der aktiven ILM-Richtlinie des Grid. Der CloudMirror-Service repliziert Objekte, sobald sie im Quell-Bucket gespeichert werden, und liefert sie so schnell wie möglich an den Ziel-Bucket. Die Bereitstellung replizierter Objekte wird ausgelöst, wenn die Objektaufnahme erfolgreich ist.



Die CloudMirror-Replizierung weist wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter ["Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung"](#).

Wenn Sie die CloudMirror-Replizierung für einen vorhandenen Bucket aktivieren, werden nur die neuen, zu diesem Bucket hinzugefügten Objekte repliziert. Alle vorhandenen Objekte in dem Bucket werden nicht repliziert. Um die Replizierung von vorhandenen Objekten zu erzwingen, können Sie die Metadaten des vorhandenen Objekts durch eine Objektkopie aktualisieren.



Wenn Sie zum Kopieren von Objekten an ein Amazon S3 Ziel CloudMirror Replizierung verwenden, beachten Sie, dass Amazon S3 die Größe der benutzerdefinierten Metadaten innerhalb jedes PUT-Anforderungsheaders auf 2 KB beschränkt. Wenn in einem Objekt benutzerdefinierte Metadaten größer als 2 KB sind, wird dieses Objekt nicht repliziert.

In StorageGRID können Sie die Objekte in einem einzelnen Bucket auf mehrere Ziel-Buckets replizieren. Geben Sie dazu das Ziel für jede Regel in der Replikationskonfiguration-XML an. Ein Objekt kann nicht gleichzeitig in mehr als einen Bucket repliziert werden.

Darüber hinaus können Sie die CloudMirror-Replizierung für versionierte oder nicht versionierte Buckets konfigurieren und ein versioniertes oder unversioniertes Bucket als Ziel angeben. Es können beliebige Kombinationen aus versionierten und nichtversionierten Buckets verwendet werden. Beispielsweise können Sie einen versionierten Bucket als Ziel für einen Bucket ohne Versionsangabe angeben oder umgekehrt. Zudem ist eine Replizierung zwischen nicht versionierten Buckets möglich.

Das Löschverhalten für den CloudMirror-Replikationsservice entspricht dem Löschverhalten des CRR-Dienstes (Cross Region Replication) von Amazon S3 — beim 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 durch das Löschen eines Objekts im Quell-Bucket der Löschmarker nicht in den Ziel-Bucket repliziert oder das Zielobjekt gelöscht.

Beim Replizieren der Objekte zum Ziel-Bucket markiert StorageGRID sie als „`replica`“. Ein StorageGRID-Zielbucket repliziert keine Objekte, die als Replikate markiert sind, und schützt Sie nicht vor versehentlichen Replikationsschleifen. Diese Replikatmarkierung ist intern in StorageGRID und verhindert nicht, dass Sie AWS CRR verwenden, wenn Sie einen Amazon S3-Bucket als Ziel verwenden.



Die benutzerdefinierte Kopfzeile, die zum Markieren eines Replikats verwendet wird, ist `x-ntap-sg-replica`. Diese Markierung verhindert einen kaskadierenden Spiegel. StorageGRID unterstützt auch einen bidirektionalen CloudMirror zwischen zwei Grids.

Die Einzigartigkeit und Reihenfolge von Ereignissen im Ziel-Bucket ist nicht garantiert. Als Folge von Betriebsabläufen wird möglicherweise mehr als eine identische Kopie eines Quellobjekts an das Ziel übergeben, um eine erfolgreiche Bereitstellung zu gewährleisten. In seltenen Fällen entspricht die Reihenfolge der Vorgänge auf dem Ziel-Bucket nicht der Reihenfolge der Ereignisse auf dem Quell-Bucket, wenn dasselbe Objekt gleichzeitig von zwei oder mehr verschiedenen StorageGRID-Standorten aktualisiert wird.

Die CloudMirror-Replizierung wird normalerweise so konfiguriert, dass sie einen externen S3-Bucket als Ziel verwendet. Die Replizierung kann jedoch auch für eine andere StorageGRID Implementierung oder einen beliebigen S3-kompatiblen Service konfiguriert werden.

Informieren Sie sich über Benachrichtigungen für Buckets

Sie können die Ereignisbenachrichtigung für einen S3-Bucket aktivieren, wenn StorageGRID Benachrichtigungen zu bestimmten Ereignissen an einen Amazon Simple Notification Service (SNS) als Ziel senden soll.

Das können Sie "[Konfigurieren Sie Ereignisbenachrichtigungen](#)" Durch Verknüpfung von XML für die Benachrichtigungskonfiguration mit einem Quell-Bucket. Die Benachrichtigungskonfiguration-XML folgt den S3-Konventionen für die Konfiguration von Bucket-Benachrichtigungen, wobei das Ziel-SNS-Thema als URN eines Endpunkts angegeben ist.

Ereignisbenachrichtigungen werden auf dem Quell-Bucket erstellt, wie in der Benachrichtigungskonfiguration angegeben, und werden an das Ziel übergeben. Wenn ein Ereignis, das einem Objekt zugeordnet ist,

erfolgreich ist, wird eine Benachrichtigung über dieses Ereignis erstellt und für die Bereitstellung in die Warteschlange verschoben.

Die Eindeutigkeit und Bestellung von Benachrichtigungen ist nicht garantiert. Möglicherweise werden mehrere Benachrichtigungen zu einem Ereignis an das Ziel übermittelt, da die Maßnahmen zur Sicherstellung des Liefererfolgs durchgeführt werden. Da die Bereitstellung asynchron ist, entspricht die Reihenfolge der Benachrichtigungen am Ziel nicht der Reihenfolge der Ereignisse auf dem Quell-Bucket. Dies gilt insbesondere für Vorgänge, die von unterschiedlichen StorageGRID-Standorten stammen. Sie können das verwenden `sequencer` Schlüssel in der Ereignismeldung, um die Reihenfolge der Ereignisse für ein bestimmtes Objekt zu bestimmen, wie in der Amazon S3-Dokumentation beschrieben.

Unterstützte Benachrichtigungen und Meldungen

StorageGRID-Ereignisbenachrichtigungen folgen der Amazon S3-API mit einigen Einschränkungen:

- Die folgenden Ereignistypen werden unterstützt:
 - `s3:ObjectCreated:*`
 - `s3:ObjectCreated:Put`
 - `s3:ObjectCreated:Post`
 - `s3:ObjectCreated:Copy`
 - `s3:ObjectCreated:CompleteMultipartUpload`
 - `s3:ObjectRemoved:*`
 - `s3:ObjectRemoved:Löschen`
 - `s3:ObjectRemoved>DeleteMarkerCreated`
 - `s3:ObjectRestore:Post`
- Aus StorageGRID gesendete Ereignisbenachrichtigungen verwenden das Standard-JSON-Format, enthalten aber keine Schlüssel und verwenden bestimmte Werte für andere, wie in der Tabelle gezeigt:

Schlüsselname	Wert von StorageGRID
EventSource	<code>sgws:s3</code>
AwsRegion	Nicht enthalten
X-amz-id-2	Nicht enthalten
arn	<code>urn:sgws:s3:::bucket_name</code>

Den Suchintegrations-Service verstehen

Sie können die Integration der Suche in einen S3-Bucket aktivieren, wenn Sie einen externen Such- und Analyseservice für Ihre Objektmetadaten verwenden möchten.

Der Suchintegrations-Service ist ein benutzerdefinierter StorageGRID Service, der automatisch und asynchron S3-Objektmetadaten an einen Ziel-Endpunkt sendet, wenn ein Objekt oder seine Metadaten aktualisiert werden. Anschließend können Sie mit den vom Ziel-Service bereitgestellten Tools für die Suche, Datenanalyse, Visualisierung und maschinelles Lernen Objektdaten suchen, analysieren und daraus

Erkenntnisse gewinnen.

Sie können den Such-Integrationservice für jeden versionierten oder nicht versionierten Bucket aktivieren. Die Suchintegration wird konfiguriert, indem eine XML-Verknüpfung für die Metadatenbenachrichtigung mit dem Bucket verknüpft wird, an dem Objekte ausgeführt werden sollen, und das Ziel für die Objektmetadaten.

Benachrichtigungen werden in Form eines JSON-Dokuments mit dem Bucket-Namen, Objektnamen und Versionsnummer generiert, falls vorhanden. Jede Metadatenbenachrichtigung enthält zusätzlich zu allen Tags und Benutzer-Metadaten des Objekts einen Standardsatz an Systemmetadaten für das Objekt.



Für Tags und Benutzer-Metadaten gibt StorageGRID Daten und Nummern an Elasticsearch als Strings oder als S3-Ereignisbenachrichtigungen weiter. Um Elasticsearch so zu konfigurieren, dass diese Strings als Daten oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen für die dynamische Feldzuordnung und die 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.

Benachrichtigungen werden generiert und in die Warteschlange für die Zustellung gestellt, wann immer:

- Ein Objekt wird erstellt.
- Ein Objekt wird gelöscht, auch wenn Objekte aus dem Vorgang der ILM-Richtlinie des Grid gelöscht werden.
- Metadaten oder Tags von Objekten werden hinzugefügt, aktualisiert oder gelöscht. Der komplette Satz an Metadaten und Tags wird immer bei Update gesendet - nicht nur die geänderten Werte.

Nachdem Sie einem Bucket die XML-Benachrichtigungskonfiguration für Metadaten hinzugefügt haben, werden Benachrichtigungen für alle neuen Objekte gesendet, die Sie erstellen, und für alle Objekte, die Sie ändern, indem Sie deren Daten, Benutzer-Metadaten oder Tags aktualisieren. Es werden jedoch keine Benachrichtigungen für Objekte gesendet, die sich bereits im Bucket befinden. Um sicherzustellen, dass Objektmetadaten für alle Objekte im Bucket an das Ziel gesendet werden, sollten Sie eines der folgenden Aktionen durchführen:

- Konfigurieren Sie den Suchintegrationsdienst unmittelbar nach dem Erstellen des Buckets und vor dem Hinzufügen von Objekten.
- Führen Sie eine Aktion für alle Objekte aus, die sich bereits im Bucket befinden, und löst eine Metadaten-Benachrichtigung aus, die an das Ziel gesendet wird.

Der StorageGRID Such-Integrationservice unterstützt ein Elasticsearch-Cluster als Ziel. Wie bei den anderen Plattformdiensten wird das Ziel im Endpunkt angegeben, dessen URN in der Konfigurations-XML für den Dienst verwendet wird. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool](#)" Um die unterstützten Versionen von Elasticsearch zu ermitteln.

Verwandte Informationen

["Konfigurations-XML für die Integration der Suche"](#)

["Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"](#)

["JSON durch den Suchintegrations-Service generiert"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

Überlegungen zu Plattformservices

Vor der Implementierung von Plattform-Services sollten Sie die Empfehlungen und Überlegungen zu deren Verwendung überprüfen.

Informationen zu S3 finden Sie unter "[S3-REST-API VERWENDEN](#)".

Überlegungen bei der Verwendung von Plattform-Services

Überlegungen	Details
Ziel-Endpoint-Monitoring	<p>Sie müssen die Verfügbarkeit jedes Zielendpunkts überwachen. Wenn die Verbindung zum Zielendpunkt über einen längeren Zeitraum unterbrochen wird und ein großer Rückstand von Anfragen besteht, schlagen zusätzliche Clientanforderungen (wie Z. B. PUT-Anforderungen) an StorageGRID fehl. Sie müssen diese fehlgeschlagenen Anforderungen erneut versuchen, wenn der Endpunkt erreichbar ist.</p>
Drosselung des Zielendpunkts	<p>StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten.</p> <p>Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich.</p> <p>CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.</p>
Bestellgarantien	<p>StorageGRID garantiert die Bestellung von Vorgängen an einem Objekt innerhalb eines Standorts. Solange sich alle Vorgänge für ein Objekt innerhalb desselben Standorts befinden, entspricht der endgültige Objektstatus (für die Replizierung) immer dem Status in StorageGRID.</p> <p>StorageGRID unternimmt alle Anstrengungen, Anfragen zu bestellen, wenn die Vorgänge an verschiedenen StorageGRID Standorten durchgeführt werden. Wenn Sie beispielsweise ein Objekt zunächst an Standort A schreiben und später dasselbe Objekt an Standort B überschreiben, ist das von CloudMirror in den Ziel-Bucket replizierte Objekt nicht garantiert, dass es sich um das neuere Objekt handelt.</p>

Überlegungen	Details
ILM-gesteuerte Objektlöschungen	<p>Um dem Löschverhalten der AWS CRR- und SNS-Dienste anzupassen, werden CloudMirror- und Ereignisbenachrichtigungsanforderungen nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID-ILM-Regeln gelöscht wird. Beispiel: Es werden keine Anfragen für CloudMirror- oder Ereignisbenachrichtigungen gesendet, wenn eine ILM-Regel ein Objekt nach 14 Tagen löscht.</p> <p>Suchintegrationsanfragen werden dagegen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.</p>

Überlegungen bei der Verwendung des CloudMirror Replikationsservice

Überlegungen	Details
Replikationsstatus	StorageGRID unterstützt das nicht <code>x-amz-replication-status</code> Kopfzeile.
Objektgröße	<p>Die maximale Größe für Objekte, die vom CloudMirror-Replikationsservice in einen Ziel-Bucket repliziert werden können, beträgt 5 tib. Dies ist die gleiche wie die maximal <i>unterstützte</i> Objektgröße.</p> <p>Hinweis: Die maximale <i>empfohlene</i> Größe für einen Single PUT-Vorgang beträgt 5 gib (5,368,709,120 Byte). Wenn Sie über Objekte mit einer Größe von mehr als 5 gib verfügen, verwenden Sie stattdessen mehrteilige Uploads.</p>
Bucket-Versionierung und VersionIDs	<p>Wenn die Versionierung im S3-Quell-Bucket von StorageGRID aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren.</p> <p>Beachten Sie bei der Verwendung der Versionierung, dass die Bestellung von Objektversionen im Ziel-Bucket am besten ist und vom CloudMirror Service nicht garantiert wird, da Einschränkungen im S3-Protokoll bestehen.</p> <p>Hinweis: Versions-IDs für den Quell-Bucket in StorageGRID hängen nicht mit den Versions-IDs für den Ziel-Bucket zusammen.</p>
Tagging für Objektversionen	<p>Der CloudMirror Service repliziert aufgrund von Einschränkungen im S3-Protokoll keine PUT Objekt-Tagging- oder DELETE Objekt-Tagging-Anfragen, die eine Version-ID bereitstellen. Da Versions-IDs für Quelle und Ziel nicht miteinander verknüpft sind, kann nicht sichergestellt werden, dass ein Tag-Update auf eine bestimmte Versions-ID repliziert wird.</p> <p>Im Gegensatz dazu repliziert der CloudMirror Service PUT Objekt-Tagging-Anfragen oder LÖSCHT Objekt-Tagging-Anfragen, die keine Version-ID angeben. Diese Anforderungen aktualisieren die Tags für den aktuellen Schlüssel (oder die aktuellste Version, wenn der Bucket versioniert ist). Normale Missionen mit Tags (keine Tagging-Updates) werden ebenfalls repliziert.</p>

Überlegungen	Details
Mehrteilige Uploads und ETag Werte	Bei der Spiegelung von Objekten, die mittels eines mehrteiligen Uploads hochgeladen wurden, bleiben die Teile vom CloudMirror-Service nicht erhalten. Als Ergebnis davon ist der ETag Wert für das gespiegelte Objekt unterscheidet sich vom 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 für die CloudMirror-Replikation in den Quell-Bucket aufzunehmen, und die Anforderung die SSE-C-Anfrageheader enthält, schlägt der Vorgang fehl.
Bucket mit S3-Objektsperre aktiviert	Wenn der Ziel-S3-Bucket für CloudMirror-Replikation S3-Objektsperre aktiviert ist, schlägt der Versuch, die Bucket-Replikation zu konfigurieren (PUT Bucket-Replikation) mit einem AccessDenied-Fehler fehl.

Plattform-Services-Endpunkte konfigurieren

Bevor Sie einen Plattformservice für einen Bucket konfigurieren können, müssen Sie mindestens einen Endpunkt als Ziel für den Plattformservice konfigurieren.

Der Zugriff auf Plattform-Services wird von einem StorageGRID Administrator nach Mandanten aktiviert. Um einen Endpunkt für Plattformservices zu erstellen oder zu verwenden, müssen Sie ein Mandantenbenutzer mit Berechtigungen zum Verwalten von Endpunkten oder Root-Zugriff in einem Grid sein, dessen Netzwerk so konfiguriert wurde, dass Storage-Nodes auf externe Endpunktressourcen zugreifen können. Weitere Informationen erhalten Sie von Ihrem StorageGRID Administrator.

Was ist ein Endpunkt für Plattformservices?

Wenn Sie einen Endpunkt für Plattformservices erstellen, geben Sie 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 Plattform-Services-Endpunkt, der die Informationen und Zugangsdaten enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket auf Amazon benötigt.

Für jeden Plattformservice ist ein eigener Endpunkt erforderlich. Daher müssen Sie für jeden zu verwendenden Plattformservice mindestens einen Endpunkt konfigurieren. Nachdem Sie einen Endpunkt für Plattformservices definiert haben, verwenden Sie den URN des Endpunkts als Ziel in der zum Aktivieren des Dienstes verwendeten Konfigurations-XML.

Sie können für mehrere Quell-Buckets denselben Endpunkt wie das Ziel verwenden. Beispielsweise könnten Sie mehrere Quell-Buckets konfigurieren, um Objektmetadaten an denselben Endpunkt für die Integration der Suchfunktion zu senden, sodass Sie Suchvorgänge über mehrere Buckets durchführen können. Sie können auch einen Quell-Bucket so konfigurieren, dass mehrere Endpunkte als Ziel verwendet werden. Dies ermöglicht es Ihnen, z. B. Benachrichtigungen zur Objekterstellung an ein SNS-Thema zu senden und Benachrichtigungen zum Löschen von Objekten an ein zweites SNS-Thema zu senden.

Endpunkte für CloudMirror Replizierung

StorageGRID unterstützt Replizierungsendpunkte, die S3-Buckets darstellen. Diese Buckets können unter

Umständen auf Amazon Web Services, derselben oder einer Remote-StorageGRID-Implementierung oder einem anderen Service gehostet werden.

Endpunkte für Benachrichtigungen

StorageGRID unterstützt SNS-Endpunkte (Simple Notification Service). Simple Queue Service (SQS)- oder AWS Lambda-Endpunkte werden nicht unterstützt.

Endpunkte für den Suchintegrations-Service

StorageGRID unterstützt Endpunkte für die Suchintegration, die Elasticsearch-Cluster darstellen. Diese Elasticsearch-Cluster können sich in einem lokalen Datacenter befinden oder in einer AWS Cloud oder an anderen Standorten 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 Erstellung des Endpunkts fehl. Sie müssen den Typ nicht erstellen, bevor Sie den Endpunkt erstellen. Bei Bedarf erstellt StorageGRID den Typ, wenn Objektmetadaten an den Endpunkt gesendet werden.

Verwandte Informationen

["StorageGRID verwalten"](#)

URN für Endpunkt von Plattformservices angeben

Wenn Sie einen Endpunkt für Plattformservices erstellen, müssen Sie einen eindeutigen Ressourcennamen (URN) angeben. Sie verwenden den URN, um auf den Endpunkt zu verweisen, wenn Sie Konfigurations-XML für den Plattfordienst erstellen. Der URN für jeden Endpunkt muss eindeutig sein.

StorageGRID validiert die Endpunkte der Plattformservices bei ihrer Erstellung. Bevor Sie einen Endpunkt für Plattformservices erstellen, vergewissern Sie sich, dass die im Endpunkt angegebene Ressource vorhanden ist und dass sie erreicht werden kann.

Elemente URN

Der URN für einen Endpunkt von Plattformservices muss mit beiden beginnen `arn:aws` Oder `urn:mysite`, Wie folgt:

- Wenn der Service auf Amazon Web Services (AWS) gehostet wird, verwenden Sie `arn:aws`.
- Wenn der Service auf der Google Cloud Platform (GCP) gehostet wird, verwenden Sie `arn:aws`.
- Wenn der Service lokal gehostet wird, verwenden Sie `urn:mysite`

Wenn Sie beispielsweise den URN für einen CloudMirror-Endpunkt angeben, der auf StorageGRID gehostet wird, kann der URN mit beginnen `urn:sgws`.

Das nächste Element des URN gibt den Typ des Plattform-Service wie folgt an:

Service	Typ
Replizierung von CloudMirror	s3

Service	Typ
Benachrichtigungen	sns
Integration von Suchen	es

Wenn Sie beispielsweise weiterhin den URN für einen CloudMirror-Endpunkt angeben möchten, der auf StorageGRID gehostet wird, fügen Sie hinzu `s3` Um zu erhalten `urn:sgws:s3`.

Das letzte Element des URN identifiziert die spezifische Zielressource am Ziel-URI.

Service	Bestimmte Ressource
Replizierung von CloudMirror	Bucket-Name
Benachrichtigungen	sns-Topic-Name
Integration von Suchen	domain-name/index-name/type-name Hinweis: Wenn der Elasticsearch-Cluster nicht konfiguriert ist, um Indizes automatisch zu erstellen, müssen Sie den Index manuell erstellen, bevor Sie den Endpunkt erstellen.

Urns für Services zum Hosten auf AWS und GCP

Für AWS und GCP-Einheiten ist der vollständige URN ein gültiger AWS ARN. Beispiel:

- CloudMirror-Replizierung:

```
arn:aws:s3:::bucket-name
```

- Benachrichtigungen:

```
arn:aws:sns:region:account-id:topic-name
```

- Integration von Suchen:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Für einen AWS Endpunkt zur Integration der Suchfunktion finden Sie hier `domain-name`. Muss den Literalstring enthalten `domain/`, Wie hier gezeigt.

Urnen für vor Ort gehostete Services

Wenn Sie lokale gehostete Services anstelle von Cloud-Services nutzen, können Sie den URN auf jede Art und Weise angeben, die einen gültigen und eindeutigen URN erstellt, solange der URN die erforderlichen Elemente in der dritten und letzten Position enthält. Sie können die durch optional angezeigten Elemente leer lassen oder sie auf eine beliebige Weise angeben, die Ihnen bei der Identifizierung der Ressource und der eindeutigen URN-Funktion hilft. Beispiel:

- CloudMirror-Replizierung:

```
urn:mysite:s3:optional:optional:bucket-name
```

Für einen CloudMirror-Endpunkt, der auf StorageGRID gehostet wird, können Sie einen gültigen URN angeben, der mit beginnt `urn:sgws:`

```
urn:sgws:s3:optional:optional:bucket-name
```

- Benachrichtigungen:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- Integration von Suchen:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



Für lokal gehostete Suchintegrationsendpunkte finden Sie auf `domain-name` Das Element kann eine beliebige Zeichenfolge sein, solange der URN des Endpunkts eindeutig ist.

Endpunkt für Plattformservices erstellen

Sie müssen mindestens einen Endpunkt des richtigen Typs erstellen, bevor Sie einen Plattfordienst aktivieren können.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Verwalten von Endpunkten oder Root-Zugriffsberechtigungen](#)".
- Die Ressource, auf die der Endpunkt der Plattformservices verweist, wurde erstellt:
 - CloudMirror Replizierung: S3 Bucket
 - Ereignisbenachrichtigung: SNS-Thema
 - Suchbenachrichtigung: Elasticsearch-Index, wenn das Ziel-Cluster nicht konfiguriert ist, Indizes automatisch zu erstellen.

- Sie haben die Informationen über die Zielressource:
 - Host und Port für den Uniform Resource Identifier (URI)



Wenn Sie einen Bucket verwenden möchten, der auf einem StorageGRID-System als Endpunkt für die CloudMirror-Replizierung gehostet wird, wenden Sie sich an den Grid-Administrator, um die erforderlichen Werte zu bestimmen.

- Eindeutiger Ressourcenname (URN)

"URN für Endpunkt von Plattformservices angeben"

- Authentifizierungsdaten (falls erforderlich):
 - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
 - Basic HTTP: Benutzername und Passwort
 - CAP (C2S Access Portal): Temporäre Anmeldeinformationen URL, Server- und Client-Zertifikate, Clientschlüssel und eine optionale private Client-Schlüssel-Passphrase.
- Sicherheitszertifikat (bei Verwendung eines benutzerdefinierten CA-Zertifikats)
- Wenn die Elasticsearch-Sicherheitsfunktionen aktiviert sind, verfügen Sie über die Berechtigung zum Überwachen des Clusters für den Verbindungstest und entweder über die Berechtigung zum Schreibindex oder sowohl über die Index- als auch Löschindexberechtigungen für Dokumentaktualisierungen.

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus.

Die Seite „Endpunkte der Plattfordienste“ wird angezeigt.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

0 endpoints

Create endpoint

Delete endpoint

	Display name ?	Last error ?	Type ?	URI ?	URN ?
No endpoints found					
<p>Create endpoint</p>					

2. Wählen Sie **Endpoint erstellen**.

Create endpoint ✕

1 Enter details

2 Select authentication type
Optional

3 Verify server
Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name ?

URI ?

URN ?

Cancel
Continue

3. Geben Sie einen Anzeigenamen ein, um den Endpunkt und seinen Zweck kurz zu beschreiben.

Der vom Endpunkt unterstützte Plattformservice wird neben dem Endpunktnamen angezeigt, wenn er auf der Seite Endpunkte aufgeführt wird. Sie müssen diese Informationen daher nicht in den Namen aufnehmen.

4. Geben Sie im Feld **URI** den eindeutigen Resource Identifier (URI) des Endpunkts an.

Verwenden Sie eines der folgenden Formate:

```
https://host:port
http://host:port
```

Wenn Sie keinen Port angeben, wird Port 443 für HTTPS-URIs und Port 80 für HTTP-URIs verwendet.

Beispielsweise kann der URI für einen Bucket, der auf StorageGRID gehostet wird, folgende sein:

```
https://s3.example.com:10443
```

In diesem Beispiel `s3.example.com` stellt den DNS-Eintrag für die virtuelle IP (VIP) der StorageGRID HA-Gruppe dar und `10443` stellt den Port dar, der im Endpunkt des Load Balancer definiert ist.



Wenn dies möglich ist, sollten Sie eine Verbindung zu einer HA-Gruppe von Load-Balancing-Nodes herstellen, um einen Single Point of Failure zu vermeiden.

Auf ähnliche Weise kann der URI für einen Bucket sein, der auf AWS gehostet wird,:

```
https://s3-aws-region.amazonaws.com
```



Wenn der Endpunkt für den CloudMirror-Replikationsservice verwendet wird, fügen Sie den Bucket-Namen nicht in den URI ein. Sie fügen 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 ändern, nachdem der Endpunkt erstellt wurde.

6. Wählen Sie **Weiter**.

7. Wählen Sie einen Wert für **Authentifizierungstyp** aus, und geben Sie dann die erforderlichen Anmeldedaten ein oder laden Sie sie hoch.

Create endpoint

1 Enter details — 2 Select authentication type (Optional) — 3 Verify server (Optional)

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous (selected)
Anonymous
Access Key
Basic HTTP
CAP (C2S Access Portal)

Previous Continue

Die von Ihnen eingegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierungstyp	Beschreibung	Anmeldedaten
Anonym	Gibt anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet AWS Zugangsdaten für die Authentifizierung von Verbindungen mit dem Ziel	<ul style="list-style-type: none"> • Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
Basis-HTTP	Verwendet einen Benutzernamen und ein Passwort, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Benutzername • Passwort
KAPPE (C2S-Zugangsportale)	Verwendet Zertifikate und Schlüssel zur Authentifizierung von Verbindungen zum Ziel.	<ul style="list-style-type: none"> • URL für temporäre Anmeldeinformationen • Server-CA-Zertifikat (PEM-Datei-Upload) • Client-Zertifikat (PEM-Datei-Upload) • Privater Client-Schlüssel (Upload der PEM-Datei, verschlüsseltes OpenSSL-Format oder unverschlüsseltes privates Schlüsselformat) • Private Client-Schlüssel-Passphrase (optional)

8. Wählen Sie **Weiter**.

9. Wählen Sie eine Optionsschaltfläche für **Server überprüfen** aus, um auszuwählen, wie die TLS-Verbindung zum Endpunkt verifiziert wird.

Create endpoint

Enter details — Select authentication type Optional — **3** Verify server Optional

Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate
 Use operating system CA certificate
 Do not verify certificate

```

-----BEGIN CERTIFICATE-----
abcdefghijklmnopkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklmnopklABCD
-----END CERTIFICATE-----
  
```

[Previous](#)
[Test and create endpoint](#)

Typ der Zertifikatverifizierung	Beschreibung
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat. Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat in das Textfeld CA-Zertifikat .
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert. Diese Option ist nicht sicher.

10. Wählen Sie **Test und Endpunkt erstellen**.

- Eine Erfolgsmeldung wird angezeigt, wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.
- Wenn die Endpoint-Validierung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn Sie den Endpunkt ändern müssen, um den Fehler zu beheben, wählen Sie **Zurück zu Endpunktdetails** und aktualisieren Sie die Informationen. Wählen Sie anschließend **Test und Endpunkt erstellen** aus.



Die Erstellung von Endpunkten schlägt fehl, wenn Plattformdienste für Ihr Mandantenkonto nicht aktiviert sind. Wenden Sie sich an den StorageGRID-Administrator.

Nachdem Sie einen Endpunkt konfiguriert haben, können Sie mit seinem URN einen Plattformdienst konfigurieren.

Verwandte Informationen

["URN für Endpunkt von Plattformservices angeben"](#)

["CloudMirror-Replizierung konfigurieren"](#)

["Konfigurieren Sie Ereignisbenachrichtigungen"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

Testen der Verbindung für Endpunkt der Plattformservices

Wenn sich die Verbindung zu einem Plattformdienst geändert hat, können Sie die Verbindung für den Endpunkt testen, um zu überprüfen, ob die Zielressource existiert und ob sie mit den von Ihnen angegebenen Anmeldeinformationen erreicht werden kann.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Verwalten von Endpunkten oder Root-Zugriffsberechtigungen"](#).

Über diese Aufgabe

StorageGRID überprüft nicht, ob die Anmeldeinformationen die richtigen Berechtigungen haben.

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus.

Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ? ↕	Last error ? ↕	Type ? ↕	URI ? ↕	URN ? ↕
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Wählen Sie den Endpunkt aus, dessen Verbindung Sie testen möchten.

Die Seite mit den Details des Endpunkts wird angezeigt.

Overview ↑

Display name: **my-endpoint-1** [✎](#)

Type: **S3 Bucket**

URI: **http://10.96.104.167:10443**

URN: **urn:sgws:s3:::bucket1**

Connection **Configuration**

Verify connection [?](#)

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

3. Wählen Sie **Verbindung testen**.

- Eine Erfolgsmeldung wird angezeigt, wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.
- Wenn die Endpoint-Validierung 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 anschließend **Test und speichern Sie die Änderungen**.

Endpunkt der Plattformdienste bearbeiten

Sie können die Konfiguration für einen Endpunkt für Plattformdienste bearbeiten, um seinen Namen, URI oder andere Details zu ändern. Beispielsweise müssen Sie möglicherweise abgelaufene Anmeldedaten aktualisieren oder den URI so ändern, dass er zu einem Backup-Elasticsearch-Index für ein Failover weist. Sie können die URN für einen Endpunkt für Plattformdienste nicht ändern.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Verwalten von Endpunkten oder Root-Zugriffsberechtigungen](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus.

Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ?	Last error ?	Type ?	URI ?	URN ?
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Wählen Sie den Endpunkt aus, den Sie bearbeiten möchten.

Die Seite mit den Details des Endpunkts wird angezeigt.

3. Wählen Sie **Konfiguration**.

Overview

Display name: **my-endpoint-3** 

Type: **Notifications**

URI: **http://10.96.104.202:8080/**

URN: **arn:aws:sns:us-west-2::example1**

Connection

Configuration

Edit configuration

Endpoint details

URI 

http://10.96.104.202:8080/

URN 

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP 

Username 

testme

Password 

••••••••

Edit password

Verify server

- Use custom CA certificate
- Use operating system CA certificate
- Do not verify certificate

```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnop1234567890ABCDEFGHIJKL  
123456/7890ABCDEFabcdefghijklmnop123456  
-----END CERTIFICATE-----
```

Test and save changes

4. Ändern Sie bei Bedarf die Konfiguration des Endpunkts.



Sie können die URN eines Endpunkts nicht ändern, nachdem der Endpunkt erstellt wurde.

- a. Um den Anzeigenamen für den Endpunkt zu ändern, wählen Sie das Bearbeiten-Symbol .
- b. Ändern Sie bei Bedarf den URI.
- c. Ändern Sie bei Bedarf den Authentifizierungstyp.
 - Zur Authentifizierung des Zugriffsschlüssels ändern Sie den Schlüssel ggf. durch Auswahl von **S3-Schlüssel bearbeiten** und Einfügen einer neuen Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels. Wenn Sie Ihre Änderungen abrechnen müssen, wählen Sie **S3-Taste Edit** rückgängig machen.
 - Ändern Sie für die grundlegende HTTP-Authentifizierung den Benutzernamen nach Bedarf. Ändern Sie das Passwort nach Bedarf, indem Sie **Passwort bearbeiten** und das neue Passwort eingeben. Wenn Sie Ihre Änderungen abrechnen müssen, wählen Sie **Passwort zurücksetzen Bearbeiten**.
 - Für die CAP-Authentifizierung (C2S Access Portal) ändern Sie die URL für temporäre Anmeldeinformationen oder die optionale private Passphrase für Clientschlüssel und laden Sie nach Bedarf neue Zertifikate und Schlüsseldateien hoch.



Der private Client-Schlüssel muss im OpenSSL-verschlüsselten Format oder unverschlüsseltem privaten Schlüssel vorliegen.

- d. Ändern Sie bei Bedarf die Methode zur Überprüfung des Servers.

5. Wählen Sie **Test und speichern Sie die Änderungen**.

- Eine Erfolgsmeldung wird angezeigt, wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort überprüft.
- Wenn die Endpoint-Validierung fehlschlägt, wird eine Fehlermeldung angezeigt. Ändern Sie den Endpunkt, um den Fehler zu beheben, und wählen Sie dann **Änderungen testen und speichern**.

Endpunkt für Plattformservices löschen

Sie können einen Endpunkt löschen, wenn Sie den zugeordneten Plattfordienst nicht mehr verwenden möchten.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Verwalten von Endpunkten oder Root-Zugriffsberechtigungen](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus.

Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Aktivieren Sie das Kontrollkästchen für jeden Endpunkt, den Sie löschen möchten.



Wenn Sie einen Endpunkt für Plattformservices löschen, der verwendet wird, wird der zugehörige Plattformdienst für alle Buckets deaktiviert, die den Endpunkt verwenden. Alle noch nicht abgeschlossenen Anfragen werden gelöscht. Neue Anfragen werden weiterhin generiert, bis Sie Ihre Bucket-Konfiguration so ändern, dass Sie nicht mehr auf den gelöschten URN verweisen. StorageGRID meldet diese Anfragen als nicht behebbare Fehler.

3. Wählen Sie **Aktionen** > **Endpunkt löschen**.

Eine Bestätigungsmeldung wird angezeigt.

Delete endpoint

Are you sure you want to delete endpoint my-endpoint-10?

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

[Cancel](#) [Delete endpoint](#)

4. Wählen Sie **Endpunkt löschen**.

Fehlerbehebung bei Endpunktfehlern bei Plattform-Services

Wenn StorageGRID versucht, mit einem Endpunkt für Plattformdienste zu kommunizieren, wird eine Meldung auf dem Dashboard angezeigt. Auf der Seite „Plattform-Services-Endpunkte“ wird in der Spalte „Letzte Fehler“ angezeigt, wie lange der Fehler bereits aufgetreten ist. Es wird kein Fehler angezeigt, wenn die Berechtigungen, die mit den Anmeldedaten eines Endpunkts verknüpft sind, falsch sind.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Fehler am Endpunkt der Plattformdienste aufgetreten sind, zeigt das Mandantenmanager-Dashboard eine Warnmeldung an. Auf der Seite Plattform-Services-Endpunkte finden Sie weitere Details zum Fehler.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Der gleiche Fehler, der auf dem Dashboard angezeigt wird, wird auch oben auf der Seite „Endpunkte für Plattformdienste“ angezeigt. So zeigen Sie eine detailliertere Fehlermeldung an:

Schritte

1. Wählen Sie in der Liste der Endpunkte den Endpunkt aus, der den Fehler hat.
2. Wählen Sie auf der Seite Details zum Endpunkt die Option **Verbindung** aus. Auf dieser Registerkarte wird nur der letzte Fehler für einen Endpunkt angezeigt und gibt an, wie lange der Fehler aufgetreten ist. Fehler, die das rote X-Symbol enthalten  Aufgetreten innerhalb der letzten 7 Tage.

Overview ^

Display name:	my-endpoint-2 
Type:	Search
URI:	http://10.96.104.30:9200
URN:	urn:sgws:es:::mydomain/sveloso/_doc

Connection

Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

Last error details

 2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

Überprüfen Sie, ob der Fehler noch immer aktuell ist

Einige Fehler werden möglicherweise weiterhin in der Spalte **Letzter Fehler** angezeigt, auch nachdem sie behoben wurden. So prüfen Sie, 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 Details des Endpunkts wird angezeigt.

2. Wählen Sie **Verbindung > Verbindung testen**.

Durch die Auswahl von **Testverbindung** überprüft StorageGRID, ob der Endpunkt für Plattformdienste vorhanden ist und ob er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Beheben von Endpunktfehlern

Sie können die Meldung **Letzter Fehler** auf der Seite Details zum Endpunkt verwenden, um zu ermitteln, was

1113

den Fehler verursacht. Bei einigen Fehlern müssen Sie möglicherweise den Endpunkt bearbeiten, um das Problem zu lösen. Beispielsweise kann ein CloudMirroring-Fehler auftreten, wenn StorageGRID nicht auf den Ziel-S3-Bucket zugreifen kann, da er nicht über die richtigen Zugriffsberechtigungen verfügt oder der Zugriffsschlüssel abgelaufen ist. Die Meldung lautet „entweder die Anmeldeinformationen des Endpunkts oder der Zielzugriff muss aktualisiert werden,“ und die Details lauten „AccessDenied“ oder „InvalidAccessKeyId“.

Wenn Sie den Endpunkt bearbeiten müssen, um einen Fehler zu beheben, wird durch Auswahl von **Änderungen testen und speichern** der aktualisierte Endpunkt von StorageGRID überprüft und bestätigt, dass er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Schritte

1. Wählen Sie den Endpunkt aus.
2. Wählen Sie auf der Seite Details zum Endpunkt die Option **Konfiguration** aus.
3. Bearbeiten Sie die Endpunkt Konfiguration nach Bedarf.
4. Wählen Sie **Verbindung > Verbindung testen**.

Endpoint-Anmeldeinformationen mit unzureichenden Berechtigungen

Wenn StorageGRID einen Endpunkt für Plattformservices validiert, bestätigt er, dass die Anmeldeinformationen des Endpunkts zur Kontaktaufnahme mit der Zielressource verwendet werden können und eine grundlegende Überprüfung der Berechtigungen durchgeführt wird. StorageGRID validiert jedoch nicht alle für bestimmte Plattform-Services-Vorgänge erforderlichen Berechtigungen. Wenn Sie daher beim Versuch, einen Plattformdienst zu verwenden (z. B. „403 Forbidden“) einen Fehler erhalten, prüfen Sie die Berechtigungen, die mit den Anmeldedaten des Endpunkts verknüpft sind.

Verwandte Informationen

- [Verwaltung von StorageGRID > Fehlerbehebung für Plattformservices](#)
- ["Endpunkt für Plattformservices erstellen"](#)
- ["Testen der Verbindung für Endpunkt der Plattformservices"](#)
- ["Endpunkt der Plattformdienste bearbeiten"](#)

CloudMirror-Replizierung konfigurieren

Der ["CloudMirror Replikationsservice"](#) Zu den drei Plattform-Services von StorageGRID gehören. Mithilfe der CloudMirror Replizierung können Sie Objekte automatisch in einen externen S3-Bucket replizieren.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator 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 haben seinen URN.
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Die CloudMirror Replizierung kopiert Objekte von einem Quell-Bucket zu einem Ziel-Bucket, der in einem Endpunkt angegeben wird.



Die CloudMirror-Replizierung weist wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter "[Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung](#)".

Um die CloudMirror-Replikation für einen Bucket zu aktivieren, müssen Sie eine gültige Bucket-Replizierungskonfiguration-XML erstellen und anwenden. Die XML-Replikationskonfiguration muss den URN eines S3-Bucket-Endpunkts für jedes Ziel verwenden.



Die Replizierung wird für Quell- oder Ziel-Buckets nicht unterstützt, wenn S3 Object Lock aktiviert ist.

Allgemeine Informationen zur Bucket-Replizierung und deren Konfiguration finden Sie unter "[Amazon Simple Storage Service \(S3\) Dokumentation: Replizierung von Objekten](#)". Informationen zur Implementierung von GetBucketReplication, DeleteBucketReplication und PutketReplication durch StorageGRID finden Sie im "[Operationen auf Buckets](#)".

Wenn Sie die CloudMirror-Replizierung für einen Bucket aktivieren, der Objekte enthält, werden neue Objekte, die dem Bucket hinzugefügt wurden, repliziert, die vorhandenen Objekte in dem Bucket werden jedoch nicht repliziert. Sie müssen vorhandene Objekte aktualisieren, um die Replikation auszulösen.

Wenn Sie in der Replikationskonfiguration-XML eine Storage-Klasse angeben, verwendet StorageGRID diese Klasse, wenn Vorgänge mit dem Ziel-S3-Endpunkt durchgeführt werden. Der Ziel-Endpunkt muss auch die angegebene Storage-Klasse unterstützen. Befolgen Sie unbedingt die Empfehlungen des Zielsystemanbieters.

Schritte

1. Replizierung für Ihren Quell-Bucket aktivieren:

Verwenden Sie einen Texteditor, um die Replikationskonfiguration-XML zu erstellen, die für die Replikation erforderlich ist, wie in der S3-Replikations-API angegeben. Bei der XML-Konfiguration:

- Beachten Sie, dass StorageGRID nur V1 der Replizierungskonfiguration unterstützt. Das bedeutet, dass StorageGRID die Verwendung von nicht unterstützt `Filter` Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration.
- Verwenden Sie den URN eines S3-Bucket-Endpunkts als Ziel.
- Fügen Sie optional die hinzu `<StorageClass>` Und geben Sie eines der folgenden Elemente an:
 - `STANDARD`: Die Standard-Speicherklasse. Wenn Sie beim Hochladen eines Objekts keine Storage-Klasse angeben, wird der angezeigt `STANDARD` Storage-Klasse wird verwendet.
 - `STANDARD_IA`: (Standard - seltener Zugang.) Nutzen Sie diese Storage-Klasse für Daten, auf die seltener zugegriffen wird, aber bei Bedarf auch schnell zugegriffen werden muss.
 - `REDUCED_REDUNDANCY`: Verwenden Sie diese Speicherklasse für nicht kritische, reproduzierbare Daten, die mit weniger Redundanz gespeichert werden können als die `STANDARD` Storage-Klasse.
- Wenn Sie ein angeben `Role` In der XML-Konfiguration wird sie 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 **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Replikation**.
5. Aktivieren Sie das Kontrollkästchen **Enable Replication**.
6. Fügen Sie die XML-Replikationskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

Bucket options
Bucket access
Platform services

Replication
Disabled
^

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

```

<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
    
```

Save changes



Platformservices müssen für jedes Mandantenkonto von einem StorageGRID-Administrator mithilfe des Grid Manager oder der Grid Management API aktiviert werden. Wenden Sie sich an Ihren StorageGRID-Administrator, wenn beim Speichern der Konfigurations-XML ein Fehler auftritt.

7. Überprüfen Sie, ob die Replikation ordnungsgemäß konfiguriert ist:
 - a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die in der Replizierungskonfiguration angegebenen Anforderungen für die Replizierung erfüllt.

In dem zuvor gezeigten Beispiel werden Objekte repliziert, die mit dem Präfix „2020“ übereinstimmen.

- b. Vergewissern Sie sich, dass das Objekt in den Ziel-Bucket repliziert wurde.

Bei kleinen Objekten wird die Replizierung schnell durchgeführt.

Verwandte Informationen

["Endpunkt für Plattformservices erstellen"](#)

Konfigurieren Sie Ereignisbenachrichtigungen

Der Benachrichtigungsservice ist einer der drei StorageGRID-Plattfordienste. Sie können Benachrichtigungen aktivieren, damit ein Bucket Informationen zu bestimmten Ereignissen an einen Zieldienst sendet, der den AWS Simple Notification Service™ (SNS) unterstützt.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Quelle für Benachrichtigungen fungiert.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, ist bereits vorhanden, und Sie haben seine URN.
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Nachdem Sie Ereignisbenachrichtigungen konfiguriert haben, wird eine Benachrichtigung generiert und an das Thema Simple Notification Service (SNS) gesendet, das als Zielendpunkt verwendet wird, sobald ein bestimmtes Ereignis für ein Objekt im Quell-Bucket eintritt. Um Benachrichtigungen für einen Bucket zu aktivieren, müssen Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden. Die XML-ID für die Benachrichtigungskonfiguration muss den URN eines Endpunkt für Ereignisbenachrichtigungen für jedes Ziel verwenden.

Allgemeine Informationen zu Ereignisbenachrichtigungen und deren Konfiguration finden Sie in der Amazon-Dokumentation. Informationen zur Implementierung der S3-Bucket-Benachrichtigungs-API von StorageGRID finden Sie in den Anweisungen zum Implementieren von S3-Client-Applikationen.

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. Benachrichtigungen für Ihren Quell-Bucket aktivieren:
 - Verwenden Sie einen Texteditor, um die XML-Benachrichtigungskonfiguration zu erstellen, die für die Aktivierung von Ereignisbenachrichtigungen erforderlich ist, wie in der S3-Benachrichtigungs-API angegeben.
 - Verwenden Sie bei der XML-Konfiguration den URN eines Endpunkt 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 Mandantenmanager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Ereignisbenachrichtigungen** aus.
5. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigungen aktivieren**.
6. Fügen Sie die XML-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

Bucket options
Bucket access
Platform services

Replication
Disabled
▼

Event notifications
Disabled
▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS).

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

Clear

```

<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>
      
```

Save changes



Platformservices müssen für jedes Mandantenkonto von einem StorageGRID-Administrator mithilfe des Grid Manager oder der Grid Management API aktiviert werden. Wenden Sie sich an Ihren StorageGRID-Administrator, wenn beim Speichern der Konfigurations-XML ein Fehler auftritt.

7. Überprüfen Sie, ob Ereignisbenachrichtigungen richtig konfiguriert sind:

- a. Führen Sie eine Aktion für ein Objekt im Quell-Bucket durch, die die Anforderungen für das Auslösen einer Benachrichtigung erfüllt, wie sie in der Konfigurations-XML konfiguriert ist.

In diesem Beispiel wird eine Ereignisbenachrichtigung gesendet, sobald ein Objekt mit dem erstellt wird `images/` Präfix.

- b. Bestätigen Sie, dass eine Benachrichtigung an das Ziel-SNS-Thema gesendet wurde.

Wenn beispielsweise Ihr Zielthema im AWS Simple Notification Service (SNS) gehostet wird, können Sie den Service so konfigurieren, dass Sie eine E-Mail senden, wenn die Benachrichtigung zugestellt wird.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

Wenn die Benachrichtigung im Zielthema empfangen wird, haben Sie Ihren Quell-Bucket für StorageGRID-Benachrichtigungen erfolgreich konfiguriert.

Verwandte Informationen

["Informieren Sie sich über Benachrichtigungen für Buckets"](#)

["S3-REST-API VERWENDEN"](#)

["Endpoint für Plattformservices erstellen"](#)

Verwenden Sie den Suchintegrationsdienst

Der Suchintegrations-Service ist einer der drei StorageGRID Plattform-Services. Sie können diesen Service aktivieren, wenn ein Objekt erstellt, gelöscht oder seine Metadaten oder Tags aktualisiert wird, Objektmetadaten an einen Zielsuchindex zu senden.

Sie können die Suchintegration mit dem Mandanten-Manager konfigurieren, um eine benutzerdefinierte StorageGRID-Konfigurations-XML auf einen Bucket anzuwenden.



Da der Suchintegrationsdienst dazu führt, dass Objektmetadaten an ein Ziel gesendet werden, wird seine Konfigurations-XML als *Metadaten Notification Configuration XML* bezeichnet. Diese Konfigurations-XML unterscheidet sich von der XML-Konfiguration *notification*, die zur Aktivierung von Ereignisbenachrichtigungen verwendet wird.

Siehe ["Anweisungen zur Implementierung von S3-Client-Applikationen"](#) Weitere Informationen zu den folgenden benutzerdefinierten StorageGRID S3 REST-API-Operationen:

- Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN
- Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN
- PUT Bucket-Metadaten-Benachrichtigungskonfiguration

Verwandte Informationen

["Konfigurations-XML für die Integration der Suche"](#)

["Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"](#)

["JSON durch den Suchintegrations-Service generiert"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

["S3-REST-API VERWENDEN"](#)

Konfigurations-XML für die Integration der Suche

Der Such-Integrationsdienst wird anhand einer Reihe von Regeln konfiguriert, die in `<MetadataNotificationConfiguration>` und `</MetadataNotificationConfiguration>` tags: Jede Regel gibt die Objekte an, auf die sich die Regel bezieht, und das Ziel, an dem StorageGRID die Metadaten dieser Objekte senden sollte.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix `images` an ein Ziel und die Metadaten für Objekte mit dem Präfix `videos` nach anderen. Konfigurationen mit überlappenden Präfixen sind nicht gültig und werden beim Einreichen abgelehnt. Beispiel: Eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` und eine zweite Regel für Objekte mit dem Präfix `test2` ist nicht zulässig.

Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden, der für den Suchintegrationsdienst erstellt wurde. Diese Endpunkte beziehen sich auf einen Index und einen Typ, der in einem Elasticsearch-Cluster definiert ist.

```
<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>
```

In der Tabelle werden die Elemente in der XML-Konfiguration für die Metadatenbenachrichtigung beschrieben.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelement.	Ja.
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration Element enthalten.	Ja.
ID	Eindeutige Kennung für die Regel. In das Element Regel aufgenommen.	Nein

Name	Beschreibung	Erforderlich
Status	<p>Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Präfix	<p>Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Urne	<p>URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • es Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl.</p> <p>URNE ist im Element Ziel enthalten.</p>	Ja.

Verwenden Sie die XML-XML-Beispielkonfiguration für Metadatenbenachrichtigungen, um zu erfahren, wie Sie Ihre eigene XML erstellen.

Konfiguration der Metadatenbenachrichtigung für alle Objekte

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>

```

Konfiguration der Metadatenbenachrichtigung mit zwei Regeln

In diesem Beispiel sind die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/images` An ein Ziel gesendet wird, während die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/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-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Verwandte Informationen

["S3-REST-API VERWENDEN"](#)

["Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"](#)

["JSON durch den Suchintegrations-Service generiert"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

Konfigurieren Sie den Suchintegrationsdienst

Der Suchintegrations-Service sendet Objektmetadaten an einen Zielindex bei jedem Erstellen, Löschen oder Aktualisieren der zugehörigen Metadaten oder Tags.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator 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 haben seinen URN.
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Nachdem Sie den Such-Integrationservice für einen Quell-Bucket konfiguriert haben, werden beim Erstellen eines Objekts oder beim Aktualisieren der Metadaten oder Tags eines Objekts Objektmetadaten ausgelöst, die an den Ziel-Endpunkt gesendet werden. Wenn Sie den Suchintegrationservice für einen Bucket aktivieren, der bereits Objekte enthält, werden Metadatenbenachrichtigungen nicht automatisch für vorhandene Objekte gesendet. Sie müssen diese vorhandenen Objekte aktualisieren, um sicherzustellen, dass ihre Metadaten dem Zielsuchindex hinzugefügt werden.

Schritte

1. Verwenden Sie einen Texteditor, um die XML-Metadatenbenachrichtigung zu erstellen, die für die Integration der Suche erforderlich ist.
 - Informationen zur Integration der Suchfunktion finden Sie in den XML-Konfigurationsdaten.
 - Verwenden Sie beim Konfigurieren des XML den URN eines Endpunkt zur Integration der Suche als Ziel.

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. Wählen Sie im Mandantenmanager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Integration suchen**
5. Aktivieren Sie das Kontrollkästchen **Enable search Integration**.

6. Fügen Sie die Konfiguration der Metadatenbenachrichtigung in das Textfeld ein, und wählen Sie **Änderungen speichern**.

Platform services

Replication Disabled

Event notifications Disabled

Search integration Disabled

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

Enable search integration

Clear

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Save changes



Platformservices müssen für jedes Mandantenkonto von einem StorageGRID-Administrator aktiviert werden, der den Grid Manager oder die Management-API verwendet. Wenden Sie sich an Ihren StorageGRID-Administrator, wenn beim Speichern der Konfigurations-XML ein Fehler auftritt.

7. Überprüfen Sie, ob der Suchintegrationsdienst richtig konfiguriert ist:
- Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die Anforderungen für das Auslösen einer Metadatenbenachrichtigung erfüllt, wie in der Konfigurations-XML angegeben.

In dem zuvor gezeigten Beispiel lösen alle Objekte, die dem Bucket hinzugefügt wurden, eine Metadatenbenachrichtigung aus.

- b. Bestätigen Sie, dass ein JSON-Dokument, das die Metadaten und Tags des Objekts enthält, zum im Endpunkt angegebenen Suchindex hinzugefügt wurde.

Nachdem Sie fertig sind

Bei Bedarf können Sie die Suchintegration für einen Bucket mithilfe einer der folgenden Methoden deaktivieren:

- Wählen Sie **STORAGE (S3) > Buckets** und deaktivieren Sie das Kontrollkästchen **Enable search Integration**.
- Wenn Sie die S3-API direkt verwenden, verwenden Sie eine Benachrichtigungsanforderung FÜR DELETE-Bucket-Metadaten. Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie in der Anleitung.

Verwandte Informationen

["Den Suchintegrations-Service verstehen"](#)

["Konfigurations-XML für die Integration der Suche"](#)

["S3-REST-API VERWENDEN"](#)

["Endpunkt für Plattformservices erstellen"](#)

JSON durch den Suchintegrations-Service generiert

Wenn Sie den Such-Integrationsservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielpunkt gesendet, wenn Metadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden.

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden kann, wenn ein Objekt mit dem Schlüssel enthält `SGWS/Tagging.txt` Wird in einem Bucket mit dem Namen erstellt `test`. Der `test` Der Bucket ist nicht versioniert, daher der `versionId` Das 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"
  }
}

```

Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten

In der Tabelle sind alle Felder aufgeführt, die im JSON-Dokument enthalten sind, die beim Aktivierung der Suchintegration an den Zielendpunkt gesendet werden.

Der Dokumentname umfasst, falls vorhanden, den Bucket-Namen, den Objektnamen und die Version-ID.

Typ	Elementname und -Beschreibung
Bucket- und Objektinformationen	bucket: Name des Eimers
key: Objektschlüsselname	versionID: Objektversion, für Objekte in versionierten Buckets
region: Eimer-Region, zum Beispiel us-east-1	System-Metadaten
size: Objektgröße (in Bytes) als sichtbar für einen HTTP-Client	md5: Objekt-Hash
Benutzer-Metadaten	metadata: Alle Benutzer-Metadaten für das Objekt, als Schlüssel-Wert-Paare key:value
Tags	tags: Alle für das Objekt definierten Objekttags, als Schlüsselwert-Paare key:value



Für Tags und Benutzer-Metadaten gibt StorageGRID Daten und Nummern an Elasticsearch als Strings oder als S3-Ereignisbenachrichtigungen weiter. Um Elasticsearch so zu konfigurieren, dass diese Strings als Daten oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen für die dynamische Feldzuordnung und die 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.

S3-REST-API VERWENDEN

Von S3 REST API unterstützte Versionen und Updates

StorageGRID unterstützt die S3-API (Simple Storage Service), die als Satz Rest-Web-Services (Representational State Transfer) implementiert wird.

Dank der Unterstützung für die S3-REST-API können serviceorientierte Applikationen, die für S3-Web-Services entwickelt wurden, mit On-Premises-Objekt-Storage verbunden werden, der das StorageGRID-System verwendet. Es sind minimale Änderungen an der aktuellen Nutzung von S3-REST-API-Aufrufen einer Client-Applikation erforderlich.

Unterstützte Versionen

StorageGRID unterstützt die folgenden spezifischen Versionen von S3 und HTTP.

Element	Version
S3-Spezifikation	<i>Simple Storage Service API Reference</i> 2006-03-01
HTTP	1.1 Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35). Hinweis: StorageGRID unterstützt HTTP/1.1-Pipelining nicht.

Verwandte Informationen

["IETF RFC 2616: Hypertext Transfer Protocol \(HTTP/1.1\)"](#)

["Amazon Web Services \(AWS\) Dokumentation: Amazon Simple Storage Service API Reference"](#)

Updates für die S3-REST-API-Unterstützung

Freigabe	Kommentare
11.7	<ul style="list-style-type: none"> • Hinzugefügt "Schnelle Referenz: Unterstützte S3-API-Anforderungen". • Zusätzliche Unterstützung für die Verwendung DES GOVERNANCE-Modus mit S3 Object Lock. • Zusätzliche Unterstützung für das StorageGRID-spezifische <code>x-ntap-sg-cgr-replication-status</code> Antwortkopf für GET Object- und HEAD-Objektanforderungen. Dieser Header stellt den Replikationsstatus eines Objekts für die Grid-übergreifende Replikation bereit. • SelectObjectContent Requests unterstützen nun Parkett-Objekte.
11.6	<ul style="list-style-type: none"> • Zusätzliche Unterstützung für die Verwendung von <code>partNumber</code> Anforderungsparameter in GET Object und HEAD Object Requests. • Zusätzliche Unterstützung für einen Standardaufbewahrungsmodus und einen Standardaufbewahrungszeitraum auf Bucket-Ebene für S3 Object Lock. • Zusätzliche Unterstützung für die <code>s3:object-lock-remaining-retention-days</code> Richtlinienbedingung-Schlüssel zum Festlegen des Bereichs zulässiger Aufbewahrungsfristen für Ihre Objekte. • Die maximale <i>recommended</i>-Größe für einen einzelnen PUT-Objekt-Vorgang wurde auf 5 gib (5,368,709,120 Bytes) geändert. Wenn Sie über Objekte mit einer Größe von mehr als 5 gib verfügen, verwenden Sie stattdessen mehrteilige Uploads.
11.5	<ul style="list-style-type: none"> • Zusätzliche Unterstützung für das Management der Bucket-Verschlüsselung • Unterstützung für S3 Object Lock und veraltete ältere Compliance-Anforderungen wurde hinzugefügt. • Zusätzliche Unterstützung beim LÖSCHEN mehrerer Objekte in versionierten Buckets. • Der <code>Content-MD5</code> Die Anforderungsüberschrift wird jetzt korrekt unterstützt.
11.4	<ul style="list-style-type: none"> • Unterstützung für DELETE Bucket-Tagging, GET Bucket-Tagging und PUT Bucket-Tagging. Kostenzuordnungstags werden nicht unterstützt. • Bei in StorageGRID 11.4 erstellten Buckets ist keine Beschränkung der Objektschlüsselnamen auf Performance-Best-Practices mehr erforderlich. • Zusätzliche Unterstützung für Bucket-Benachrichtigungen auf der <code>s3:ObjectRestore:Post</code> Ereignistyp. • Die Größenbeschränkungen von AWS für mehrere Teile werden nun durchgesetzt. Jedes Teil eines mehrteiligen Uploads muss zwischen 5 MiB und 5 gib liegen. Der letzte Teil kann kleiner als 5 MiB sein. • Unterstützung für TLS 1.3 hinzugefügt

Freigabe	Kommentare
11.3	<ul style="list-style-type: none"> • Zusätzliche Unterstützung für serverseitige Verschlüsselung von Objektdaten mit vom Kunden bereitgestellten Schlüsseln (SSE-C). • Unterstützung für VORGÄNGE IM Bucket-Lebenszyklus (nur Aktion „Ablauf“) und für den wurde hinzugefügt <code>x-amz-expiration</code> Kopfzeile der Antwort. • Aktualisiertes PUT-Objekt, PUT-Objekt – Copy und Multipart-Upload, um die Auswirkungen von ILM-Regeln zu beschreiben, die synchrone Platzierung bei der Aufnahme verwenden. • TLS 1.1-Chiffren werden nicht mehr unterstützt.
11.2	<p>Unterstützung für DIE WIEDERHERSTELLUNG NACH Objekten wurde hinzugefügt und kann in Cloud-Storage-Pools verwendet werden. Unterstützung für die Verwendung der AWS-Syntax für ARN, Richtlinienzustandsschlüssel und Richtlinienvariablen in Gruppen- und Bucket-Richtlinien Vorhandene Gruppen- und Bucket-Richtlinien, die die StorageGRID-Syntax verwenden, werden weiterhin unterstützt.</p> <p>Hinweis: die Verwendung von ARN/URN in anderen Konfigurationen JSON/XML, einschließlich derjenigen, die in benutzerdefinierten StorageGRID-Funktionen verwendet werden, hat sich nicht geändert.</p>
11.1	Zusätzliche Unterstützung für die Cross-Origin Resource Sharing (CORS), HTTP für S3-Clientverbindungen zu Grid-Nodes und Compliance-Einstellungen für Buckets.
11.0	Unterstützung für die Konfiguration von Plattform-Services (CloudMirror Replizierung, Benachrichtigungen und Elasticsearch-Integration) für Buckets. Außerdem werden Einschränkungen für Objektkennzeichnung bei Buckets sowie die verfügbaren Einstellungen für die Konsistenzsteuerung unterstützt.
10.4	Unterstützung für ILM-Scanning-Änderungen an Versionierung, Seitenaktualisierungen von Endpoint Domain-Namen, Bedingungen und Variablen in Richtlinien, Richtlinienbeispiele und die Berechtigung <code>PutOverwriteObject</code> .
10.3	Zusätzliche Unterstützung für Versionierung
10.2	Unterstützung für Gruppen- und Bucket-Zugriffsrichtlinien und für mehrteilige Kopien (Upload Part - Copy) hinzugefügt
10.1	Unterstützung für mehrteilige Uploads, virtuelle Hosted-Style-Anforderungen und v4 Authentifizierung
10.0	Die erste Unterstützung der S3-REST-API durch das StorageGRID-System. die derzeit unterstützte Version der <i>Simple Storage Service API Reference</i> lautet 2006-03-01.

Schnelle Referenz: Unterstützte S3-API-Anforderungen

Auf dieser Seite wird zusammengefasst, wie StorageGRID Amazon Simple Storage

Service (S3) APIs unterstützt.

Diese Seite umfasst nur die S3-Vorgänge, die von StorageGRID unterstützt werden.



Um die AWS Dokumentation für jeden Vorgang anzuzeigen, klicken Sie in der Überschrift auf den Link.

Allgemeine URI-Abfrageparameter und Anforderungsheader

Sofern nicht angegeben, werden die folgenden gängigen URI-Abfrageparameter unterstützt:

- `versionId` (Bei Bedarf für Objekt-Operationen)

Sofern nicht anders angegeben, werden die folgenden gängigen Anforderungsheader unterstützt:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Verwandte Informationen

- ["Details zur S3-REST-API-Implementierung"](#)
- ["Amazon Simple Storage Service API-Referenz: Common Request Header"](#)

"AbortMeh rteilaUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen zusätzlichen URI-Abfrageparameter:

- `uploadId`

Text anfordern

Keine

StorageGRID-Dokumentation

["Vorgänge für mehrteilige Uploads"](#)

"CompleteMultipartUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen

zusätzlichen URI-Abfrageparameter:

- uploadId

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- CompleteMultipartUpload
- Part
- ETag
- PartNumber

StorageGRID-Dokumentation

["Abschließen Von Mehrteiligen Uploads"](#)

"CopyObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- 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>`

Text anfordern

Keine

StorageGRID-Dokumentation

["PUT Objektkopie"](#)

"CreateBucket"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- x-amz-bucket-object-lock-enabled

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"CreateMultipartUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- 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>`

Text anfordern

Keine

StorageGRID-Dokumentation

["Initiieren Von Mehrteiligen Uploads"](#)

"DeleteBucket"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketLifecycle"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

- ["Operationen auf Buckets"](#)
- ["S3-Lebenszykluskonfiguration erstellen"](#)

"DeleteBucketRichtlinien"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen zusätzlichen Anforderungsheader:

- `x-amz-bypass-governance-retention`

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"Objekte deObjekteObjekte"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen zusätzlichen Anforderungsheader:

- `x-amz-bypass-governance-retention`

Text anfordern

StorageGRID unterstützt alle Parameter des Anforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen für Objekte"](#) (DELETE mehrere Objekte)

"DeleteObjectTagging"

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"GetBucketAcl"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketLifecycleKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

- ["Operationen auf Buckets"](#) (BUCKET-Lebenszyklus ABRUFEN)
- ["S3-Lebenszykluskonfiguration erstellen"](#)

"GetBucketLocation"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketNotificationConfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#) (Bucket-Benachrichtigung ABRUFEN)

"GetBucketPolicy"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketTagging"

URI-Abfrageparameter und Anforderungskopfeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketVersioning"

URI-Abfrageparameter und Anforderungskopfeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetObject"

URI-Abfrageparameter und Anforderungskopfeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen URI-Abfrageparameter:

- 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

Text anfordern

Keine

StorageGRID-Dokumentation

["GET Objekt"](#)

"GetObjectAcl"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"GetObjectLegalHold"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

"GetObjectLockConfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

"GetObjectRetention"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

"GetObjectTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"HeadBucket"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"HeadObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- 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

Text anfordern

Keine

StorageGRID-Dokumentation

["HEAD Objekt"](#)

"ListBuchs"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

[Operationen im Dienst](#) › [SERVICE ABRUFEN](#)

"ListMultipartUploads"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- delimiter
- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

Text anfordern

Keine

StorageGRID-Dokumentation

["Mehnteilige Uploads Auflisten"](#)

"ListObjekte"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- delimiter
- encoding-type
- marker
- max-keys
- prefix

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#) (BUCKET ABRUFEN)

"ListObjekteV2"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#) (BUCKET ABRUFEN)

"ListObjectVersions"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#) (GET Bucket-Objektversionen)

"ListenTeile"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- max-parts

- part-number-marker
- uploadId

Text anfordern

Keine

StorageGRID-Dokumentation

["Mehrteilige Uploads Auflisten"](#)

"PutBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Anforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- ServerSideEncryptionConfiguration
- Rule
- ApplyServerSideEncryptionByDefault
- SSEAlgorithm

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketLifecycleKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- NewerNoncurrentVersions
- LifecycleConfiguration
- Rule

- Expiration
- Days
- Filter
- And
- Prefix
- Tag
- Key
- Value
- Prefix
- Tag
- Key
- Value
- ID
- NoncurrentVersionExpiration
- NoncurrentDays
- Prefix
- Status

StorageGRID-Dokumentation

- ["Operationen auf Buckets"](#) (PUT-Bucket-Lebenszyklus)
- ["S3-Lebenszykluskonfiguration erstellen"](#)

"PutBucketNotificationKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- Prefix
- Suffix
- NotificationConfiguration
- TopicConfiguration
- Event
- Filter
- S3Key
- FilterRule

- Name
- Value
- Id
- Topic

StorageGRID-Dokumentation

["Operationen auf Buckets"](#) (PUT Bucket-Benachrichtigung)

"PutBucketPolicy"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Weitere Informationen zu den unterstützten JSON-Textfeldern finden Sie unter ["Verwendung von Bucket- und Gruppenzugriffsrichtlinien"](#).

"PutBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

- ReplicationConfiguration
- Status
- Prefix
- Destination
- Bucket
- StorageClass
- Rule

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Anforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketVersioning"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Body-Parameter anfordern

StorageGRID unterstützt die folgenden Parameter des Anfragenkörpers:

- VersioningConfiguration
- Status

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- 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>`

Text anfordern

- Binäre Daten des Objekts

StorageGRID-Dokumentation

["PUT Objekt"](#)

"PutObjectLegalHold"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

"PutObjectLockKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

"PutObjectRetention"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzliche Kopfzeile:

- `x-amz-bypass-governance-retention`

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

"PutObjectTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"SelektierObjectContent"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Weitere Informationen zu den unterstützten Textfeldern finden Sie in den folgenden Informationen:

- ["Verwenden Sie S3 Select"](#)
- ["Wählen Sie Objektinhalt Aus"](#)

"UploadTeil"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen URI-Abfrageparameter:

- partNumber
- uploadId

Und diese zusätzlichen Anforderungsheader:

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

Text anfordern

- Binäre Daten des Teils

StorageGRID-Dokumentation

["Hochladen Von Teilen"](#)

"UploadPartCopy"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden 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

Text anfordern

Keine

StorageGRID-Dokumentation

["Hochladen Von Teilen - Kopieren"](#)

Mandantenkonten und -Verbindungen konfigurieren

Wenn StorageGRID konfiguriert wird, um Verbindungen von Client-Applikationen zu akzeptieren, müssen ein oder mehrere Mandantenkonten erstellt und die Verbindungen eingerichtet werden.

S3-Mandantenkonten erstellen und konfigurieren

Bevor S3-API-Clients Objekte auf StorageGRID speichern und abrufen können, ist ein S3-Mandantenkonto erforderlich. Jedes Mandantenkonto hat seine eigene Konto-ID, Gruppen, Benutzer, Buckets und Objekte.

S3-Mandantenkonten werden von einem StorageGRID Grid-Administrator erstellt, der den Grid Manager oder die Grid Management API verwendet. Siehe ["Verwalten von Mandanten"](#) Entsprechende Details. Nach der Erstellung eines S3-Mandantenkontos können Mandantenbenutzer auf den Tenant Manager zugreifen, um Gruppen, Benutzer, Zugriffsschlüssel und Buckets zu managen. Siehe ["Verwenden Sie ein Mandantenkonto"](#) Entsprechende Details.



Benutzer von S3-Mandanten können mit dem Tenant Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen, müssen jedoch Objekte mit einer S3-Client-Applikation aufnehmen und managen. Siehe ["S3-REST-API VERWENDEN"](#) Entsprechende Details.

So konfigurieren Sie Clientverbindungen

Ein Grid-Administrator trifft Konfigurationsmöglichkeiten, die Einfluss darauf haben, wie S3-Clients sich mit StorageGRID verbinden, um Daten zu speichern und abzurufen. Für die Verbindung von StorageGRID mit einer beliebigen S3-Anwendung gibt es vier grundlegende Schritte:

- Führen Sie erforderliche Aufgaben in StorageGRID aus, je nachdem, wie die Clientanwendung eine Verbindung zu StorageGRID herstellt.
- Verwenden Sie StorageGRID, um die Werte abzurufen, die die Anwendung für die Verbindung mit dem Grid benötigt. Sie können entweder ["Verwenden Sie den S3-Einrichtungsassistenten"](#) Oder konfigurieren Sie jede StorageGRID-Einheit manuell.
- Verwenden Sie die S3-Anwendung, um die Verbindung zu StorageGRID abzuschließen. Erstellen Sie DNS-Einträge, um IP-Adressen mit beliebigen Domännennamen zu verknüpfen, die Sie verwenden

möchten.

- Laufende Aufgaben in der Applikation und in StorageGRID werden durchgeführt, um Objekt-Storage über einen längeren Zeitraum zu managen und zu überwachen.

Weitere Informationen zu diesen Schritten finden Sie unter "[Client-Verbindungen konfigurieren](#)".

Für Client-Verbindungen erforderliche Informationen

Zum Speichern oder Abrufen von Objekten stellen S3-Clientanwendungen eine Verbindung zum Load Balancer-Dienst her, der auf allen Admin-Knoten und Gateway-Knoten enthalten ist, oder zum Local Distribution Router (LDR)-Dienst, der auf allen Storage-Nodes enthalten ist.

Client-Applikationen können mithilfe der IP-Adresse eines Grid-Node und der Portnummer des Service auf diesem Node eine Verbindung zu StorageGRID herstellen. Optional können Sie Gruppen für Hochverfügbarkeit (High Availability, HA) von Load-Balancing-Nodes erstellen, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn Sie eine Verbindung zu StorageGRID über einen vollständig qualifizierten Domänennamen (FQDN) anstelle einer IP- oder VIP-Adresse herstellen möchten, können Sie DNS-Einträge konfigurieren.

Siehe "[Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen](#)" Finden Sie weitere Informationen.

Entscheiden Sie sich für die Verwendung von HTTPS- oder HTTP-Verbindungen

Wenn Client-Verbindungen mit einem Load Balancer-Endpunkt hergestellt werden, müssen Verbindungen über das Protokoll (HTTP oder HTTPS) hergestellt werden, das für diesen Endpunkt angegeben wurde. Um HTTP für Clientverbindungen zu Storage Nodes zu verwenden, müssen Sie die Verwendung von HTTP aktivieren.

Wenn Clientanwendungen eine Verbindung zu Storage Nodes herstellen, müssen sie standardmäßig für alle Verbindungen verschlüsseltes HTTPS verwenden. Optional können Sie weniger sichere HTTP-Verbindungen aktivieren, indem Sie im Grid Manager **CONFIGURATION > Security settings > Network and Objects > Enable HTTP for Storage Node Connections** auswählen. Eine Client-Anwendung kann beispielsweise HTTP verwenden, wenn die Verbindung zu einem Speicherknoten in einer nicht produktiven Umgebung getestet wird.



Seien Sie vorsichtig, wenn Sie HTTP für ein Produktionsraster aktivieren, da Anfragen und Antworten unverschlüsselt gesendet werden.

Verwandte Informationen

["StorageGRID verwalten"](#)

["Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen"](#)

S3-Endpunkt-Domänennamen für S3-Anforderungen

Bevor Sie S3-Endpunktdomänennamen für Client-Anfragen verwenden können, muss ein StorageGRID-Administrator das System so konfigurieren, dass Verbindungen akzeptiert werden, die S3-Endpunktdomänennamen im S3-Pfadstil sowie Anforderungen im virtuellen S3-Hoststil verwenden.

Über diese Aufgabe

Um Ihnen die Verwendung von virtuellen S3-Hosted-Style-Anforderungen zu ermöglichen, muss ein Grid-Administrator die folgenden Aufgaben durchführen:

- Verwenden Sie den Grid-Manager, um dem StorageGRID System die S3-Endpunkt-Domain-Namen hinzuzufügen.

- Stellen Sie sicher, dass das Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet, für alle vom Client erforderlichen Domänennamen signiert ist.

Beispiel: Wenn der Endpunkt des S3-API-Service der Domänenendpunkt ist `s3.company.com` Der Grid-Administrator muss sicherstellen, dass das für HTTPS-Verbindungen verwendete Zertifikat vorhanden ist `s3.company.com` Als allgemeiner Betreff und in den alternativen Namen des Subjekts, und `*.s3.company.com` Im Betreff Alternative Namen.

- ["Konfigurieren Sie den DNS-Server"](#) Wird vom Client verwendet, um DNS-Einträge einzubeziehen, die mit den S3-Endpunkt-Domänennamen übereinstimmen, einschließlich aller erforderlichen Platzhaltereinträge.

Wenn der Client über den Load Balancer-Service eine Verbindung herstellt, ist das Zertifikat, das der Grid-Administrator konfiguriert, das Zertifikat für den vom Client verwendeten Load Balancer-Endpunkt.



Jeder Load Balancer-Endpunkt verfügt über ein eigenes Zertifikat. Jeder Endpunkt kann so konfiguriert werden, dass er unterschiedliche S3-Endpunkt-Domänennamen erkennt.

Wenn der Client eine Verbindung zu Storage-Nodes herstellt, ist das vom Grid-Administrator konfigurierten Zertifikat das für das Grid verwendete benutzerdefinierte Serverzertifikat.

Siehe Anweisungen für ["Administration von StorageGRID"](#) Finden Sie weitere Informationen.

Nachdem diese Schritte abgeschlossen sind, können Sie Virtual-Hosted-Style-Anforderungen verwenden.

Testen Sie die S3-REST-API-Konfiguration

Mit der Amazon Web Services Command Line Interface (AWS CLI) können Sie die Verbindung zum System testen und überprüfen, ob Sie Objekte lesen und in das System schreiben können.

Bevor Sie beginnen

- Sie haben die AWS CLI von heruntergeladen und installiert ["aws.amazon.com/cli"](https://aws.amazon.com/cli).
- Sie haben im StorageGRID System ein S3-Mandantenkonto erstellt.
- Sie haben einen Zugriffsschlüssel im Mandantenkonto erstellt.

Schritte

1. Konfigurieren Sie die AWS-CLI-Einstellungen so, dass das im StorageGRID-System erstellte Konto verwendet wird:
 - a. Konfigurationsmodus aufrufen: `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 Standardregion ein, die verwendet werden soll, z. B. US-East-1.
 - e. Geben Sie das zu verwendende Standardausgabeformat ein, oder drücken Sie **Enter**, um JSON auszuwählen.
2. Erstellen eines Buckets:

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:

```
"Location": "/testbucket"
```

3. Hochladen eines Objekts.

```
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
```

Unterstützung von StorageGRID Plattform-Services

Mithilfe der StorageGRID Plattform-Services können StorageGRID-Mandantenkonten externe Services wie einen Remote-S3-Bucket, einen SNS-Endpunkt (Simple Notification Service) oder ein Elasticsearch-Cluster verwenden, um die Services eines Grids zu erweitern.

In der folgenden Tabelle sind die verfügbaren Plattform-Services und die zur Konfiguration verwendeten S3-APIs zusammengefasst.

Plattform-Service	Zweck	Zum Konfigurieren des Service wird die S3-API verwendet
Replizierung von CloudMirror	Repliziert Objekte aus einem StorageGRID-Quell-Bucket in den konfigurierten Remote-S3-Bucket	PUT Bucket-Replikation (siehe "Operationen auf Buckets")
Benachrichtigungen	Sendet Benachrichtigungen zu Ereignissen in einem StorageGRID-Quell-Bucket an einen konfigurierten SNS-Endpunkt (Simple Notification Service).	PUT Bucket-Benachrichtigung (siehe "Operationen auf Buckets")
Integration von Suchen	Sendet Objektmetadaten für Objekte, die in einem StorageGRID Bucket gespeichert sind, an einen konfigurierten Elasticsearch-Index.	"PUT Bucket-Metadaten-Benachrichtigungskonfiguration" Hinweis: Dies ist ein StorageGRID Custom S3 API.

Ein Grid-Administrator muss die Nutzung von Plattformservices für ein Mandantenkonto aktivieren, bevor sie verwendet werden können. Siehe ["StorageGRID verwalten"](#). Anschließend muss ein Mandantenadministrator einen Endpunkt erstellen, der für den Remote-Service im Mandantenkonto steht. Dieser Schritt ist erforderlich, bevor ein Service konfiguriert werden kann. Siehe ["Verwenden Sie ein Mandantenkonto"](#).

Empfehlungen für die Nutzung von Plattform-Services

Vor der Verwendung von Plattform-Services müssen Sie die folgenden Empfehlungen beachten:

- NetApp empfiehlt, nicht mehr als 100 aktive Mandanten mit S3-Anforderungen zu zulassen, die eine CloudMirror-Replizierung, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren S3-Client-Performance führen.
- Wenn in einem S3 Bucket im StorageGRID System sowohl die Versionierung als auch die CloudMirror Replizierung aktiviert sind, empfiehlt NetApp, dass für den Zielpunkt auch die S3-Bucket-Versionierung aktiviert ist. So kann die CloudMirror-Replizierung ähnliche Objektversionen auf dem Endpunkt generieren.
- Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.
- Die CloudMirror-Replikation schlägt mit einem AccessDenied-Fehler fehl, wenn auf dem Ziel-Bucket ältere Compliance-Funktionen aktiviert sind.

So implementiert StorageGRID die S3-REST-API

In Konflikt stehende Clientanforderungen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst.

Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

Konsistenzkontrollen

Konsistenzkontrollen sorgen für ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg, wie von Ihrer Anwendung gefordert.

Standardmäßig garantiert StorageGRID eine Lese-/Nachher-Konsistenz für neu erstellte Objekte. Jeder GET nach einem erfolgreich abgeschlossenen PUT wird in der Lage sein, die neu geschriebenen Daten zu lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen sind schließlich konsistent. Überschreibungen dauern in der Regel nur wenige Sekunden oder Minuten, können jedoch bis zu 15 Tage in Anspruch nehmen.

Wenn Sie Objektvorgänge auf einer anderen Konsistenzstufe ausführen möchten, können Sie für jeden Bucket oder für jeden API-Vorgang eine Konsistenzkontrolle angeben.

Konsistenzkontrollen

Die Konsistenzkontrolle beeinflusst die Verteilung der Metadaten, die StorageGRID zum Verfolgen von Objekten zwischen Nodes verwendet, und somit die Verfügbarkeit von Objekten für Client-Anforderungen.

Sie können die Konsistenzkontrolle für einen Bucket- oder API-Vorgang auf einen der folgenden Werte festlegen:

- **All:** Alle Knoten erhalten die Daten sofort, oder die Anfrage schlägt fehl.
- **Strong-global:** Garantiert Lese-After-Write-Konsistenz für alle Kundenanfragen über alle Standorte hinweg.
- **Strong-site:** Garantiert Lese-After-Write Konsistenz für alle Kundenanfragen innerhalb einer Site.
- **Read-after-New-write:** (Standard) bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
- **Verfügbar:** Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

Verwenden Sie die Consistency Controls „read-after-New-write“ und „available“

Wenn bei einem HEAD oder GET-Vorgang die Konsistenzkontrolle „read-after-New-write“ verwendet wird, führt StorageGRID die Suche in mehreren Schritten durch:

- Es sieht zunächst das Objekt mit einer niedrigen Konsistenz.
- Wenn diese Suche fehlschlägt, wiederholt sie die Suche auf der nächsten Konsistenzebene, bis sie eine Konsistenzstufe erreicht, die dem Verhalten für Strong-Global entspricht.

Wenn eine HEAD- oder GET-Operation das Konsistenzsteuerelement „read-after-New-write“ verwendet, das Objekt aber nicht existiert, erreicht die Objekt-Lookup immer eine Konsistenzstufe, die dem Verhalten für strong-global entspricht. Da für diese Konsistenzstufe mehrere Kopien der Objektmetadaten an jedem Standort verfügbar sein müssen, können Sie eine hohe Anzahl von 500 internen Serverfehlern erhalten, wenn zwei oder mehr Storage-Nodes am selben Standort nicht verfügbar sind.

Sofern Sie keine Konsistenzgarantien ähnlich wie Amazon S3 benötigen, können Sie diese Fehler bei DEN HEAD- und GET-Vorgängen vermeiden, indem Sie die Konsistenzkontrolle auf „Available“ setzen. Wenn bei

einem HEAD oder GET-Vorgang die Konsistenzkontrolle „Available“ verwendet wird, bietet StorageGRID eventuell nur Konsistenz. Bei einem fehlgeschlagenen Vorgang wird nicht erneut versucht, die Konsistenzstufen zu erhöhen, daher müssen nicht mehrere Kopien der Objekt-Metadaten verfügbar sein.

Festlegen der Konsistenzkontrolle für den API-Betrieb

Um die Consistency Control für einen einzelnen API-Vorgang festzulegen, müssen für den Vorgang Konsistenzkontrollen unterstützt werden, und Sie müssen die Consistency Control in der Anforderungs-Kopfzeile angeben. In diesem Beispiel wird die Consistency Control auf „strong-site“ für EINE GET Object Operation gesetzt.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Sie müssen für DEN PUT-Objekt- und DEN GET-Objektbetrieb dasselbe Konsistenzsteuerelement verwenden.

Festlegen der Konsistenzkontrolle für Bucket

Zum Festlegen der Konsistenzkontrolle für Bucket können Sie die StorageGRID PUT Bucket-Konsistenzanforderung und DIE ANFORDERUNG FÜR GET-Bucket-Konsistenz verwenden. Alternativ können Sie den Tenant Manager oder die Mandantenmanagement-API verwenden.

Beachten Sie beim Festlegen der Konsistenzkontrollen für einen Bucket Folgendes:

- Durch das Festlegen der Konsistenzkontrolle für einen Bucket wird festgelegt, welche Konsistenzkontrolle für S3-Operationen verwendet wird, die für Objekte im Bucket oder in der Bucket-Konfiguration durchgeführt werden. Er hat keine Auswirkungen auf die Vorgänge auf dem Bucket selbst.
- Die Konsistenzkontrolle für einen einzelnen API-Vorgang überschreibt die Konsistenzkontrolle für den Bucket.
- Im Allgemeinen sollten Buckets die Standardkonsistenzkontrolle „read-after-New-write.“ verwenden. Wenn die Anforderungen nicht korrekt funktionieren, ändern Sie das Client-Verhalten der Anwendung, wenn möglich. Oder konfigurieren Sie den Client so, dass für jede API-Anforderung das Consistency Control angegeben wird. Legen Sie die Consistency Control auf Bucket-Ebene nur als letztes Resort fest.

wie Konsistenzkontrollen und ILM-Regeln interagieren, um den Datenschutz zu beeinträchtigen

Die Wahl der Konsistenzkontrolle und der ILM-Regel haben Auswirkungen auf den Schutz von Objekten. Diese Einstellungen können interagieren.

Die beim Speichern eines Objekts verwendete Konsistenzkontrolle beeinflusst beispielsweise die anfängliche Platzierung von Objekt-Metadaten, während das für die ILM-Regel ausgewählte Aufnahmeverhalten sich auf die anfängliche Platzierung von Objektkopien auswirkt. Da StorageGRID Zugriff auf die Metadaten eines Objekts und seine Daten benötigt, um Kundenanforderungen zu erfüllen, kann die Auswahl der passenden Sicherungsstufen für Konsistenz und Aufnahme-Verhalten eine bessere Erstsicherung und zuverlässigere Systemantworten ermöglichen.

Die folgenden Aufnahmeverhalten stehen für ILM-Regeln zur Verfügung:

- **Dual Commit:** StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Client zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.
- **Streng:** Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor der Erfolg an den Client zurückgesendet wird.
- **Ausgewogen:** StorageGRID versucht bei der Aufnahme alle in der ILM-Regel festgelegten Kopien zu erstellen; wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg an den Client zurückgesendet. Die Kopien, die in der ILM-Regel angegeben sind, werden, wenn möglich gemacht.



Lesen Sie vor der Auswahl des Aufnahmeverhaltens für eine ILM-Regel die vollständige Beschreibung dieser Einstellungen in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Beispiel für die Interaktion zwischen Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel:** Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe:** „strong-global“ (Objektmetadaten werden sofort auf alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „strong-site“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten an den Remote Standort repliziert wurden, aber bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Get Bucket-Konsistenz"](#)

["PUT Bucket-Konsistenz"](#)

Managen von Objekten durch StorageGRID ILM-Regeln

Der Grid-Administrator erstellt Informationen Lifecycle Management (ILM)-Regeln für das Management von Objektdaten, die von S3-REST-API-Client-Applikationen in das StorageGRID-System aufgenommen werden. Diese Regeln werden dann zur ILM-Richtlinie hinzugefügt, um zu bestimmen, wie und wo Objektdaten im Laufe der Zeit gespeichert werden.

ILM-Einstellungen bestimmen die folgenden Aspekte eines Objekts:

- **Geographie**

Der Speicherort der Objektdaten kann entweder im StorageGRID-System (Storage-Pool) oder in einem Cloud-Storage-Pool gespeichert werden.

- * Speicherklasse*

Storage-Typ zur Speicherung von Objektdaten, z. B. Flash oder rotierende Festplatte

- **Verlustschutz**

Wie viele Kopien erstellt werden und welche Arten von Kopien erstellt werden: Replizierung, Erasure Coding oder beides.

- **Aufbewahrung**

Es ändert sich im Laufe der Zeit, wie Objektdaten verwaltet werden, wo sie gespeichert sind und wie sie vor Verlust geschützt sind.

- **Schutz während der Aufnahme**

Methode zum Schutz von Objektdaten bei der Aufnahme: Synchrone Platzierung (mit ausgeglichenen oder strengen Optionen für das Aufnahmeverhalten) oder Erstellung von vorläufigen Kopien (unter Verwendung der Option Dual-Commit)

ILM-Regeln können Objekte filtern und auswählen. Bei mit S3 aufgenommenen Objekten können ILM-Regeln Objekte auf Basis der folgenden Metadaten filtern:

- Mandantenkonto
- Bucket-Name
- Aufnahmezeit
- Taste
- Zeitpunkt des letzten Zugriffs



Standardmäßig werden Updates der letzten Zugriffszeit für alle S3 Buckets deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option „Letzte Zugriffszeit“ verwendet, müssen Sie für die in dieser Regel angegebenen S3 Buckets Updates für den letzten Zugriff aktivieren. Verwenden Sie die Anforderung ZUM letzten Zugriff auf Bucket, den Tenant Manager (siehe) "[Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit](#)") Oder die Mandanten-Management-API. Beachten Sie bei der Aktivierung von Updates der letzten Zugriffszeit, dass die Performance von StorageGRID möglicherweise reduziert wird, insbesondere bei Systemen mit kleinen Objekten.

- Positionsbeschränkung
- Objektgröße
- Benutzer-Metadaten
- Objekt-Tag

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

["Objektmanagement mit ILM"](#)

["PUT Bucket-Zeit für den letzten Zugriff"](#)

Objektversionierung

Sie können mithilfe der Versionierung mehrere Versionen eines Objekts aufbewahren, das vor versehentlichem Löschen von Objekten schützt und Ihnen das Abrufen und Wiederherstellen älterer Versionen eines Objekts ermöglicht.

Das StorageGRID System implementiert Versionierung mit Unterstützung für die meisten Funktionen und weist einige Einschränkungen auf. StorageGRID unterstützt bis zu 1,000 Versionen jedes Objekts.

Die Objektversionierung kann mit StorageGRID Information Lifecycle Management (ILM) oder mit der S3 Bucket Lifecycle-Konfiguration kombiniert werden. Sie müssen für jeden Bucket die Versionierung aktivieren, um diese Funktion für den Bucket zu aktivieren. Jedem Objekt im Bucket wird eine Version-ID zugewiesen, die vom StorageGRID-System generiert wird.

Die Verwendung von MFA (Multi-Faktor-Authentifizierung) Löschen wird nicht unterstützt.



Die Versionierung kann nur auf 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 bewertet sie anhand der aktuellen ILM-Richtlinie neu. Alle Änderungen, die Sie an ILM-Richtlinien vornehmen, werden auf alle zuvor aufgenommenen Objekte angewendet. Dies umfasst bereits aufgenommene Versionen, wenn die Versionierung aktiviert ist. Beim ILM-Scannen werden neue ILM-Änderungen an zuvor aufgenommenen Objekten angewendet.

Bei S3-Objekten in versionierungsfähigen Buckets können Sie mithilfe der Versionierungsunterstützung ILM-Regeln erstellen, die „noncurrent time“ als Referenzzeit verwenden. Wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ aus. Zoll "[Schritt 1 des Assistenten zum Erstellen einer ILM-Regel](#)". Wenn ein Objekt aktualisiert wird, werden seine vorherigen Versionen nicht aktuell. Mit dem Filter „noncurrent time“ können Sie Richtlinien erstellen, die die Auswirkungen früherer Objektversionen auf den Storage verringern.



Wenn Sie eine neue Version eines Objekts über einen mehrteiligen Upload-Vorgang hochladen, wird der nicht aktuelle Zeitpunkt für die Originalversion des Objekts angezeigt, wenn der mehrteilige Upload für die neue Version erstellt wurde, nicht erst nach Abschluss des mehrteiligen Uploads. In begrenzten Fällen kann die nicht aktuelle Zeit der ursprünglichen Version Stunden oder Tage früher als die Zeit für die aktuelle Version sein.

Siehe "[ILM-Regeln und Richtlinien für versionierte S3-Objekte \(Beispiel 4\)](#)".

Konfigurieren Sie die S3-Objektsperre über die S3-REST-API

Wenn die globale S3-Objektsperre für Ihr StorageGRID-System aktiviert ist, können Sie Buckets mit aktivierter S3-Objektsperre erstellen. Sie können für jeden Bucket oder

die Aufbewahrungseinstellungen für jede Objektversion die Standardaufbewahrung festlegen.

Aktivieren der S3-Objektsperre für einen Bucket

Wenn die globale S3-Objektsperreneinstellung für Ihr StorageGRID-System aktiviert ist, können Sie bei der Erstellung jedes Buckets optional die S3-Objektsperre aktivieren.

S3 Object Lock ist eine permanente Einstellung, die nur beim Erstellen eines Buckets aktiviert werden kann. Sie können S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde.

Verwenden Sie eine der folgenden Methoden, um S3 Object Lock für einen Bucket zu aktivieren:

- Erstellen Sie den Bucket mit Tenant Manager. Siehe "[S3-Bucket erstellen](#)".
- Erstellen Sie den Bucket mithilfe einer PUT-Bucket-Anforderung zusammen mit dem `x-amz-bucket-object-lock-enabled` Kopfzeile der Anfrage. Siehe "[Operationen auf Buckets](#)".

S3 Object Lock erfordert eine Bucket-Versionierung, die beim Erstellen des Buckets automatisch aktiviert wird. Die Versionierung für den Bucket kann nicht unterbrochen werden. Siehe "[Objektversionierung](#)".

Standardeinstellungen für die Aufbewahrung eines Buckets

Wenn S3 Object Lock für einen Bucket aktiviert ist, können Sie optional die Standardaufbewahrung für den Bucket aktivieren und einen Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer festlegen.

Standardaufbewahrungsmodus

- Im COMPLIANCE-Modus:
 - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
 - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
 - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im GOVERNANCE-Modus:
 - Benutzer mit `s3:BypassGovernanceRetention` Berechtigung kann den verwenden `x-amz-bypass-governance-retention: true` Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen.
 - Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
 - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Standardaufbewahrungszeitraum

Für jeden Bucket kann ein Standardaufbewahrungszeitraum in Jahren oder Tagen angegeben werden.

Festlegen der Standardaufbewahrung für einen Bucket

Verwenden Sie eine der folgenden Methoden, um die Standardaufbewahrung für einen Bucket festzulegen:

- Managen Sie die Bucket-Einstellungen über den Tenant Manager. Siehe "[Erstellen eines S3-Buckets](#)" Und "[Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung](#)".
- Stellen Sie eine ANFORDERUNG ZUR OBJEKTSPERRKONFIGURATION für den Bucket AUS, um den Standardmodus und die Standardanzahl von Tagen oder Jahren festzulegen.

PUT Objekt Lock-Konfiguration

Mit DER ANFORDERUNG „OBJEKTSPERRKONFIGURATION“ KÖNNEN Sie den Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum für einen Bucket festlegen und ändern, für den S3 Object Lock aktiviert ist. Sie können auch zuvor konfigurierte Standardeinstellungen entfernen.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der standardmäßige Aufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` Und `x-amz-object-lock-retain-until-date` Sind nicht angegeben. Der Standardaufbewahrungszeitraum wird verwendet, um das Aufbewahrungsdatum von IF zu berechnen `x-amz-object-lock-retain-until-date` Ist nicht angegeben.

Wenn der Standardaufbewahrungszeitraum nach der Aufnahme einer Objektversion geändert wird, bleibt das „bis-Aufbewahrung“-Datum der Objektversion identisch und wird im neuen Standardaufbewahrungszeitraum nicht neu berechnet.

Sie müssen die haben `s3:PutBucketObjectLockConfiguration` Berechtigung, oder Konto root, um diesen Vorgang abzuschließen.

Der `Content-MD5` Der Anforderungskopf muss in der PUT-Anforderung angegeben werden.

Anforderungsbeispiel

In diesem Beispiel wird S3 Object Lock für einen Bucket aktiviert und der Standardaufbewahrungsmodus auf COMPLIANCE und der Standardaufbewahrungszeitraum auf 6 Jahre festgelegt.

```
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>
```

Bestimmen der Standardaufbewahrung für einen Bucket

Verwenden Sie eine der folgenden Methoden, um zu ermitteln, ob S3 Object Lock für einen Bucket aktiviert ist und den Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum anzuzeigen:

- Zeigen Sie den Bucket im Tenant Manager an. Siehe ["S3 Buckets anzeigen"](#).
- Geben Sie eine Anforderung ZUM ABRUFEN der Objektsperrenkonfiguration aus.

Konfiguration der Objektsperre ABRUFEN

Mit der Anforderung OBJEKTSPERRKONFIGURATION ABRUFEN können Sie festlegen, ob S3 Object Lock für einen Bucket aktiviert ist. Ist diese Option aktiviert, können Sie prüfen, ob für den Bucket ein Standardaufbewahrungsmodus und eine Aufbewahrungsfrist konfiguriert sind.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der standardmäßige Aufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` ist nicht angegeben. Der Standardaufbewahrungszeitraum wird verwendet, um das Aufbewahrungsdatum von IF zu berechnen `x-amz-object-lock-retain-until-date` ist nicht angegeben.

Sie müssen die haben `s3:GetBucketObjectLockConfiguration` Berechtigung, oder Konto root, 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/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
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>
```

Festlegen von Aufbewahrungseinstellungen für ein Objekt

Ein Bucket mit aktivierter S3-Objektsperre kann eine Kombination von Objekten mit und ohne Aufbewahrungseinstellungen für S3-Objektsperre enthalten.

Aufbewahrungseinstellungen auf Objektebene werden über die S3-REST-API angegeben. Die Aufbewahrungseinstellungen für ein Objekt überschreiben alle Standardaufbewahrungseinstellungen für den Bucket.

Sie können für jedes Objekt die folgenden Einstellungen festlegen:

- **Retention Mode:** Entweder COMPLIANCE oder GOVERNANCE.
- **Bis-Datum behalten:** Ein Datum, das angibt, wie lange die Objektversion von StorageGRID beibehalten werden muss.
 - Wenn im COMPLIANCE-Modus das Aufbewahrungsdatum in der Zukunft liegt, kann das Objekt abgerufen, aber nicht geändert oder gelöscht werden. Das Aufbewahrungsdatum kann erhöht werden, aber dieses Datum kann nicht verringert oder entfernt werden.
 - Im GOVERNANCE-Modus können Benutzer mit besonderer Berechtigung die Einstellung „bis zum Datum behalten“ umgehen. Sie können eine Objektversion löschen, bevor der Aufbewahrungszeitraum abgelaufen ist. Außerdem können sie das Aufbewahrungsdatum erhöhen, verringern oder sogar entfernen.
- **Legal Hold:** Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflicht hat kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten.

Die Legal Hold-Einstellung für ein Objekt ist unabhängig vom Aufbewahrungsmodus und dem Aufbewahrungsdatum. Befindet sich eine Objektversion unter einem Legal Hold, kann diese Version nicht

gelöscht werden.

Wenn Sie beim Hinzufügen einer Objektversion zu einem Bucket S3-Objektsperreinstellungen angeben möchten, geben Sie ein "PUT Objekt", "PUT Objekt - Kopieren", Oder "Initiieren Von Mehrteiligen Uploads" Anfrage.

Sie können Folgendes verwenden:

- `x-amz-object-lock-mode`, Die COMPLIANCE oder GOVERNANCE sein können (Groß-/Kleinschreibung beachten).



Wenn Sie angeben `x-amz-object-lock-mode`, Sie müssen auch angeben `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
 - Der Wert für „bis-Datum beibehalten“ muss das Format aufweisen `2020-08-10T21:46:00Z`. Fraktionale Sekunden sind zulässig, aber nur 3 Dezimalstellen bleiben erhalten (Präzision in Millisekunden). Andere ISO 8601-Formate sind nicht zulässig.
 - Das „Aufbewahrung bis“-Datum muss in der Zukunft liegen.
- `x-amz-object-lock-legal-hold`

Wenn die gesetzliche Aufbewahrungspflichten LIEGEN (Groß-/Kleinschreibung muss beachtet werden), wird das Objekt unter einer gesetzlichen Aufbewahrungspflichten platziert. Wenn die gesetzliche Aufbewahrungspflichten AUS DEM WEG gehen, wird keine gesetzliche Aufbewahrungspflichten platziert. Jeder andere Wert führt zu einem 400-Fehler (InvalidArgument).

Wenn Sie eine dieser Anfrageheadern verwenden, beachten Sie die folgenden Einschränkungen:

- Der `Content-MD5` Der Anforderungskopf ist erforderlich `x-amz-object-lock-*` In DER PUT-Objektanforderung ist eine Anforderungsüberschrift vorhanden. `Content-MD5` Ist für PUT Object – Copy oder Initiierung von mehrteiligen Uploads nicht erforderlich.
- Wenn für den Bucket die S3-Objektsperre nicht aktiviert ist und ein `x-amz-object-lock-*` Der Anforderungskopf ist vorhanden, es wird ein 400-Fehler (InvalidRequest) zurückgegeben.
- Die PUT-Objektanforderung unterstützt die Verwendung von `x-amz-storage-class: REDUCED_REDUNDANCY` Passend zum Verhalten von AWS. Wird ein Objekt jedoch mit aktivierter S3-Objektsperre in einen Bucket aufgenommen, führt StorageGRID immer eine Dual-Commit-Aufnahme durch.
- Eine nachfolgende ANTWORT AUF GET- oder HEAD Object-Version enthält die Kopfzeilen `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, und `x-amz-object-lock-legal-hold`, Wenn konfiguriert und wenn der Anforderungssender die richtige hat `s3:Get*` Berechtigungen.

Sie können das verwenden `s3:object-lock-remaining-retention-days` Policy Condition Key zur Begrenzung der minimalen und maximalen zulässigen Aufbewahrungsfristen für Ihre Objekte.

Aktualisieren von Aufbewahrungseinstellungen für ein Objekt

Wenn Sie die Einstellungen für die gesetzliche Aufbewahrungs- oder Aufbewahrungseinstellung einer vorhandenen Objektversion aktualisieren müssen, können Sie die folgenden Vorgänge der Unterressource des Objekts ausführen:

- PUT Object legal-hold

Wenn der neue Legal-Hold-Wert AKTIVIERT ist, wird das Objekt unter einer gesetzlichen Aufbewahrungspflichten platziert. Wenn DER Rechtsvorenthalten-Wert DEAKTIVIERT ist, wird die gesetzliche Aufbewahrungspflichten aufgehoben.

- PUT Object retention
 - Der Wert des Modus kann COMPLIANCE oder GOVERNANCE sein (Groß-/Kleinschreibung muss beachtet werden).
 - Der Wert für „bis-Datum beibehalten“ muss das Format aufweisen 2020-08-10T21:46:00Z. Fraktionale Sekunden sind zulässig, aber nur 3 Dezimalstellen bleiben erhalten (Präzision in Millisekunden). Andere ISO 8601-Formate sind nicht zulässig.
 - Wenn eine Objektversion über ein vorhandenes Aufbewahrungsdatum verfügt, können Sie sie nur erhöhen. Der neue Wert muss in der Zukunft liegen.

So verwenden Sie DEN GOVERNANCE-Modus

Benutzer, die über das verfügen `s3:BypassGovernanceRetention` Berechtigung kann die aktiven Aufbewahrungseinstellungen eines Objekts umgehen, das DEN GOVERNANCE-Modus verwendet. Alle LÖSCHVORGÄNGE für die Objektaufbewahrung müssen den enthalten `x-amz-bypass-governance-retention:true` Kopfzeile der Anfrage. Diese Benutzer können die folgenden zusätzlichen Vorgänge ausführen:

- Führen SIE VORGÄNGE ZUM LÖSCHEN von Objekten aus oder LÖSCHEN Sie mehrere Objekte, um eine Objektversion vor Ablauf des Aufbewahrungszeitraums zu löschen.

Objekte, die sich unter einem Legal Hold befinden, können nicht gelöscht werden. Legal Hold muss DEAKTIVIERT sein.

- Führen SIE PUT Objektaufbewahrungsvorgänge durch, bei denen der Modus einer Objektversion von GOVERNANCE zu COMPLIANCE geändert wird, bevor der Aufbewahrungszeitraum des Objekts abgelaufen ist.

Die Änderung des Modus von COMPLIANCE zu GOVERNANCE ist niemals zulässig.

- Führen SIE PUT Objektaufbewahrungsvorgänge durch, um den Aufbewahrungszeitraum einer Objektversion zu erhöhen, zu verringern oder zu entfernen.

Verwandte Informationen

- ["Objekte managen mit S3 Object Lock"](#)
- ["Verwenden Sie S3 Objektsperre, um Objekte beizubehalten"](#)
- ["Amazon Simple Storage Service Benutzerhandbuch: S3 Object Lock verwenden"](#)

S3-Lebenszykluskonfiguration erstellen

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 das Löschen bestimmter Objekte aus bestimmten S3-Buckets kontrollieren kann. Das Beispiel in diesem Abschnitt dient nur zu Illustrationszwecken. Weitere Informationen zum Erstellen von S3-Lebenszykluskonfigurationen

finden Sie unter ["Amazon Simple Storage Service Developer Guide: Lifecycle Management von Objekten"](#). Beachten Sie, dass StorageGRID nur Aktionen nach Ablauf unterstützt. Es werden keine Aktionen zur Transition unterstützt.

Welche Lifecycle-Konfiguration ist

Eine Lifecycle-Konfiguration 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 einigen Tagen).

StorageGRID unterstützt in einer Lebenszykluskonfiguration bis zu 1,000 Lebenszyklusregeln. Jede Regel kann die folgenden XML-Elemente enthalten:

- Ablauf: Löschen eines Objekts, wenn ein bestimmtes Datum erreicht wird oder wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend mit dem Zeitpunkt der Aufnahme des Objekts.
- NoncurrentVersionExpiration: Löschen Sie ein Objekt, wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend ab dem Zeitpunkt, an dem das Objekt nicht mehr aktuell wurde.
- Filter (Präfix, Tag)
- Status
- ID

Wenn Sie eine Lifecycle-Konfiguration auf einen Bucket anwenden, überschreiben die Lifecycle-Einstellungen für den Bucket immer die StorageGRID-ILM-Einstellungen. StorageGRID verwendet die Verfallseinstellungen für den Bucket und nicht ILM, um zu bestimmen, ob bestimmte Objekte gelöscht oder aufbewahrt werden sollen.

Aus diesem Grund kann ein Objekt aus dem Grid entfernt werden, obwohl die Speicheranweisungen in einer ILM-Regel noch auf das Objekt gelten. Alternativ kann ein Objekt auch dann im Grid aufbewahrt werden, wenn eine ILM-Platzierungsanleitung für das Objekt abgelaufen ist. Weitere Informationen finden Sie unter ["Funktionsweise von ILM während der gesamten Nutzungsdauer eines Objekts"](#).



Die Bucket-Lifecycle-Konfiguration kann für Buckets verwendet werden, für die S3-Objektsperre aktiviert ist. Die Bucket-Lifecycle-Konfiguration wird jedoch für ältere Buckets, die Compliance verwenden, nicht unterstützt.

StorageGRID unterstützt den Einsatz der folgenden Bucket-Operationen zum Management der Lebenszykluskonfigurationen:

- Bucket-Lebenszyklus LÖSCHEN
- BUCKET-Lebenszyklus ABRUFEN
- PUT Bucket-Lebenszyklus

Lebenszykluskonfiguration erstellen

Als erster Schritt beim Erstellen einer Lebenszykluskonfiguration erstellen Sie eine JSON-Datei mit einem oder mehreren Regeln. Diese JSON-Datei enthält beispielsweise drei Regeln:

1. Regel 1 gilt nur für Objekte, die mit dem Präfix übereinstimmen `category1/` Und das hat ein `key2` Der Wert von `tag2`. Der `Expiration` Der Parameter gibt an, dass Objekte, die dem Filter entsprechen, um Mitternacht am 22. August 2020 ablaufen.
2. Regel 2 gilt nur für Objekte, die mit dem Präfix übereinstimmen `category2/`. Der `Expiration` Parameter

gibt an, dass Objekte, die dem Filter entsprechen, 100 Tage nach der Aufnahme ablaufen.



Regeln, die eine Anzahl von Tagen angeben, sind relativ zu dem Zeitpunkt, an dem das Objekt aufgenommen wurde. 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` Parameter gibt an, dass nicht aktuelle Versionen übereinstimmender Objekte 50 Tage nach deren Nichtstrom 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"
    }
  ]
}

```

Lifecycle-Konfiguration auf Bucket anwenden

Nachdem Sie die Lifecycle-Konfigurationsdatei erstellt haben, wenden Sie sie durch Ausgabe einer PUT Bucket Lifecycle-Anforderung auf einen Bucket an.

Diese Anforderung wendet die Lebenszykluskonfiguration in der Beispieldatei auf Objekte in einem Bucket mit dem Namen an `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Um zu überprüfen, ob eine Lifecycle-Konfiguration erfolgreich auf den Bucket angewendet wurde, geben Sie eine ANFORDERUNG FÜR DEN GET Bucket-Lebenszyklus aus. Beispiel:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Eine erfolgreiche Antwort zeigt die Konfiguration des Lebenszyklus, die Sie gerade angewendet haben.

Überprüfen, ob der Bucket-Lebenszyklus für das Objekt gilt

Sie können feststellen, ob eine Ablaufregel in der Lebenszykluskonfiguration auf ein bestimmtes Objekt angewendet wird, wenn Sie eine PUT-Objekt-, HEAD-Objekt- oder GET-Objektanforderung ausgeben. Wenn eine Regel zutrifft, enthält die Antwort ein `Expiration` Parameter, der angibt, wann das Objekt abläuft und welche Ablaufregel übereinstimmt.



Da der Bucket-Lebenszyklus ILM überschreibt, wird der `expiry-date` Hier wird das tatsächliche Datum angezeigt, an dem das Objekt gelöscht wird. Weitere Informationen finden Sie unter "[Wie die Aufbewahrung von Objekten bestimmt wird](#)".

Zum Beispiel, diese PUT Objekt Anfrage wurde am 22. Juni 2020 und platziert ein Objekt in der `testbucket` Eimer.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

Die Erfolgsreaktion zeigt an, dass das Objekt in 100 Tagen (01. Oktober 2020) abläuft und dass es mit Regel 2 der Lebenszykluskonfiguration übereinstimmt.

```
{
  *Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
  ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Diese HEAD Object-Anfrage wurde beispielsweise verwendet, um Metadaten für dasselbe Objekt im Testbucket zu erhalten.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

Die Erfolgsreaktion umfasst die Metadaten des Objekts und gibt an, dass das Objekt in 100 Tagen abläuft und dass es mit Regel 2 übereinstimmt.

```
{
  "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": {}
}
```

Empfehlungen für die Implementierung der S3-REST-API

Bei der Implementierung der S3-REST-API zur Verwendung mit StorageGRID sollten Sie diese Empfehlungen beachten.

Empfehlungen für Köpfe zu nicht vorhandenen Objekten

Wenn Ihre Anwendung regelmäßig prüft, ob ein Objekt an einem Pfad vorhanden ist, wo Sie nicht erwarten, dass das Objekt tatsächlich existiert, sollten Sie die Konsistenzkontrolle „available“ verwenden. Verwenden Sie zum Beispiel die Konsistenzkontrolle „Available“, wenn Ihre Anwendung einen Speicherort vor DEM ANSETZEN an sie leitet.

Andernfalls werden möglicherweise 500 Fehler des internen Servers angezeigt, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.

Sie können die Konsistenzkontrolle „Available“ für jeden Bucket mithilfe der PUT Bucket-Konsistenzanforderung festlegen oder Sie können die Konsistenzkontrolle in der Anforderungs-Kopfzeile für einen einzelnen API-Vorgang festlegen.

Empfehlungen für Objektschlüssel

Befolgen Sie diese Empfehlungen für Objektschlüsselnamen auf Basis des ersten Erstells des Buckets.

Buckets, die in StorageGRID 11.4 oder früher erstellt wurden

- Verwenden Sie keine Zufallswerte als die ersten vier Zeichen von Objektschlüsseln. Dies steht im Gegensatz zu der früheren AWS Empfehlung für wichtige Präfixe. Verwenden Sie stattdessen nicht zufällige, nicht eindeutige Präfixe, z. B. `image`.
- Wenn Sie der früheren AWS-Empfehlung folgen, zufällige und eindeutige Zeichen in Schlüsselpräfixen zu verwenden, setzen Sie den Objektschlüsseln einen Verzeichnisnamen vor. Verwenden Sie dieses Format:

```
mybucket/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

```
mybucket/f8e3-image3132.jpg
```

Buckets, die in StorageGRID 11.4 oder höher erstellt wurden

Es ist nicht erforderlich, Objektschlüsselnamen auf die Best Practices für die Performance zu beschränken. In den meisten Fällen können Sie zufällige Werte für die ersten vier Zeichen von Objektschlüsselnamen verwenden.



Eine Ausnahme ist ein S3-Workload, der nach kurzer Zeit kontinuierlich alle Objekte entfernt. Um die Auswirkungen auf die Performance in diesem Anwendungsfall zu minimieren, variieren Sie alle tausend Objekte mit einem ähnlichen Datum einen führenden Teil des Schlüsselnamens. Angenommen, ein S3-Client schreibt in der Regel 2,000 Objekte/Sekunde, und die ILM- oder Bucket-Lifecycle-Richtlinie entfernt alle Objekte nach drei Tagen. Um die Auswirkungen auf die Performance zu minimieren, können Sie Schlüssel anhand eines Musters wie folgt benennen: `/mybucket/mydir/yyyymddhhmmss-random_UUID.jpg`

Empfehlungen für „Range reads“

Wenn der "[Globale Option zum Komprimieren gespeicherter Objekte](#)" Ist aktiviert, sollten S3-Client-Applikationen die Ausführung VON OPERATIONEN FÜR DAS ABRUFEN von Objekten verhindern, die einen Bereich von zurückgegebenen Bytes angeben. Diese Vorgänge „range Read“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. VORGÄNGE ZUM ABRUFEN von Objekten, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.



Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Verwandte Informationen

- "[Konsistenzkontrollen](#)"
- "[PUT Bucket-Konsistenz](#)"
- "[StorageGRID verwalten](#)"

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 der meisten Operationen und mit einigen Einschränkungen. Wenn Sie S3 REST-API-Client-Applikationen integrieren, sind die Implementierungsdetails bekannt.

Das StorageGRID System unterstützt sowohl Virtual-Hosted-Style-Anforderungen als auch Anforderungen im Pfadstil.

Umgang mit Daten

Die StorageGRID Implementierung der S3-REST-API unterstützt nur gültige HTTP-Datumsformate.

Das StorageGRID-System unterstützt nur gültige HTTP-Datumsformate für alle Header, die Datumswerte akzeptieren. Der Zeitbereich des Datums kann im Greenwich Mean Time (GMT)-Format oder im UTC-Format (Universal Coordinated Time) ohne Zeitzonensversatz angegeben werden (+0000 muss angegeben werden). Wenn Sie die einschließen `x-amz-date` Kopfzeile in Ihrer Anfrage, es überschreibt alle Werte, die in der Kopfzeile der Datumsanforderung angegeben sind. Bei Verwendung von AWS Signature Version 4, das `x-amz-date` Die Kopfzeile muss in der signierten Anforderung vorhanden sein, da die Datumsüberschrift nicht unterstützt wird.

Allgemeine Anfragemöpfe

Das StorageGRID-System unterstützt die von definierten allgemeinen Anforderungsheader "[Amazon Simple Storage Service API-Referenz: Common Request Header](#)", Mit einer Ausnahme.

Kopfzeile der Anfrage	Implementierung
Autorisierung	Vollständige Unterstützung für AWS Signature Version 2 Unterstützung für AWS Signature Version 4, mit folgenden Ausnahmen: <ul style="list-style-type: none">• Der SHA256-Wert wird für den Körper der Anforderung nicht berechnet. Der vom Benutzer eingereichte Wert wird ohne Validierung angenommen, als ob der Wert <code>UNSIGNED-PAYLOAD</code> War für die vorgesehenen <code>x-amz-content-sha256</code> Kopfzeile.
X-amz-Sicherheits-Token	Nicht implementiert. Kehrt Zurück <code>XNotImplemented</code> .

Allgemeine Antwortkopfzeilen

Das StorageGRID System unterstützt alle gängigen Antwortheader, die durch die *Simple Storage Service API Reference* definiert wurden. Eine Ausnahme bilden die Antwort.

Kopfzeile der Antwort	Implementierung
X-amz-id-2	Nicht verwendet

Authentifizieren von Anfragen

Das StorageGRID-System unterstützt über die S3-API sowohl authentifizierten als auch anonymen Zugriff auf Objekte.

Die S3-API unterstützt Signature Version 2 und Signature Version 4 zur Authentifizierung von S3-API-Anforderungen.

Authentifizierte Anfragen müssen mit Ihrer Zugriffsschlüssel-ID und Ihrem geheimen Zugriffsschlüssel signiert werden.

Das StorageGRID System unterstützt zwei Authentifizierungsmethoden: Den HTTP `Authorization` Kopfzeile und Verwendung von Abfrageparametern.

Verwenden Sie den HTTP-Autorisierungskopf

Das HTTP `Authorization` Kopfzeile wird von allen S3-API-Operationen verwendet außer anonymen Anfragen, sofern dies durch die Bucket-Richtlinie zulässig ist. Der `Authorization` Header enthält alle erforderlichen Signierungsdaten, um eine Anforderung zu authentifizieren.

Abfrageparameter verwenden

Sie können Abfrageparameter verwenden, um Authentifizierungsinformationen zu einer URL hinzuzufügen. Dies wird als Vorsignierung der URL bezeichnet, mit der ein temporärer Zugriff auf bestimmte Ressourcen gewährt werden kann. Benutzer mit der vorgeschichteten URL müssen den geheimen Zugriffsschlüssel nicht kennen, um auf die Ressource zuzugreifen. So können Sie beschränkten Zugriff von Drittanbietern auf eine Ressource bereitstellen.

Betrieb auf dem Service

Das StorageGRID System unterstützt die folgenden Vorgänge beim Service.

Betrieb	Implementierung
GET Service (ListBuckets)	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. Änderungen vorbehalten.
GET Storage-Auslastung	Der Antrag ZUR GET Storage-Nutzung gibt Ihnen die Gesamtzahl des verwendeten Storage durch ein Konto und für jeden mit dem Account verknüpften Bucket an. Dies ist eine Operation auf dem Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter (?x-ntap-sg-usage) Hinzugefügt.
OPTIONEN /	Client-Applikationen können Probleme haben <code>OPTIONS</code> / Anfragen an den S3-Port auf einem Storage-Node ohne die Zugangsdaten für die S3-Authentifizierung, um zu ermitteln, ob der Storage-Node verfügbar ist. Sie können diese Anforderung zum Monitoring verwenden oder um zu ermöglichen, dass externe Load Balancer eingesetzt werden, wenn ein Storage-Node ausfällt.

Verwandte Informationen

["GET Storage-Auslastung"](#)

Operationen auf Buckets

Das StorageGRID System unterstützt für jedes S3-Mandantenkonto maximal 1,000 Buckets.

Einschränkungen für Bucket-Namen folgen den regionalen Einschränkungen des AWS US Standard. Sie sollten sie jedoch weiter auf DNS-Namenskonventionen beschränken, um Anforderungen im virtuellen Hosted-Stil von S3 zu unterstützen.

Weitere Informationen finden Sie im Folgenden:

- ["Amazon Web Services \(AWS\) Dokumentation: Bucket-Einschränkungen und -Einschränkungen"](#)
- ["Konfigurieren Sie die Domännennamen des S3-Endpunkts"](#)

Operationen „GET Bucket“ (Listenobjekte) und „GET Bucket-Versionen“ unterstützen die StorageGRID-Konsistenzkontrollen.

Sie können überprüfen, ob für einzelne Buckets Updates zur letzten Zugriffszeit aktiviert oder deaktiviert wurden.

In der folgenden Tabelle wird beschrieben, wie StorageGRID S3-REST-API-Bucket-Operationen implementiert. Um einen dieser Vorgänge durchzuführen, müssen die erforderlichen Anmeldedaten für den Zugriff für das Konto bereitgestellt werden.

Betrieb	Implementierung
Bucket LÖSCHEN	Durch diesen Vorgang wird der Bucket gelöscht.
Bucket-Cors LÖSCHEN	Durch diesen Vorgang wird die CORS-Konfiguration für den Bucket gelöscht.
Bucket-Verschlüsselung LÖSCHEN	Bei diesem Vorgang wird die Standardverschlüsselung aus dem Bucket gelöscht. Vorhandene verschlüsselte Objekte bleiben verschlüsselt, neue Objekte, die dem Bucket hinzugefügt wurden, werden jedoch nicht verschlüsselt.
Bucket-Lebenszyklus LÖSCHEN	Bei diesem Vorgang wird die Lebenszyklukonfiguration aus dem Bucket gelöscht. Siehe "S3-Lebenszykluskonfiguration erstellen" .
Bucket-Richtlinie LÖSCHEN	Bei diesem Vorgang wird die Richtlinie gelöscht, die dem Bucket zugeordnet ist.
Bucket-Replizierung LÖSCHEN	Bei diesem Vorgang wird die an den Bucket angeschlossene Replizierungskonfiguration gelöscht.
Bucket-Tagging LÖSCHEN	Dieser Vorgang verwendet das <code>tagging</code> unterressource, um alle Tags aus einem Bucket zu entfernen

Betrieb	Implementierung
GET Bucket (ListObjects) (ListObjectsV2)	<p>Dieser Vorgang 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 aufgenommen wurde <code>REDUCED_REDUNDANCY</code> Option für Storage-Klasse:</p> <ul style="list-style-type: none"> • <code>STANDARD</code>, Die angibt, dass das Objekt in einem Speicherpool gespeichert wird, der aus Storage-Nodes besteht. • <code>GLACIER</code>, Dies bedeutet, dass das Objekt in den vom Cloud-Speicherpool angegebenen externen Bucket verschoben wurde. <p>Wenn der Bucket eine große Anzahl von gelöschten Schlüsseln enthält, die dasselbe Präfix haben, kann die Antwort einige enthalten <code>CommonPrefixes</code> Die keine Schlüssel enthalten.</p>
Get Bucket-Objektversionen (ListObjectVersions)	<p>Mit LESEZUGRIFF auf einen Bucket erfolgt dieser Vorgang mit dem <code>versions</code> unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.</p>
Bucket-acl ABRUFEN	<p>Dieser Vorgang gibt eine positive Antwort und die ID, DisplayName und die Erlaubnis des Bucket-Besitzers zurück, was darauf hinweist, dass der Besitzer vollen Zugriff auf den Bucket hat.</p>
Bucket-Cors ABRUFEN	<p>Dieser Vorgang gibt den zurück <code>cors</code> Konfiguration für den Bucket.</p>
Get Bucket-Verschlüsselung	<p>Dieser Vorgang gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.</p>
BUCKET-Lebenszyklus ABRUFEN (GetBucketLifecycleConfiguration)	<p>Dieser Vorgang gibt die Lifecycle-Konfiguration für den Bucket zurück. Siehe "S3-Lebenszykluskonfiguration erstellen".</p>
Bucket-Speicherort ABRUFEN	<p>Dieser Vorgang gibt die Region zurück, die mit dem festgelegt wurde <code>LocationConstraint</code> Element in DER PUT Bucket Anforderung. Wenn der Eimer-Bereich ist <code>us-east-1</code>, Eine leere Zeichenfolge wird für die Region zurückgegeben.</p>
Bucket-Benachrichtigung ABRUFEN (GetBucketNotificationConfiguration)	<p>Dieser Vorgang gibt die Benachrichtigungskonfiguration an den Bucket zurück.</p>
Get Bucket-Richtlinie	<p>Dieser Vorgang gibt die Richtlinie zurück, die dem Bucket zugeordnet ist.</p>

Betrieb	Implementierung
GET Bucket-Replizierung	Dieser Vorgang gibt die am Bucket angeschlossene Replizierungskonfiguration zurück.
Get Bucket-Tagging	Dieser Vorgang verwendet das <code>tagging</code> unterressource, um alle Tags für einen Bucket zurückzugeben
Get Bucket-Versionierung	<p>Diese Implementierung verwendet das <code>versioning</code> subressource zur Rückgabe des Versionierungsstatus eines Buckets.</p> <ul style="list-style-type: none"> • <i>Blank</i>: Versionierung wurde noch nie aktiviert (Bucket ist „Unversioniert“) • <i>Aktiviert</i>: Versionierung ist aktiviert • <i>Suspendiert</i>: Die Versionierung war zuvor aktiviert und wird ausgesetzt
Konfiguration der Objektsperre ABRUFEN	<p>Dieser Vorgang liefert den Bucket-Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum, sofern konfiguriert.</p> <p>Siehe "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".</p>
EIMER	<p>Dieser Vorgang bestimmt, ob ein Bucket vorhanden ist und Sie über die Berechtigung zum Zugriff auf ihn verfügen.</p> <p>Dieser Vorgang liefert Folgendes zurück:</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: Die UUID des Buckets im UUID-Format. • <code>x-ntap-sg-trace-id</code>: Die eindeutige Trace-ID der zugehörigen Anfrage.

Betrieb	Implementierung
Put Bucket	<p>Durch diesen Vorgang wird ein neuer Bucket erstellt. Mit dem Erstellen des Buckets werden Sie zum Bucket-Eigentümer.</p> <ul style="list-style-type: none"> • Bucket-Namen müssen die folgenden Regeln einhalten: <ul style="list-style-type: none"> ◦ Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). ◦ Muss DNS-konform sein. ◦ Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten. ◦ Kann eine Reihe von einer oder mehreren Etiketten sein, wobei angrenzende Etiketten durch einen Zeitraum getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden. ◦ Darf nicht wie eine Text-formatierte IP-Adresse aussehen. ◦ Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. • Standardmäßig werden Buckets im erstellten <code>us-east-1</code> Region; jedoch können Sie die verwenden <code>LocationConstraint</code> Anforderungselement im Anforderungskörper, um eine andere Region anzugeben. Bei Verwendung des <code>LocationConstraint</code> Element, Sie müssen 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 Regionalnamen nicht kennen. <p>Hinweis: Ein Fehler tritt auf, wenn Ihre PUT Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.</p> <ul style="list-style-type: none"> • Sie können die einschließen <code>x-amz-bucket-object-lock-enabled</code> Kopfzeile zum Erstellen eines Buckets anfordern, wobei S3-Objektsperre aktiviert ist. Siehe "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API". <p>Sie müssen die S3-Objektsperre aktivieren, wenn Sie den Bucket erstellen. Sie können S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde. Für die S3-Objektsperre ist eine Bucket-Versionierung erforderlich. Diese wird bei der Erstellung des Buckets automatisch aktiviert.</p>
Bucket-Cors EINGEBEN	<p>Mit diesem Vorgang wird die CORS-Konfiguration für einen Bucket festgelegt, damit der Bucket die Cross-Origin-Requests bedienen kann. CORS (Cross-Origin Resource Sharing) ist ein Sicherheitsmechanismus, mit dem Client-Webanwendungen in einer Domäne auf Ressourcen in einer anderen Domäne zugreifen können. Angenommen, Sie verwenden einen S3-Bucket mit dem Namen <code>images</code> Zum Speichern von Grafiken. Durch Festlegen der CORS-Konfiguration für das <code>images</code> Bucket: Sie können zulassen, dass die Bilder in diesem Bucket auf der Website angezeigt werden <code>http://www.example.com</code>.</p>

Betrieb	Implementierung
Bucket-Verschlüsselung	<p>Dieser Vorgang legt den Standardverschlüsselungsstatus eines vorhandenen Buckets fest. Bei aktivierter Verschlüsselung auf Bucket-Ebene sind alle neuen dem Bucket hinzugefügten Objekte verschlüsselt. StorageGRID unterstützt serverseitige Verschlüsselung mit von StorageGRID gemanagten Schlüsseln. Wenn Sie die Konfigurationsregel für die serverseitige Verschlüsselung angeben, legen Sie die fest SSEAlgorithm Parameter an AES256`Und verwenden Sie nicht die `KMSMasterKeyID Parameter.</p> <p>Die Standardverschlüsselungskonfiguration von Buckets wird ignoriert, wenn in der Anfrage für das Hochladen von Objekten bereits eine Verschlüsselung angegeben ist (d. h., wenn die Anforderung den umfasst <code>x-amz-server-side-encryption-*</code> Kopfzeile der Anfrage).</p>
PUT Bucket-Lebenszyklus (PutBucketLifecycleConfiguration)	<p>Dieser Vorgang erstellt eine neue Lifecycle-Konfiguration für den Bucket oder ersetzt eine vorhandene Lifecycle-Konfiguration. StorageGRID unterstützt in einer Lebenszykluskonfiguration bis zu 1,000 Lebenszyklusregeln. Jede Regel kann die folgenden XML-Elemente enthalten:</p> <ul style="list-style-type: none"> • Ablauf (Tage, Datum) • NoncurrentVersionExpiration (NoncurrentDays) • Filter (Präfix, Tag) • Status • ID <p>StorageGRID bietet folgende Maßnahmen nicht:</p> <ul style="list-style-type: none"> • AbortInsetteMultipartUpload • ExpiredObjectDeleteMarker • Übergang <p>Siehe "S3-Lebenszykluskonfiguration erstellen". Informationen über die Interaktion der Aktion „Ablauf“ in einem Bucket-Lebenszyklus mit den Anweisungen zur ILM-Platzierung finden Sie unter "Wie ILM im gesamten Leben eines Objekts funktioniert".</p> <p>Hinweis: Die Konfiguration des Bucket-Lebenszyklus kann für Buckets verwendet werden, für die S3-Objektsperrung aktiviert ist. Die Bucket-Lebenszykluskonfiguration wird jedoch für ältere kompatible Buckets nicht unterstützt.</p>

Betrieb	Implementierung
PUT Bucket-Benachrichtigung (PutkBucketNotificationConfiguration)	<p>Mit diesem Vorgang werden Benachrichtigungen für den Bucket mithilfe der im Anfraentext enthaltenen XML-Benachrichtigungskonfiguration konfiguriert. Sie sollten folgende Implementierungsdetails kennen:</p> <ul style="list-style-type: none"> • StorageGRID unterstützt SNS-Themen (Simple Notification Service) als Ziele. SQS (Simple Queue Service)- oder Amazon Lambda-Endpunkte werden nicht unterstützt. • Das Ziel für Benachrichtigungen muss als URN eines StorageGRID-Endpunkts angegeben werden. Endpunkte können mit dem Mandanten-Manager oder der Mandanten-Management-API erstellt werden. <p>Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, A 400 Bad Request Der Code gibt einen Fehler zurück InvalidArgument.</p> <ul style="list-style-type: none"> • Sie können keine Benachrichtigung für die folgenden Ereignistypen konfigurieren. Diese Ereignistypen werden nicht unterstützt. <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed • Aus StorageGRID gesendete Ereignisbenachrichtigungen verwenden das JSON-Standardformat, außer dass sie einige Schlüssel nicht enthalten und bestimmte Werte für andere verwenden, wie in der folgenden Liste gezeigt: <ul style="list-style-type: none"> ◦ EventSource sgws:s3 ◦ AwsRegion Nicht enthalten ◦ * X-amz-id-2* Nicht enthalten ◦ arn urn:sgws:s3:::bucket_name
Bucket-Richtlinie	Dieser Vorgang legt die Richtlinie fest, die an den Bucket gebunden ist.

Betrieb	Implementierung
PUT Bucket-Replizierung	<p>Dieser Vorgang wird konfiguriert "StorageGRID CloudMirror Replizierung" Für den Bucket unter Verwendung der XML-Replikationskonfiguration, die im Anforderungskörper bereitgestellt wurde. Für die CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten:</p> <ul style="list-style-type: none"> • StorageGRID unterstützt nur V1 der Replizierungskonfiguration. Das bedeutet, dass StorageGRID die Verwendung von nicht unterstütz <code>Filter</code> Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Weitere Informationen finden Sie im "Amazon S3-Dokumentation zur Replizierungskonfiguration". • Die Bucket-Replizierung 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 auf mehrere Ziel-Bucket replizieren. • Ziel-Buckets müssen als URN der StorageGRID-Endpunkte angegeben werden, wie im Mandantenmanager oder der Mandantenmanagement-API angegeben. Siehe "CloudMirror-Replizierung konfigurieren". <p>Der Endpunkt muss vorhanden sein, damit die Replizierungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, schlägt die Anforderung als <code>400 Bad Request</code>. In der Fehlermeldung steht: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN</code>.</p> <ul style="list-style-type: none"> • Sie müssen keinen angeben <code>Role</code> In der Konfigurations-XML. Dieser Wert wird von StorageGRID nicht verwendet und wird bei der Einreichung ignoriert. • Wenn Sie die Storage-Klasse aus der XML-Konfiguration weglassen, verwendet StorageGRID das <code>STANDARD</code> Standardmäßig Storage-Klasse. • Wenn Sie ein Objekt aus dem Quell-Bucket löschen oder den Quell-Bucket selbst löschen, sieht das Verhalten der regionsübergreifenden Replizierung wie folgt aus: <ul style="list-style-type: none"> ◦ Wenn Sie das Objekt oder den Bucket löschen, bevor es repliziert wurde, wird das Objekt/Bucket nicht repliziert, und Sie werden nicht benachrichtigt. ◦ Wenn Sie das Objekt oder Bucket nach der Replizierung löschen, befolgt StorageGRID das standardmäßige Löschverhalten von Amazon S3 für die V1 der regionsübergreifenden Replizierung.

Betrieb	Implementierung
PUT Bucket-Tagging	<p>Dieser Vorgang verwendet das <code>tagging</code> unterressource, um einen Satz von Tags für einen Bucket hinzuzufügen oder zu aktualisieren. Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen:</p> <ul style="list-style-type: none"> • StorageGRID und Amazon S3 unterstützen für jeden Bucket bis zu 50 Tags. • Tags, die einem Bucket zugeordnet sind, müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein. • Die Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. • Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.
PUT Bucket-Versionierung	<p>Diese Implementierung verwendet das <code>versioning</code> unterressource, um den Versionierungsstatus eines vorhandenen Buckets festzulegen. Sie können den Versionierungsstatus mit einem der folgenden Werte festlegen:</p> <ul style="list-style-type: none"> • Aktiviert: Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Version-ID. • Suspendiert: Deaktiviert die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten die Version-ID <code>null</code>.
PUT Objekt Lock-Konfiguration	<p>Dieser Vorgang konfiguriert oder entfernt den Bucket-Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum.</p> <p>Wenn der Standardaufbewahrungszeitraum geändert wird, bleiben die bisherigen Objektversionen unverändert und werden im neuen Standardaufbewahrungszeitraum nicht neu berechnet.</p> <p>Siehe "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API" Ausführliche Informationen finden Sie unter.</p>

Verwandte Informationen

["Konsistenzkontrollen"](#)

["ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN"](#)

["Verwendung von Bucket- und Gruppenzugriffsrichtlinien"](#)

["S3-Vorgänge werden in Prüfprotokollen nachverfolgt"](#)

Benutzerdefinierte Vorgänge für Buckets

Das StorageGRID System unterstützt benutzerdefinierte Bucket-Vorgänge, die der S3-REST-API hinzugefügt wurden und sich speziell auf das System beziehen.

In der folgenden Tabelle sind die von StorageGRID unterstützten benutzerdefinierten Bucket-Vorgänge aufgeführt.

Betrieb	Beschreibung	Finden Sie weitere Informationen
Get Bucket-Konsistenz	Gibt die auf einen bestimmten Bucket angewendete Konsistenzstufe zurück.	"Get Bucket-Konsistenz"
PUT Bucket-Konsistenz	Legt die Konsistenzstufe für einen bestimmten Bucket fest.	"PUT Bucket-Konsistenz"
ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN	Gibt an, ob Updates der letzten Zugriffszeit für einen bestimmten Bucket aktiviert oder deaktiviert wurden.	"ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN"
PUT Bucket-Zeit für den letzten Zugriff	Hiermit können Sie Updates der letzten Zugriffszeit für einen bestimmten Bucket aktivieren oder deaktivieren.	"PUT Bucket-Zeit für den letzten Zugriff"
Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN	Löscht die XML-Konfiguration für die Metadatenbenachrichtigung, die mit einem bestimmten Bucket verknüpft ist.	"Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN"
Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN	Gibt die XML-XML-Benachrichtigungskonfiguration für Metadaten zurück, die einem bestimmten Bucket zugeordnet ist.	"Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN"
PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Konfiguriert den Metadaten-Benachrichtigungsdienst für einen Bucket	"PUT Bucket-Metadaten-Benachrichtigungskonfiguration"
Bucket mit Compliance-Einstellungen	Veraltet und nicht unterstützt: Sie können keine neuen Buckets mit aktivierter Compliance mehr erstellen.	"Veraltet: Put Bucket mit Compliance-Einstellungen"
Bucket-Compliance	Veraltet, aber unterstützt: Gibt die Compliance-Einstellungen zurück, die derzeit für einen vorhandenen Legacy-konformen Bucket wirksam sind.	"Veraltet: EINHALTUNG von Bucket ABRUFEN"
BUCKET-Compliance	Veraltet, aber unterstützt: Ermöglicht es Ihnen, die Compliance-Einstellungen für einen vorhandenen, älteren konformen Bucket zu ändern.	"Veraltet: EINHALTUNG VON PUT Bucket"

Verwandte Informationen

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

Operationen für Objekte

In diesem Abschnitt wird beschrieben, wie das StorageGRID System S3-REST-API-Vorgänge für Objekte implementiert.

Die folgenden Bedingungen gelten für alle Objektvorgänge:

- StorageGRID "**Konsistenzkontrollen**" Werden von allen Operationen auf Objekten unterstützt, mit Ausnahme der folgenden:
 - GET Objekt-ACL
 - OPTIONS /
 - LEGALE Aufbewahrung des Objekts EINGEBEN
 - AUFBEWAHRUNG von Objekten
 - Wählen Sie Objektinhalt
- Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Auswertung „latest-WINS“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.
- Alle Objekte in einem StorageGRID-Bucket sind im Eigentum des Bucket-Inhabers. Dies umfasst Objekte, die von einem anonymen Benutzer oder einem anderen Konto erstellt wurden.
- Der Zugriff auf Datenobjekte, die über Swift in das StorageGRID System aufgenommen wurden, ist nicht über S3 möglich.

In der folgenden Tabelle wird beschrieben, wie StorageGRID S3-REST-API-Objektvorgänge implementiert.

Betrieb	Implementierung
Objekt LÖSCHEN	<p>Multi-Faktor Authentication (MFA) und Response Header <code>x-amz-mfa</code> Werden nicht unterstützt.</p> <p>Bei der Verarbeitung einer LÖSCHOBJEKTANFORDERUNG versucht StorageGRID, alle Kopien des Objekts sofort von allen gespeicherten Speicherorten zu entfernen. Wenn erfolgreich, gibt StorageGRID sofort eine Antwort an den Client zurück. Wenn nicht innerhalb von 30 Sekunden alle Kopien entfernt werden können (z. B. weil ein Speicherort vorübergehend nicht verfügbar ist), stellt StorageGRID die Kopien in eine Warteschlange zur Entfernung und zeigt dann den Erfolg des Clients an.</p> <p>Versionierung</p> <p>Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und den verwenden <code>versionId</code> unterressource. Durch die Verwendung dieser Unterressource wird die Version dauerhaft gelöscht. Wenn der <code>versionId</code> Entspricht einer Löschen-Markierung, dem Antwortkopf <code>x-amz-delete-marker</code> Wird auf festgelegt <code>true</code>.</p> <ul style="list-style-type: none"> • Wird ein Objekt ohne gelöscht <code>versionId</code> unterressource auf einem Bucket mit Versionsfunktion führt zur Generierung einer Löschemarkierung. Der <code>versionId</code> Für die Löschen-Markierung wird mit dem zurückgegeben <code>x-amz-version-id</code> Kopfzeile der Antwort und das <code>x-amz-delete-marker</code> Der Antwortkopf wird auf festgelegt <code>true</code>. • Wird ein Objekt ohne gelöscht <code>versionId</code> unterressource in einem Version suspended Bucket führt es zu einer dauerhaften Löschung einer bereits vorhandenen 'null' Version oder eines 'null' Löschemarker und der Generierung eines neuen 'null' Löschemarker. Der <code>x-amz-delete-marker</code> Der Antwortkopf wird auf festgelegt <code>true</code>. <p>Hinweis: In bestimmten Fällen können für ein Objekt mehrere Löschen-Marker vorhanden sein.</p> <p>Siehe "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API" Anleitung zum Löschen von Objektversionen im GOVERNANCE-Modus.</p>
LÖSCHEN Sie mehrere Objekte (DeleteObjects)	<p>Multi-Faktor Authentication (MFA) und Response Header <code>x-amz-mfa</code> Werden nicht unterstützt.</p> <p>In derselben Anforderungsmeldung können mehrere Objekte gelöscht werden.</p> <p>Siehe "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API" Anleitung zum Löschen von Objektversionen im GOVERNANCE-Modus.</p>

Betrieb	Implementierung
Objekt-Tagging LÖSCHEN	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags aus einem Objekt zu entfernen.</p> <p>Versionierung</p> <p>Wenn der <code>versionId</code> Der Abfrageparameter wird in der Anforderung nicht angegeben. Der Vorgang löscht alle Tags von der neuesten Version des Objekts in einem versionierten Bucket. Wenn die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „MethodNotAllowed“ zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
GET Objekt	"GET Objekt"
GET Objekt-ACL	Wenn für das Konto die erforderlichen Zugangsdaten bereitgestellt werden, gibt der Vorgang eine positive Antwort und die ID, DisplayName und die Berechtigung des Objekteigentümers zurück und gibt an, dass der Eigentümer vollen Zugriff auf das Objekt hat.
HOLD-Aufbewahrung für Objekte	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
Aufbewahrung von Objekten	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
GET Objekt-Tagging	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags für ein Objekt zurückzugeben.</p> <p>Versionierung</p> <p>Wenn der <code>versionId</code> Der Abfrageparameter wird in der Anforderung nicht angegeben. Der Vorgang gibt alle Tags der neuesten Version des Objekts in einem versionierten Bucket zurück. Wenn die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „MethodNotAllowed“ zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
HEAD Objekt	"HEAD Objekt"
WIEDERHERSTELLUNG VON POSTOBJEKTEN	"WIEDERHERSTELLUNG VON POSTOBJEKTEN"
PUT Objekt	"PUT Objekt"
PUT Objekt - Kopieren	"PUT Objekt - Kopieren"
LEGALE Aufbewahrung des Objekts EINGEBEN	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
AUFBEWAHRUNG von Objekten	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"

Betrieb	Implementierung
PUT Objekt-Tagging	<p>Verwendet das <code>tagging</code> unterressource, um einem vorhandenen Objekt einen Satz von Tags hinzuzufügen.</p> <p>Grenzwerte für Objekt-Tags</p> <p>Sie können neue Objekte mit Tags hinzufügen, wenn Sie sie hochladen, oder Sie können sie zu vorhandenen Objekten hinzufügen. StorageGRID und Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Tags, die einem Objekt zugeordnet sind, müssen über eindeutige Tag-Schlüssel verfügen. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein, und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.</p> <p>Tag-Updates und Ingest-Verhalten</p> <p>Wenn Sie PUT Objekt-Tagging zum Aktualisieren der Tags eines Objekts verwenden, nimmt StorageGRID das Objekt nicht erneut auf. Das bedeutet, dass die in der übereinstimmenden ILM-Regel angegebene Option für das Aufnahmeverhalten nicht verwendet wird. Sämtliche durch das Update ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird.</p> <p>Das heißt, wenn die ILM-Regel die strikte Option für das Aufnahmeverhalten verwendet, werden keine Maßnahmen ergriffen, wenn 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.</p> <p>Konflikte lösen</p> <p>Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „latest-WINS“-Basis gelöst. Der Zeitpunkt für die Auswertung „latest-WINS“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.</p> <p>Versionierung</p> <p>Wenn der <code>versionId</code> Der Abfrageparameter wird in der Anforderung nicht angegeben, und der Vorgang fügt Tags zur aktuellen Version des Objekts in einem versionierten Bucket hinzu. Wenn die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „MethodNotAllowed“ zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
SelektierObjectContent	"SelektierObjectContent"

Verwandte Informationen

["S3-Vorgänge werden in Prüfprotokollen nachverfolgt"](#)

Verwenden Sie S3 Select

StorageGRID unterstützt die folgenden Amazon S3 Select-Klauseln, Datentypen und Operatoren für die ["SelectObjectContent, Befehl"](#).



Nicht aufgeführte Elemente werden nicht unterstützt.

Syntax finden Sie unter ["SelektierObjectContent"](#). Weitere Informationen zu S3 Select finden Sie im ["AWS-Dokumentation für S3 Select"](#).

Nur Mandantenkonten, für die S3 Select aktiviert ist, können SelectObjectContent-Abfragen ausgeben. Siehe ["Überlegungen und Anforderungen bei der Verwendung von S3 Select"](#).

Klauseln

- Wählen Sie die Liste aus
- FROM-Klausel
- WHERE-Klausel
- BEGRENZUNGSKLAUSEL

Datentypen

- bool
- Ganzzahl
- Zeichenfolge
- Schweben
- Dezimal, numerisch
- Zeitstempel

Operatoren

Logische Operatoren

- UND
- NICHT
- ODER

Vergleichsoperatoren

- <
- >
- ≪=
- >=
- =
- =
- <>

- !=
- ZWISCHEN
- IN

Operatoren für die Musteranpassung

- GEFÄLLT MIR
- _
- %

Einheitliche Operatoren

- IST NULL
- IST NICHT NULL

Mathematische Operatoren

- +
- -
- *
- /
- %

StorageGRID folgt der Priorität des Amazon S3 Select-Operators.

Aggregatfunktionen

- DURCHSCHN.()
- ANZAHL (*)
- MAX.()
- MIN.()
- SUMME()

Bedingte Funktionen

- FALL
- ZUSAMMENSCHMELZEN
- NULL LIF

Konvertierungsfunktionen

- CAST (für unterstützten Datentyp)

Datumsfunktionen

- DATUM_HINZUFÜGEN
- DATE_DIFF

- EXTRAHIEREN
- TO_STRING
- TO_ZEITSTEMPEL
- UTCNOW

Zeichenfolgenfunktionen

- CHAR_LENGTH, CHARACTER_LENGTH
- NIEDRIGER
- TEILSTRING
- TRIMMEN
- OBEN

Serverseitige Verschlüsselung

Die serverseitige Verschlüsselung schützt Ihre Objektdaten im Ruhezustand. StorageGRID verschlüsselt die Daten beim Schreiben des Objekts und entschlüsselt sie beim Zugriff auf das Objekt.

Wenn Sie die serverseitige Verschlüsselung verwenden möchten, können Sie eine der zwei Optionen auswählen, die sich gegenseitig ausschließen, je nachdem, wie die Verschlüsselungsschlüssel verwaltet werden:

- **SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln):** Bei der Ausgabe einer S3-Anfrage zum Speichern eines Objekts verschlüsselt StorageGRID das Objekt mit einem eindeutigen Schlüssel. Wenn Sie zum Abrufen des Objekts eine S3-Anforderung ausstellen, entschlüsselt StorageGRID das Objekt mithilfe des gespeicherten Schlüssels.
- **SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln):** Wenn Sie eine S3-Anfrage zum Speichern eines Objekts ausgeben, geben Sie Ihren eigenen Verschlüsselungsschlüssel an. Wenn Sie ein Objekt abrufen, geben Sie denselben Verschlüsselungsschlüssel wie in Ihrer Anfrage ein. Stimmen die beiden Verschlüsselungsschlüssel überein, wird das Objekt entschlüsselt und die Objektdaten zurückgegeben.

StorageGRID managt zwar alle Objektverschlüsselung und Entschlüsselungsvorgänge, muss aber die von Ihnen zur Verfügung gelegten Verschlüsselungsschlüssel verwalten.



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.



Wenn ein Objekt mit SSE oder SSE-C verschlüsselt wird, werden sämtliche Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

Verwenden Sie SSE

Um ein Objekt mit einem eindeutigen, von StorageGRID gemanagten Schlüssel zu verschlüsseln, verwenden Sie die folgende Anforderungsüberschrift:

`x-amz-server-side-encryption`

Der SSE-Anforderungsheader wird durch die folgenden Objektoperationen unterstützt:

- "PUT Objekt"
- "PUT Objekt - Kopieren"
- "Initiieren Von Mehrteiligen Uploads"

Verwenden Sie SSE-C

Um ein Objekt mit einem eindeutigen Schlüssel zu verschlüsseln, den Sie verwalten, verwenden Sie drei Anforderungsheader:

Kopfzeile der Anfrage	Beschreibung
x-amz-server-side-encryption-customer-algorithm	Geben Sie den Verschlüsselungsalgorithmus an. Der Kopfzeilenwert muss sein 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, base64-codiert sein.
x-amz-server-side-encryption-customer-key-MD5	Geben Sie den MD5-Digest des Verschlüsselungsschlüssels gemäß RFC 1321 an, der dafür sorgt, dass der Verschlüsselungsschlüssel fehlerfrei übertragen wurde. Der Wert für das MD5 Digest muss base64-codiert 128-Bit sein.

Die SSE-C-Anfrageheader werden durch die folgenden Objektoperationen unterstützt:

- "GET Objekt"
- "HEAD Objekt"
- "PUT Objekt"
- "PUT Objekt - Kopieren"
- "Initiieren Von Mehrteiligen Uploads"
- "Hochladen Von Teilen"
- "Hochladen Von Teilen - Kopieren"

Überlegungen zur Verwendung serverseitiger Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)

Beachten Sie vor der Verwendung von SSE-C die folgenden Punkte:

- Sie müssen https verwenden.



StorageGRID lehnt alle über http gestellten Anfragen bei der Verwendung von SSE-C. ab Aus Sicherheitsgründen sollten Sie jeden Schlüssel, den Sie versehentlich über http senden, in Betracht ziehen, um kompromittiert zu werden. Entsorgen Sie den Schlüssel, und drehen Sie ihn nach Bedarf.

- Der ETag in der Antwort ist nicht das MD5 der Objektdaten.
- Sie müssen die Zuordnung von Schlüsseln zu Objekten managen. StorageGRID speichert keine Schlüssel. Sie sind für die Nachverfolgung des Verschlüsselungsschlüssels verantwortlich, den Sie für jedes Objekt bereitstellen.
- Wenn Ihr Bucket mit Versionierung aktiviert ist, sollte für jede Objektversion ein eigener Verschlüsselungsschlüssel vorhanden sein. Sie sind verantwortlich für das Tracking des Verschlüsselungsschlüssels, der für jede Objektversion verwendet wird.
- Da Sie Verschlüsselungsschlüssel auf Client-Seite verwalten, müssen Sie auch zusätzliche Schutzmaßnahmen, wie etwa die Rotation von Schlüsseln, auf Client-Seite verwalten.



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.

- Wenn die Grid-übergreifende Replizierung oder CloudMirror Replizierung für den Bucket konfiguriert ist, können SSE-C-Objekte nicht aufgenommen werden. Der Aufnahmeprozess schlägt fehl.

Verwandte Informationen

["Amazon S3 Entwicklerleitfaden: Schutz von Daten durch serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln \(SSE-C\)"](#)

GET Objekt

Sie können die S3-GET-Objektanfrage verwenden, um ein Objekt aus einem S3-Bucket abzurufen.

ABRUFEN von Objekten und Objekten mit mehreren Teilen

Sie können das verwenden `partNumber` Parameter anfordern, um einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts abzurufen. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, wie viele Teile das Objekt hat.

Sie können festlegen `partNumber` Zu 1 für segmentierte/mehrteilige Objekte und nicht segmentierte/nicht-mehrteilige Objekte; jedoch der `x-amz-mp-parts-count` Antwortelement wird nur für segmentierte oder mehrteilige Objekte zurückgegeben.

UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. GET Requests for an object with escaped UTF-8 characters in user-defined metadata don't return the `x-amz-missing-meta` Kopfzeile, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

Nicht unterstützte Anforderungsüberschrift

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`:

- `x-amz-website-redirect-location`

Versionierung

Wenn `versionId` unterressource wird nicht angegeben. Der Vorgang ruft die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist,

wird mit dem ein Status „not found“ zurückgegeben x-amz-delete-marker Antwortkopfzeile auf gesetzt true.

Kopfzeilen zur serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln anfordern (SSE-C)

Verwenden Sie alle drei Kopfzeilen, wenn das Objekt mit einem eindeutigen Schlüssel verschlüsselt ist, den Sie angegeben haben.

- x-amz-server-side-encryption-customer-algorithm: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen in prüfen "[Serverseitige Verschlüsselung](#)".

Verhalten DES GET Object für Cloud-Storage-Pool-Objekte

Wenn ein Objekt in einem gespeichert wurde "[Cloud-Storage-Pool](#)", Das Verhalten einer GET Object Anfrage hängt vom Zustand des Objekts ab. Siehe "[HEAD Objekt](#)" Entnehmen.



Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, werden GET-Objektanfragen versuchen, Daten aus dem Grid abzurufen, bevor sie aus dem Cloud-Storage-Pool abgerufen werden.

Status des Objekts	Verhalten VON GET Object
Objekt, das in StorageGRID aufgenommen wurde, durch ILM jedoch noch nicht evaluiert wurde, oder Objekt, das in einem herkömmlichen Storage-Pool gespeichert ist oder Erasure Coding verwendet	200 OK Eine Kopie des Objekts wird abgerufen.
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	200 OK Eine Kopie des Objekts wird abgerufen.
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	403 Forbidden, InvalidObjectState Verwenden Sie A " WIEDERHERSTELLUNG VON POSTOBJEKTEN " Anforderung zur Wiederherstellung des Objektstatus in einem abrufbaren Zustand.

Status des Objekts	Verhalten VON GET Object
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	403 Forbidden, InvalidObjectState Warten Sie, bis die Anforderung zur Wiederherstellung DES POSTOBJEKTS abgeschlossen ist.
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	200 OK Eine Kopie des Objekts wird abgerufen.

Mehrteilige oder segmentierte Objekte in einem Cloud Storage-Pool

Wenn Sie ein mehrteilige Objekt hochgeladen StorageGRID oder ein großes Objekt in Segmente aufgeteilt haben, bestimmt StorageGRID, ob das Objekt im Cloud-Storage-Pool verfügbar ist, indem Sie eine Teilmenge der Teile oder Segmente des Objekts testen. In manchen Fällen wird eine GET Object-Anforderung möglicherweise falsch zurückgegeben 200 OK Wenn bereits Teile des Objekts in einen nicht aufrufbaren Zustand überführt wurden oder Teile des Objekts noch nicht wiederhergestellt wurden.

In diesen Fällen:

- Die GET Object-Anforderung gibt möglicherweise einige Daten zurück, stoppt jedoch mitten durch die Übertragung.
- Eine nachfolgende GET Object-Anforderung kann zurückgegeben werden 403 Forbidden.

Objekt- und Grid-Replizierung

Wenn Sie verwenden "Grid-Verbund" Und "Grid-übergreifende Replizierung" Ist für einen Bucket aktiviert, kann der S3-Client den Replizierungsstatus eines Objekts durch Ausgabe einer GET Object-Anforderung überprüfen. Die Antwort bezieht sich auf das StorageGRID-spezifische `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	<ul style="list-style-type: none"> • SUCCESS: Die Replikation war erfolgreich. • AUSSTEHEND: Das Objekt wurde noch nicht repliziert. • FAILURE: Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.
Ziel	REPLIKAT: Das Objekt wurde aus dem Quellraster repliziert.



StorageGRID unterstützt das nicht `x-amz-replication-status` Kopfzeile.

Verwandte Informationen

["S3-Vorgänge werden in Prüfprotokollen nachverfolgt"](#)

HEAD Objekt

Mithilfe der S3 HEAD Object-Anfrage können Metadaten von einem Objekt abgerufen werden, ohne das Objekt selbst zurückzugeben. Wenn das Objekt in einem Cloud Storage Pool gespeichert ist, können Sie MITHILFE VON HEAD Object den Übergangstatus des Objekts bestimmen.

HEAD Objekt und mehrteilige Objekte

Sie können das verwenden `partNumber` Parameter anfordern, um Metadaten für einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts abzurufen. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, wie viele Teile das Objekt hat.

Sie können festlegen `partNumber` Zu 1 für segmentierte/mehrteilige Objekte und nicht segmentierte/nicht-mehrteilige Objekte; jedoch der `x-amz-mp-parts-count` Antwortelement wird nur für segmentierte oder mehrteilige Objekte zurückgegeben.

UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. HEAD-Anforderungen für ein Objekt mit ausbleibenden UTF-8-Zeichen in benutzerdefinierten Metadaten geben den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

Nicht unterstützte Anforderungsüberschrift

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`:

- `x-amz-website-redirect-location`

Versionierung

Wenn `versionId` unterressource wird nicht angegeben. Der Vorgang ruft die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird mit dem ein Status „not found“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

Kopfzeilen zur serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln anfordern (SSE-C)

Verwenden Sie alle drei dieser Kopfzeilen, wenn das Objekt mit einem eindeutigen Schlüssel verschlüsselt ist, den Sie angegeben haben.

- `x-amz-server-side-encryption-customer-algorithm`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen in prüfen "[Serverseitige Verschlüsselung](#)".

HEAD Objektantworten für Cloud Storage Pool Objekte

Wenn das Objekt in einem gespeichert ist "[Cloud-Storage-Pool](#)", Die folgenden Antwortheader werden zurückgegeben:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Die Antwortheader liefern Informationen zum Status eines Objekts beim Verschieben in einen Cloud Storage Pool, beim Wechsel in einen nicht abrufbaren Zustand und wieder verfügbar.

Status des Objekts	Reaktion auf HEAD Objekt
Objekt, das in StorageGRID aufgenommen wurde, durch ILM jedoch noch nicht evaluiert wurde, oder Objekt, das in einem herkömmlichen Storage-Pool gespeichert ist oder Erasure Coding verwendet	200 OK (Es wird keine spezielle Antwortheader zurückgegeben.)
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Bis das Objekt in einen nicht aufrufbaren Zustand überführt wird, wird der Wert für <code>expiry-date</code> Wird in der Zukunft auf eine ferne Zeit gesetzt. Die genaue Zeit der Transition wird nicht durch das StorageGRID System gesteuert.

Status des Objekts	Reaktion auf HEAD Objekt
Das Objekt ist in den nicht aufrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Grid vorhanden	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Der Wert für <code>expiry-date</code> Wird in der Zukunft auf eine ferne Zeit gesetzt.</p> <p>Hinweis: Wenn die Kopie auf dem Raster nicht verfügbar ist (z. B. ist ein Storage Node ausgefallen), müssen Sie einen ausstellen "WIEDERHERSTELLUNG VON POSTOBJEKTEN" Anforderung zur Wiederherstellung der Kopie aus dem Cloud-Storage-Pool, bevor Sie das Objekt erfolgreich abrufen können.</p>
Das Objekt wurde in einen nicht abrufbaren Zustand versetzt, und es ist keine Kopie im Grid vorhanden	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"</p> <p>Der <code>expiry-date</code> Gibt an, wann das Objekt im Cloud Storage Pool wieder in einen Zustand zurückversetzt werden soll, der nicht abrufbar ist.</p>

Mehrteilige oder segmentierte Objekte in Cloud Storage Pool

Wenn Sie ein mehrteilige Objekt hochgeladen StorageGRID oder ein großes Objekt in Segmente aufgeteilt haben, bestimmt StorageGRID, ob das Objekt im Cloud-Storage-Pool verfügbar ist, indem Sie eine Teilmenge der Teile oder Segmente des Objekts testen. In einigen Fällen wird möglicherweise eine HEAD Object-Anfrage falsch zurückgegeben `x-amz-restore: ongoing-request="false"` Wenn bereits Teile des Objekts in einen nicht aufrufbaren Zustand überführt wurden oder Teile des Objekts noch nicht wiederhergestellt wurden.

HEAD Object- und Grid-übergreifende Replizierung

Wenn Sie verwenden "Grid-Verbund" Und "Grid-übergreifende Replizierung" Ist für einen Bucket aktiviert, kann der S3-Client den Replizierungsstatus eines Objekts durch Ausgabe einer HEAD Object-Anforderung überprüfen. Die Antwort bezieht sich auf das StorageGRID-spezifische `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	<ul style="list-style-type: none">• SUCCESS: Die Replikation war erfolgreich.• AUSSTEHEND: Das Objekt wurde noch nicht repliziert.• FAILURE: Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.
Ziel	REPLIKAT : Das Objekt wurde aus dem Quellraster repliziert.



StorageGRID unterstützt das nicht `x-amz-replication-status` Kopfzeile.

Verwandte Informationen

["S3-Vorgänge werden in Prüfprotokollen nachverfolgt"](#)

WIEDERHERSTELLUNG VON POSTOBJEKTEN

Sie können die Wiederherstellungsanforderung für S3-OBJEKTE NACH DEM Posten verwenden, um ein Objekt wiederherzustellen, das in einem Cloud-Storage-Pool gespeichert ist.

Unterstützter Anforderungstyp

StorageGRID unterstützt nur ANFRAGEN zur WIEDERHERSTELLUNG EINES Objekts NACH DEM WIEDERHERSTELLEN. Das unterstützt nicht `SELECT` Art der Wiederherstellung. Wählen Sie Rückgabeanforderungen aus `XNotImplemented`.

Versionierung

Geben Sie optional an `versionId` Zum Wiederherstellen einer bestimmten Version eines Objekts in einem versionierten Bucket Wenn Sie keine Angabe machen `versionId`, Die neueste Version des Objekts wird wiederhergestellt

Verhalten DER WIEDERHERSTELLUNG NACH Objekten in Cloud-Storage-Pool-Objekten

Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wurde (siehe Anweisungen zum Managen von Objekten mit Information Lifecycle Management), weist eine Anfrage zur WIEDERHERSTELLUNG NACH dem Objekt auf Basis des Status des Objekts das folgende Verhalten auf. Weitere Informationen finden Sie unter „HEAD Object“.



Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wird und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, muss das Objekt nicht durch eine Wiederherstellungsanforderung FÜR DAS POSTOBJEKT wiederhergestellt werden. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

Status des Objekts	Verhalten DER WIEDERHERSTELLUNG NACH Objekten
Objekt wird in StorageGRID aufgenommen, aber noch nicht durch ILM evaluiert oder Objekt befindet sich nicht in einem Cloud-Storage-Pool	403 Forbidden, InvalidObjectState
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	200 OK Es werden keine Änderungen vorgenommen. Hinweis: Bevor ein Objekt in einen nicht-abrufbaren Zustand überführt wurde, kann es nicht geändert werden <code>expiry-date</code> .
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	202 Accepted Stellt eine abrufbare Kopie des Objekts für die im Anforderungstext angegebene Anzahl an Tagen in den Cloud-Speicher-Pool wieder her. Am Ende dieses Zeitraums wird das Objekt in einen nicht aufrufbaren Zustand zurückgeführt. Verwenden Sie optional den <code>Tier</code> Element anfordern, um zu bestimmen, wie lange der Wiederherstellungsauftrag dauern wird (Expedited, Standard, Oder Bulk). Wenn Sie keine Angabe machen <code>Tier</code> , Das Standard <code>Tier</code> wird verwendet. Wichtig: Wenn ein Objekt in S3 Glacier Deep Archive überführt wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, können Sie es nicht mit wiederherstellen <code>Expedited</code> Ebene: Der folgende Fehler wird zurückgegeben 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	409 Conflict, RestoreAlreadyInProgress
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	200 OK Hinweis: Wenn ein Objekt in einen aufrufbaren Zustand wiederhergestellt wurde, können Sie dessen ändern <code>expiry-date</code> Indem Sie die Anforderung zur Wiederherstellung DES POSTOBJEKTS mit einem neuen Wert für neu ausgeben <code>Days</code> . Das Wiederherstellungsdatum wird zum Zeitpunkt der Anfrage aktualisiert.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

"HEAD Objekt"

"S3-Vorgänge werden in Prüfprotokollen nachverfolgt"

PUT Objekt

Sie können die S3 PUT-Objektanforderung verwenden, um einem Bucket ein Objekt hinzuzufügen.

Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

Objektgröße

Die maximale Größe *empfohlen* für einen Vorgang mit einem PUT Objekt beträgt 5 gib (5,368,709,120 Byte). Wenn Sie über Objekte mit einer Größe von mehr als 5 gib verfügen, verwenden Sie stattdessen mehrteilige Uploads.

Die maximale *supported*-Größe für einen einzelnen PUT-Objekt-Vorgang beträgt 5 tib (5,497,558,138,880 Byte). Der Alarm * S3 PUT Objektgröße zu groß* wird jedoch ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das mehr als 5 gib beträgt.

Größe der Benutzer-Metadaten

Amazon S3 begrenzt die Größe der benutzerdefinierten Metadaten innerhalb jeder PUT-Anforderung-Kopfzeile auf 2 KB. StorageGRID begrenzt die Benutzermetadaten auf 24 KiB. Die Größe der benutzerdefinierten Metadaten wird gemessen, indem die Summe der Anzahl Bytes in der UTF-8-Codierung jedes Schlüssels und jeden Wert angegeben wird.

UTF-8 Zeichen in Benutzermetadaten

Wenn eine Anfrage UTF-8-Werte im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthält, ist das StorageGRID-Verhalten nicht definiert.

StorageGRID parst oder interpretiert keine entgangenen UTF-8-Zeichen, die im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthalten sind. Entgangenen UTF-8 Zeichen werden als ASCII-Zeichen behandelt:

- PUT-, PUT-Objekt-Copy-, GET- und HEAD-Anforderungen sind erfolgreich, wenn benutzerdefinierte Metadaten entgangenen UTF-8-Zeichen enthalten.
- StorageGRID gibt den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes undruckbare Zeichen enthält.

Grenzwerte für Objekt-Tags

Sie können neue Objekte mit Tags hinzufügen, wenn Sie sie hochladen, oder Sie können sie zu vorhandenen Objekten hinzufügen. StorageGRID und Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Tags, die einem Objekt zugeordnet sind, müssen über eindeutige Tag-Schlüssel verfügen. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein, und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.

Objekteigentümer

In StorageGRID sind alle Objekte Eigentum des Bucket-Besitzers-Kontos, einschließlich der Objekte, die von einem Konto ohne Eigentümer oder einem anonymen Benutzer erstellt wurden.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- Cache-Control
- Content-Disposition
- Content-Encoding

Wenn Sie angeben `aws-chunked` Für `Content-Encoding`StorageGRID überprüft die folgenden Elemente nicht:

- StorageGRID überprüft das nicht `chunk-signature` Auf die Chunk-Daten:
- StorageGRID überprüft nicht den Wert, den Sie für angeben `x-amz-decoded-content-length` Gegen das Objekt.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

Die Chunked-Übertragungscodierung wird unterstützt, wenn `aws-chunked` Zudem wird das Nutzlastsignieren verwendet.

- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten.

Verwenden Sie bei der Angabe des Name-value-Paars für benutzerdefinierte Metadaten dieses allgemeine Format:

```
x-amz-meta-name: value
```

Wenn Sie die Option **User Defined Creation Time** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie diese verwenden `creation-time` Als Name der Metadaten, die beim Erstellen des Objekts zeichnet. Beispiel:

```
x-amz-meta-creation-time: 1443399726
```

Der Wert für `creation-time` Wird seit dem 1. Januar 1970 als Sekunden ausgewertet.



Eine ILM-Regel kann nicht sowohl eine **benutzerdefinierte Erstellungszeit** für die Referenzzeit als auch die ausgeglichenen oder strengen Optionen für das Aufnahmeverhalten verwenden. Beim Erstellen der ILM-Regel wird ein Fehler zurückgegeben.

- `x-amz-tagging`
- S3-Objektsperungs-Anfrageheader
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

Wenn eine Anforderung ohne diese Header ausgeführt wird, werden die Standardaufbewahrungseinstellungen für Buckets verwendet, um den Versionsmodus des Objekts zu berechnen und das „behalt-bis“-Datum zu erhalten. Siehe "[Konfigurieren Sie die S3-Objektsperre über die S3-REST-API](#)".

- SSE-Anfragezeilen:
 - `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`

Siehe [Anforderungsheader für serverseitige Verschlüsselung](#)

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- Der `x-amz-acl` Die Anforderungsüberschrift wird nicht unterstützt.
- Der `x-amz-website-redirect-location` Die Anforderungsüberschrift wird nicht unterstützt und gibt zurück `XNotImplemented`.

Optionen der Storage-Klasse

Der `x-amz-storage-class` Die Anfrageüberschrift wird unterstützt. Der Wert, der für eingereicht wurde `x-amz-storage-class` Beeinträchtigt, wie StorageGRID Objektdaten während der Aufnahme schützt und nicht die Anzahl der persistenten Kopien des Objekts im StorageGRID System (das durch ILM bestimmt wird)

Wenn die ILM-Regel, die zu einem aufgenommenen Objekt passt, die strikte Option für das Aufnahmeverhalten verwendet, wird der aktiviert `x-amz-storage-class` Kopfzeile hat keine Wirkung.

Für können die folgenden Werte verwendet werden `x-amz-storage-class`:

- STANDARD (Standard)
 - **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, sobald ein Objekt aufgenommen wird, wird eine zweite Kopie dieses Objekts erstellt und auf einen anderen Storage Node verteilt (Dual Commit). Bei Bewertung des ILM bestimmt StorageGRID, ob diese ersten

Zwischenkopien die Anweisungen zur Platzierung in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an unterschiedlichen Standorten erstellt werden, und die ersten Zwischenkopien müssen eventuell 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 sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt `x-amz-storage-class` Kopfzeile hat keine Wirkung.

- **REDUCED_REDUNDANCY**

- **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
- **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt, erstellt StorageGRID nur eine Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung. Der `REDUCED_REDUNDANCY` Am besten eignet sich die Option, wenn die ILM-Regel, die mit dem Objekt übereinstimmt, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

Verwenden der `REDUCED_REDUNDANCY` Unter anderen Umständen wird eine Option nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhte das Risiko von Objektdatenverlusten bei der Aufnahme Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.



Da nur eine Kopie zu einem beliebigen Zeitpunkt repliziert werden kann, sind Daten einem ständigen Verlust ausgesetzt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Angaben `REDUCED_REDUNDANCY` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

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 Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird.

- `x-amz-server-side-encryption`
- **SSE-C:** Verwenden Sie alle drei dieser Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
 - `x-amz-server-side-encryption-customer-algorithm`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen für prüfen "[Serverseitige Verschlüsselung](#)".



Wenn ein Objekt mit SSE oder SSE-C verschlüsselt wird, werden sämtliche Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

Versionierung

Wenn die Versionierung für einen Bucket aktiviert ist, ist dies ein eindeutiger `versionId` Wird automatisch für die Version des zu speichernden Objekts generiert. Das `versionId` Wird auch in der Antwort mit zurückgegeben `x-amz-version-id` Kopfzeile der Antwort.

Wenn die Versionierung unterbrochen wird, wird die Objektversion mit einem Null gespeichert `versionId` Und wenn bereits eine Null-Version vorhanden ist, wird sie überschrieben.

Signaturberechnungen für den Autorisierungskopf

Bei Verwendung des `Authorization` Header zur Authentifizierung von Anfragen unterscheidet sich StorageGRID von AWS folgendermaßen:

- StorageGRID erfordert nicht `host` Kopfzeilen, die in enthalten sein sollen `CanonicalHeaders`.
- StorageGRID erfordert nicht `Content-Type` In enthalten sein `CanonicalHeaders`.
- StorageGRID erfordert nicht `x-amz-*` Kopfzeilen, die in enthalten sein sollen `CanonicalHeaders`.



Als allgemeine Best Practice sollten Sie diese Kopfzeilen immer in aufnehmen `CanonicalHeaders` Um sicherzustellen, dass sie überprüft werden; wenn Sie diese Header jedoch ausschließen, gibt StorageGRID keinen Fehler zurück.

Weitere Informationen finden Sie unter "[Signaturberechnungen für den Autorisierungskopf: Payload in einem einzelnen Chunk übertragen \(AWS Signature Version 4\)](#)".

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Operationen auf Buckets"](#)

["S3-Vorgänge werden in Prüfprotokollen nachverfolgt"](#)

"Wie Client-Verbindungen konfiguriert werden können"

PUT Objekt - Kopieren

Sie können das S3 PUT Object – Copy-Request verwenden, um eine Kopie eines Objekts zu erstellen, das bereits in S3 gespeichert ist. Ein PUT Object - Copy-Vorgang ist der gleiche wie ein GET und dann ein PUT.

Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

Objektgröße

Die maximale Größe *empfohlen* für einen Vorgang mit einem PUT Objekt beträgt 5 gib (5,368,709,120 Byte). Wenn Sie über Objekte mit einer Größe von mehr als 5 gib verfügen, verwenden Sie stattdessen mehrteilige Uploads.

Die maximale *supported*-Größe für einen einzelnen PUT-Objekt-Vorgang beträgt 5 tib (5,497,558,138,880 Byte). Der Alarm * S3 PUT Objektgröße zu groß* wird jedoch ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das mehr als 5 gib beträgt.

UTF-8 Zeichen in Benutzermetadaten

Wenn eine Anfrage UTF-8-Werte im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthält, ist das StorageGRID-Verhalten nicht definiert.

StorageGRID parst oder interpretiert keine entgangenen UTF-8-Zeichen, die im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthalten sind. Entgangenen UTF-8 Zeichen werden als ASCII-Zeichen behandelt:

- Anforderungen sind erfolgreich, wenn benutzerdefinierte Metadaten entgangenen UTF-8 Zeichen enthalten.
- StorageGRID gibt den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes undruckbare Zeichen enthält.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen 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`, Mit der Sie das Objekt und die zugehörigen Metadaten kopieren können.

Sie können angeben `REPLACE` Um beim Kopieren des Objekts die vorhandenen Metadaten zu überschreiben oder die Objektmetadaten zu aktualisieren.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: Der Standardwert ist `COPY`, Mit dem 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-Objektsperungs-Anfrageheader:**

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Wenn eine Anforderung ohne diese Header ausgeführt wird, werden die Standardaufbewahrungseinstellungen für Buckets verwendet, um den Versionsmodus des Objekts zu berechnen und das „behalt-bis“-Datum zu erhalten. Siehe ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

- **SSE-Anfragezeilen:**

- `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`

Siehe [Anforderungsheader für serverseitige Verschlüsselung](#)

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

Optionen der Storage-Klasse

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und hat Auswirkungen auf die Anzahl der Objektkopien, die StorageGRID erstellt, wenn die übereinstimmende ILM-Regel ein Aufnahmeverhalten der doppelten Übertragung oder Ausgewogenheit angibt.

- STANDARD

(Standard) gibt einen Dual-Commit-Aufnahmevergung an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance auf das Erstellen von Zwischenkopien zurückgreift.

- REDUCED_REDUNDANCY

Gibt einen Single-Commit-Aufnahmevergung an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitlicher Kopien zurückgreift.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt REDUCED_REDUNDANCY Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der REDUCED_REDUNDANCY Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

Verwenden von `x-amz-copy-source` in PUT Object - Copy

Wenn der Quell-Bucket und der Schlüssel im angegeben sind `x-amz-copy-source` Kopfzeile: Unterscheidet sich vom Ziel-Bucket und -Schlüssel, eine Kopie der Quell-Objektdaten wird auf das Ziel geschrieben.

Wenn die Quelle und das Ziel übereinstimmen, und die `x-amz-metadata-directive` Kopfzeile wird als angegeben REPLACE, Die Metadaten des Objekts werden mit den Metadaten aktualisiert, die in der Anforderung angegeben sind. In diesem Fall nimmt StorageGRID das Objekt nicht erneut auf. Dies hat zwei wichtige Folgen:

- SIE können PUT Object - Copy nicht verwenden, um ein vorhandenes Objekt zu verschlüsseln oder die Verschlüsselung eines vorhandenen Objekts zu ändern. Wenn Sie den bereitstellen `x-amz-server-side-encryption` Kopfzeile oder der `x-amz-server-side-encryption-customer-algorithm` Header, StorageGRID lehnt die Anforderung ab und gibt sie zurück XNotImplemented.
- Die in der übereinstimmenden ILM-Regel angegebene Option für das Aufnahmeverhalten wird nicht verwendet. Sämtliche durch das Update ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird.

Das heißt, wenn die ILM-Regel die strikte Option für das Aufnahmeverhalten verwendet, werden keine Maßnahmen ergriffen, wenn 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 Sie die serverseitige Verschlüsselung verwenden, hängen die von Ihnen zur Verfügung gestellten Anfrageheadern 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 wird,

müssen Sie die folgenden drei Header in die ANFORDERUNG PUT Object - Copy einschließen, damit das Objekt entschlüsselt und kopiert werden kann:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angabe 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, müssen Sie die folgenden drei Header angeben:
 - `x-amz-server-side-encryption-customer-algorithm`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen für prüfen "[Serverseitige Verschlüsselung](#)".

- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID (SSE) verwaltet wird, fügen Sie diesen Header in das PUT Object - Copy Request ein:

- `x-amz-server-side-encryption`



Der `server-side-encryption` Wert des Objekts kann nicht aktualisiert werden. Erstellen Sie stattdessen eine Kopie mit einer neuen `server-side-encryption`. Nutzen `x-amz-metadata-directive: REPLACE`.

Versionierung

Wenn der Quell-Bucket versioniert ist, können Sie den verwenden `x-amz-copy-source` Kopfzeile zum Kopieren der neuesten Version eines Objekts. Zum Kopieren einer bestimmten Version eines Objekts müssen Sie explizit die Version angeben, die kopiert werden soll `versionId` unterressource. Wenn der Ziel-Bucket versioniert ist, wird die generierte Version im zurückgegeben `x-amz-version-id` Kopfzeile der Antwort. Wenn die Versionierung für den Ziel-Bucket ausgesetzt ist, dann `x-amz-version-id` Gibt einen Wert „null“ zurück.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["S3-Vorgänge werden in Prüfprotokollen nachverfolgt"](#)

["PUT Objekt"](#)

SelektierObjectContent

Sie können die S3 SelectObjectContent-Anfrage verwenden, um den Inhalt eines S3-Objekts anhand einer einfachen SQL-Anweisung zu filtern.

Weitere Informationen finden Sie im ["AWS Dokumentation für SelectObjectContent"](#).

Bevor Sie beginnen

- Das Mandantenkonto hat die S3 Select-Berechtigung.
- Das ist schon `s3:GetObject` Berechtigung für das Objekt, das Sie abfragen möchten.
- Das Objekt, das Sie abfragen möchten, muss eines der folgenden Formate aufweisen:
 - **CSV**. Kann wie ist verwendet oder in GZIP- oder BZIP2-Archiven komprimiert werden.
 - **Parkett**. Zusätzliche Anforderungen an Parkett-Objekte:
 - S3 Select unterstützt nur Spaltenkomprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Komprimierung ganzer Objekte für Parkett-Objekte.
 - S3 Select unterstützt keine Parkett-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
 - Die maximale Größe der nicht komprimierten Zeilengruppe beträgt 512 MB.
 - Sie müssen die im Objektschema angegebenen Datentypen verwenden.
 - Sie können KEINE logischen TYPEN VON INTERVALL, JSON, LISTE, ZEIT oder UUID verwenden.
- Ihr SQL-Ausdruck hat eine maximale Länge von 256 KB.
- Jeder Datensatz im Eingang oder Ergebnis hat eine maximale Länge von 1 MiB.



Die Verwendung von ScanRange wird nicht unterstützt.

Beispiel für eine CSV-Anfrage-Syntax

```

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 Syntax der Parkettanforderung

```

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>

```

Beispiel für eine SQL-Abfrage

Diese Abfrage erhält den Staatsnamen, 2010 Populationen, geschätzte 2015 Populationen und den Prozentsatz der Änderung von den Daten der US-Volkszählung. Datensätze in der Datei, die keine Status 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, So aussehen:

```
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
```

Beispiel für die Verwendung von AWS und CLI (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 Zeilen der Ausgabedatei, changes.csv, So aussehen:

```
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
```

Beispiel für die Nutzung von AWS-CLI (Parkett)

```
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 wie folgt 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

In diesem Abschnitt wird beschrieben, wie StorageGRID Vorgänge für mehrteilige Uploads unterstützt.

Die folgenden Bedingungen und Hinweise gelten für alle mehrteiligen Uploadvorgänge:

- Sie sollten nicht mehr als 1,000 gleichzeitige mehrteilige Uploads in einen einzelnen Bucket durchführen, da die Ergebnisse der „List Multipart Uploads“-Abfragen für diesen Bucket möglicherweise unvollständige Ergebnisse liefern.
- StorageGRID setzt AWS Größenbeschränkungen für mehrere Teile durch. S3-Clients müssen folgende Richtlinien einhalten:
 - Jedes Teil eines mehrteiligen Uploads muss zwischen 5 MiB (5,242,880 Byte) und 5 gib (5,368,709,120 Byte) liegen.
 - Der letzte Teil kann kleiner als 5 MiB (5,242,880 Byte) sein.
 - Im Allgemeinen sollten die Teilemaße so groß wie möglich sein. Verwenden Sie z. B. für ein Objekt mit 100 gib die Teilenummer 5 gib. Da jedes Teil als ein eindeutiges Objekt angesehen wird, sinkt der Overhead für StorageGRID Metadaten durch die Verwendung großer Teilgrößen.
 - Verwenden Sie für Objekte, die kleiner als 5 gib sind, stattdessen einen Upload ohne mehrere Teile.
- ILM wird für jeden aufgenommenen Teil eines mehrteiligen Objekts und für das gesamte Objekt nach Abschluss des mehrteiligen Uploads bewertet, sofern die ILM-Regel das ausgewogene oder strikte Einspielverhalten verwendet. Sie sollten sich bewusst sein, wie dies die Objekt- und Teileplatzierung beeinflusst:
 - Wenn sich ILM-Änderungen während des Hochladens mehrerer S3-Teile ändern, erfüllt der mehrteilige Upload einige Teile des Objekts möglicherweise nicht die aktuellen ILM-Anforderungen. Nicht korrekt platzierte Teile werden zur ILM-Neubewertung in die Warteschlange verschoben und werden später an

den richtigen Ort verschoben.

- Bei der Evaluierung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils und nicht der Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn z. B. eine Regel angibt, dass alle Objekte ab 10 GB auf DC1 gespeichert werden, während alle kleineren Objekte an DC2 gespeichert sind, wird bei Aufnahme jeder 1 GB-Teil eines 10-teiligen mehrteiligen Uploads auf DC2 gespeichert. Wenn ILM für das Objekt als Ganzes bewertet wird, werden alle Teile des Objekts auf DC1 verschoben.
- Alle mehrteiligen Uploadvorgänge unterstützen die StorageGRID-Konsistenzkontrollen.
- Falls erforderlich, können Sie die Verschlüsselung auf Serverseite mit mehrteiligen Uploads verwenden. Um SSE (serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln) zu verwenden, müssen Sie das angeben `x-amz-server-side-encryption` Kopfzeile anfordern in der Anfrage zum Senden von mehrteiligen Uploads. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der Anfrage zum Hochladen von mehreren Teilen und bei jeder nachfolgenden Anfrage zum Hochladen von Teilen dieselben Schlüsselkopfzeilen an.

Betrieb	Implementierung
Mehrteilige Uploads Auflisten	Siehe " Mehrteilige Uploads Auflisten "
Initiieren Von Mehrteiligen Uploads	Siehe " Initiieren Von Mehrteiligen Uploads "
Hochladen Von Teilen	Siehe " Hochladen Von Teilen "
Hochladen Von Teilen - Kopieren	Siehe " Hochladen Von Teilen - Kopieren "
Abschließen Von Mehrteiligen Uploads	Siehe " Abschließen Von Mehrteiligen Uploads "
Abbrechen Von Mehrteiligen Uploads	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. Änderungen vorbehalten.
Teile Auflisten	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. Änderungen vorbehalten.

Verwandte Informationen

- "[Konsistenzkontrollen](#)"
- "[Serverseitige Verschlüsselung](#)"

Mehrteilige Uploads Auflisten

In der Operation „Mehrteilige Uploads auflisten“ werden derzeit mehrteilige Uploads für einen Bucket aufgeführt.

Die folgenden Anforderungsparameter werden unterstützt:

- `encoding-type`
- `key-marker`

- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Wenn der Vorgang zum vollständigen Hochladen mehrerer Teile ausgeführt wird, ist dies der Punkt, an dem Objekte erstellt werden (und gegebenenfalls versioniert).

Initiieren Von Mehrteiligen Uploads

Der Vorgang „Mehrteiliges Hochladen initiieren“ (CreateMultipartUpload) initiiert einen mehrteiligen Upload für ein Objekt und gibt eine Upload-ID zurück.

Der `x-amz-storage-class` Die Anfrageüberschrift wird unterstützt. Der Wert, der für eingereicht wurde `x-amz-storage-class` Beeinträchtigt, wie StorageGRID Objektdaten während der Aufnahme schützt und nicht die Anzahl der persistenten Kopien des Objekts im StorageGRID System (das durch ILM bestimmt wird)

Wenn die ILM-Regel, die zu einem aufgenommenen Objekt passt, die strikte Option für das Aufnahmeverhalten verwendet, wird der aktiviert `x-amz-storage-class` Kopfzeile hat keine Wirkung.

Für können die folgenden Werte verwendet werden `x-amz-storage-class`:

- STANDARD (Standard)
 - **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, sobald ein Objekt aufgenommen wird, wird eine zweite Kopie dieses Objekts erstellt und auf einen anderen Storage Node verteilt (Dual Commit). Bei Bewertung des ILM bestimmt StorageGRID, ob diese ersten Zwischenkopien die Anweisungen zur Platzierung in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an unterschiedlichen Standorten erstellt werden, und die ersten Zwischenkopien müssen eventuell 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 sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt `x-amz-storage-class` Kopfzeile hat keine Wirkung.

- REDUCED_REDUNDANCY
 - **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
 - **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt, erstellt StorageGRID nur eine Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann.

Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung. Der `REDUCED_REDUNDANCY` Am besten eignet sich die Option, wenn die ILM-Regel, die mit dem Objekt übereinstimmt, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

Verwenden der `REDUCED_REDUNDANCY` Unter anderen Umständen wird eine Option nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhte das Risiko von Objektdatenverlusten bei der Aufnahme Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.



Da nur eine Kopie zu einem beliebigen Zeitpunkt repliziert werden kann, sind Daten einem ständigen Verlust ausgesetzt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Angaben `REDUCED_REDUNDANCY` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

Die folgenden Anfragezeilen werden unterstützt:

- `Content-Type`
- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten

Verwenden Sie bei der Angabe des Name-value-Paars für benutzerdefinierte Metadaten dieses allgemeine Format:

```
x-amz-meta-__name__: `value`
```

Wenn Sie die Option **User Defined Creation Time** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie diese verwenden `creation-time` Als Name der Metadaten, die beim Erstellen des Objekts zeichnet. Beispiel:

```
x-amz-meta-creation-time: 1443399726
```

Der Wert für `creation-time` Wird seit dem 1. Januar 1970 als Sekunden ausgewertet.



Wird Hinzugefügt `creation-time` Da benutzerdefinierte Metadaten nicht zulässig sind, wenn Sie einem Bucket hinzufügen, auf dem die ältere Compliance aktiviert ist, ein Objekt. Ein Fehler wird zurückgegeben.

- S3-Objektsperungs-Anfrageheader:

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Wenn eine Anfrage ohne diese Header erstellt wird, werden die Bucket-Standardeinstellungen zur Aufbewahrung der Objektversion herangezogen, um die Aufbewahrung bis dato zu berechnen.

"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"

- SSE-Anfragezeilen:

- `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 darüber, wie StorageGRID UTF-8-Zeichen verarbeitet, finden Sie in der Dokumentation ZU PUT Object.

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 Anfrage Multipart hochladen, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird. Geben Sie diese Kopfzeile in keiner der Teileanforderungen hochladen an.
 - `x-amz-server-side-encryption`
- **SSE-C:** Verwenden Sie alle drei dieser Header in der Anfrage zum Initiate Multipart Upload (und in jeder nachfolgenden Anfrage zum Hochladen von Teilen), wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
 - `x-amz-server-side-encryption-customer-algorithm`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen für prüfen "[Serverseitige Verschlüsselung](#)".

Nicht unterstützte Anforderungsheader

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`

- `x-amz-website-redirect-location`

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["PUT Objekt"](#)

Hochladen Von Teilen

Der Vorgang „Teile hochladen“ lädt ein Teil in einem mehrteiligen Upload für ein Objekt hoch.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- `Content-Length`
- `Content-MD5`

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie die SSE-C-Verschlüsselung für die Anfrage zum Hochladen von mehreren Teilen angegeben haben, müssen Sie die folgenden Anfrageheader in jede Anfrage zum Hochladen von Teilen angeben:

- `x-amz-server-side-encryption-customer-algorithm`: Angabe AES256.
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der Anfrage zum Hochladen von mehreren Teilen angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den gleichen MD5-Digest an, den Sie in der Anfrage zum Hochladen mehrerer Teile angegeben haben.



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „[serverseitige Verschlüsselung verwenden](#)“.

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

Verwandte Informationen

["Serverseitige Verschlüsselung"](#)

Hochladen Von Teilen - Kopieren

Der Vorgang „Teil hochladen – Kopieren“ lädt einen Teil eines Objekts hoch, indem Daten aus einem vorhandenen Objekt als Datenquelle kopiert werden.

Der Vorgang „Hochladen von Teilen – Kopieren“ ist mit dem Verhalten der gesamten Amazon S3-REST-API implementiert. Änderungen vorbehalten.

Diese Anforderung liest und schreibt die Objektdaten, die in angegeben wurden `x-amz-copy-source-range` Innerhalb des StorageGRID-Systems.

Die folgenden Anfragezeilen 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 die SSE-C-Verschlüsselung für die Anfrage zum Hochladen von mehreren Teilen angegeben haben, müssen Sie die folgenden Anforderungsheader auch in jeden Upload Part - Copy request angeben:

- `x-amz-server-side-encryption-customer-algorithm`: Angabe AES256.
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der Anfrage zum Hochladen von mehreren Teilen angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den gleichen MD5-Digest an, den Sie in der Anfrage zum Hochladen mehrerer Teile angegeben haben.

Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt wird, müssen Sie die folgenden drei Header in die Anfrage „Teil hochladen – Kopieren“ aufnehmen, damit das Objekt entschlüsselt und anschließend kopiert werden kann:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden“.

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

Abschließen Von Mehrteiligen Uploads

Der komplette mehrteilige Upload-Vorgang führt einen mehrteiligen Upload eines Objekts durch, indem die zuvor hochgeladenen Teile zusammengebaut werden.

Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

Anfragekopfzeilen

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und hat Auswirkungen auf die Anzahl der Objektkopien, die StorageGRID erstellt, wenn die übereinstimmende ILM-Regel ein Aufnahmeverhalten der doppelten Übertragung oder Ausgewogenheit angibt.

- STANDARD

(Standard) gibt einen Dual-Commit-Aufnahmevergang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance auf das Erstellen von Zwischenkopien zurückgreift.

- REDUCED_REDUNDANCY

Gibt einen Single-Commit-Aufnahmevergang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitlicher Kopien zurückgreift.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigte REDUCED_REDUNDANCY Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der REDUCED_REDUNDANCY Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.



Wenn ein mehrtei. 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 Implementierung der Amazon S3-API `ETag` Wert für mehrteilige Objekte.

Versionierung

Durch diesen Vorgang ist ein mehrtei. Upload abgeschlossen. 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, ist dies ein eindeutiger `versionId` Wird automatisch für die Version des zu speichernden Objekts generiert. Das `versionId` Wird auch in der Antwort mit zurückgegeben `x-amz-version-id` Kopfzeile der Antwort.

Wenn die Versionierung unterbrochen wird, wird die Objektversion mit einem Null gespeichert `versionId` Und wenn bereits eine Null-Version vorhanden ist, wird sie überschrieben.



Wenn die Versionierung für einen Bucket aktiviert ist, erstellt das Abschließen eines mehrteiligen Uploads immer eine neue Version, selbst wenn mehrere Teile gleichzeitig auf denselben Objektschlüssel hochgeladen wurden. Wenn die Versionierung für einen Bucket nicht aktiviert ist, ist es möglich, einen mehrteiligen Upload zu initiieren und dann einen weiteren mehrteiligen Upload zu initiieren und zuerst auf demselben Objektschlüssel abzuschließen. In Buckets, die nicht versioniert sind, hat der mehrteilige Upload, der den letzten Teil abschließt, Vorrang.

Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

Wenn der Bucket, in dem der mehrteilige Upload stattfindet, für einen Plattformdienst konfiguriert ist, ist der mehrteilige Upload erfolgreich, auch wenn die zugehörige Replizierungs- oder Benachrichtigungsaktion fehlschlägt.

In diesem Fall wird im Grid Manager on Total Events (SMTT) ein Alarm ausgelöst. In der Meldung Letztes Ereignis wird „Fehler beim Veröffentlichen von Benachrichtigungen für Bucket-nameobject key“ für das letzte Objekt angezeigt, dessen Benachrichtigung fehlgeschlagen ist. (Um diese Meldung anzuzeigen, wählen Sie **NODES > Storage Node > Ereignisse**. Letztes Ereignis oben in der Tabelle anzeigen.) Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

Ein Mandant kann die fehlgeschlagene Replizierung oder Benachrichtigung auslösen, indem die Metadaten oder Tags des Objekts aktualisiert werden. Ein Mieter kann die vorhandenen Werte erneut einreichen, um unerwünschte Änderungen zu vermeiden.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

Fehlerantworten

Das StorageGRID System unterstützt alle zutreffenden S3-REST-API-Standardfehlerantworten. Darüber hinaus fügt die StorageGRID Implementierung mehrere individuelle Antworten hinzu.

Unterstützte S3-API-Fehlercodes

Name	HTTP-Status
AccessDenied	403 Verbotene
BadDigest	400 Fehlerhafte Anfrage

Name	HTTP-Status
BucketAlreadyExists	409 Konflikt
BucketNotEmpty	409 Konflikt
IncompleteBody	400 Fehlerhafte Anfrage
Interner Fehler	500 Fehler Des Internen Servers
InvalidAccessKey ID	403 Verbotene
InvalidArgument	400 Fehlerhafte Anfrage
InvalidBucketName	400 Fehlerhafte Anfrage
InvalidBucketState	409 Konflikt
InvalidDigest	400 Fehlerhafte Anfrage
InvalidVerschlüsselungAlgorithmFehler	400 Fehlerhafte Anfrage
InvalidTeil	400 Fehlerhafte Anfrage
InvalidPartOrder	400 Fehlerhafte Anfrage
InvalidRange	416 Angeforderter Bereich Nicht Zu Unterprüfbar
InvalidRequest	400 Fehlerhafte Anfrage
InvalidStorageClass	400 Fehlerhafte Anfrage
InvalidTag	400 Fehlerhafte Anfrage
InvalidURI	400 Fehlerhafte Anfrage
KeyTooLong	400 Fehlerhafte Anfrage
MalformedXML	400 Fehlerhafte Anfrage
MetadataTooLarge	400 Fehlerhafte Anfrage
MethodenAlled	405 Methode Nicht Zulässig
MissingContentLänge	411 Länge Erforderlich

Name	HTTP-Status
MissingRequestBodyError	400 Fehlerhafte Anfrage
MissingSecurityHeader	400 Fehlerhafte Anfrage
NoSuchBucket	404 Nicht Gefunden
NoSuchKey	404 Nicht Gefunden
NoSuchUpload	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
NoSuchBucketRichtlinien	404 Nicht Gefunden
ObjektLockKonfigurationNotgefundenFehler	404 Nicht Gefunden
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
AnforderungTimeTooSkewed	403 Verbotene
Servicenicht verfügbar	503 Service Nicht Verfügbar
SignalDoesNotMatch	403 Verbotene
TooManyDickets	400 Fehlerhafte Anfrage
UserKeyMustBespezifiziert	400 Fehlerhafte Anfrage

Benutzerdefinierte StorageGRID-Fehlercodes

Name	Beschreibung	HTTP-Status
XBucketLifecycleNotAlled	In einem zuvor konformen Bucket ist die Konfiguration des Bucket-Lebenszyklus nicht zulässig	400 Fehlerhafte Anfrage
XBucketPolicyParseException	Fehler beim Parsen der JSON der empfangenen Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XComplianceKonflikt	Vorgang aufgrund von Compliance-Einstellungen abgelehnt.	403 Verbotene
XComplianceReducedRAID-RedundanzVerbotenen	Reduzierte Redundanz ist in einem älteren, konformen Bucket nicht zulässig	400 Fehlerhafte Anfrage

Name	Beschreibung	HTTP-Status
XMaxBucketPolicyLengthexceed	Ihre Richtlinie überschreitet die maximal zulässige Länge der Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XMissingInternRequestHeader	Eine Kopfzeile einer internen Anforderung fehlt.	400 Fehlerhafte Anfrage
XNoSuchBucketCompliance	Für den angegebenen Bucket ist die veraltete Compliance nicht aktiviert.	404 Nicht Gefunden
XNotAcceptable	Die Anforderung enthält mindestens einen Übernehmen-Header, der nicht erfüllt werden konnte.	406 Nicht Akzeptabel
XNotImplemented	Die von Ihnen gestellte Anfrage beinhaltet Funktionen, die nicht implementiert sind.	501 Nicht Implementiert

StorageGRID S3-Anforderungen

Get Bucket-Konsistenz

Die GET Bucket-Konsistenzanforderung ermöglicht es Ihnen, das auf einen bestimmten Bucket angewendete Konsistenzlevel zu bestimmen.

Die standardmäßigen Konsistenzkontrollen garantieren „Read-after-Write“ für neu erstellte Objekte.

Sie verfügen über die s3:GetBucketConsistency-Berechtigung oder als Account-Root, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwort

In der XML-Antwortantwort <Consistency> Gibt einen der folgenden Werte zurück:

Konsistenzkontrolle	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.

Konsistenzkontrolle	Beschreibung
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
Verfügbar	Bietet eventuelle Konsistenz für neue Objekte und Objektaktualisierungen. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

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>
```

Verwandte Informationen

["Konsistenzkontrollen"](#)

PUT Bucket-Konsistenz

In der PUT Bucket-Konsistenzanforderung können Sie die Konsistenzstufe für Operationen angeben, die in einem Bucket durchgeführt werden.

Die standardmäßigen Konsistenzkontrollen garantieren „Read-after-Write“ für neu erstellte Objekte.

Bevor Sie beginnen

Sie haben die s3:PutBucketConsistency-Berechtigung, oder als Account-Root, um diesen Vorgang abzuschließen.

Anfrage

Der x-ntap-sg-consistency Parameter muss einen der folgenden Werte enthalten:

Konsistenzkontrolle	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
Verfügbar	Bietet eventuelle Konsistenz für neue Objekte und Objektaktualisierungen. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

Hinweis: im Allgemeinen sollten Sie den Wert der Consistency consistency control "read-after-New-write" verwenden. Wenn die Anforderungen nicht korrekt funktionieren, ändern Sie das Client-Verhalten der Anwendung, wenn möglich. Oder konfigurieren Sie den Client so, dass für jede API-Anforderung das Consistency Control angegeben wird. Legen Sie die Consistency Control auf Bucket-Ebene nur als letztes Resort fest.

Anforderungsbeispiel

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Verwandte Informationen

["Konsistenzkontrollen"](#)

ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN

In der Anforderung „letzte Bucket-Zugriffszeit“ KÖNNEN Sie festlegen, ob Updates der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind.

Sie verfügen über die berechtigung s3:GetBucketLastAccessTime oder als Kontostamm, 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 Updates 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-Zeit für den letzten Zugriff

In der ANFORDERUNG PUT Bucket Last Access Time können Sie Updates der letzten Zugriffszeit für einzelne Buckets aktivieren oder deaktivieren. Durch das Deaktivieren von Updates der letzten Zugriffszeit wird die Performance verbessert. Dies ist die Standardeinstellung für alle Buckets, die mit Version 10.3 oder höher erstellt wurden.

Sie haben die `s3:PutBucketLastAccessTime`-Berechtigung für einen Bucket oder als Account-Root, um diesen Vorgang abzuschließen.



Ab StorageGRID Version 10.3 sind Updates der letzten Zugriffszeit für alle neuen Buckets standardmäßig deaktiviert. Wenn Sie Buckets haben, die mit einer früheren Version von StorageGRID erstellt wurden und denen das neue Standardverhalten entsprechen möchten, müssen Sie für jeden dieser früheren Buckets explizit die Updates der letzten Zugriffszeit deaktivieren. Sie können Updates für die letzte Zugriffszeit aktivieren oder deaktivieren, indem Sie im Tenant Manager das Kontrollkästchen **S3 > Buckets > Letzte Zugriffseinstellung ändern** oder die Tenant Management API VERWENDEN.

Wenn Updates der letzten Zugriffszeit für einen Bucket deaktiviert wurden, wird das folgende Verhalten auf die Vorgänge auf dem Bucket angewendet:

- GET Object, GET Object ACL, GET Object Tagging und HEAD Object Requests aktualisieren nicht die letzte Zugriffszeit. Das Objekt wird zur Bewertung des Information Lifecycle Management (ILM) nicht zu Warteschlangen hinzugefügt.
- PUT Object – Copy and PUT Objekt-Tagging-Anforderungen, die nur die Metadaten aktualisieren, werden auch die letzte Zugriffszeit aktualisiert. Das Objekt wird Warteschlangen für die ILM-Bewertung

hinzugefügt.

- Wenn Updates zur letzten Zugriffszeit für den Quell-Bucket deaktiviert sind, AKTUALISIEREN PUT Object - Copy Requests nicht die letzte Zugriffszeit für den Quell-Bucket. Das kopierte Objekt wird nicht zu Warteschlangen für die ILM-Bewertung für den Quell-Bucket hinzugefügt. ALLERDINGS FÜR das Ziel PUT Object - Kopieranforderungen immer die letzte Zugriffszeit aktualisieren. Die Kopie des Objekts wird zu Warteschlangen für eine ILM-Bewertung hinzugefügt.
- Abschließen von mehrteiligen Upload-Anfragen, die die letzte Zugriffszeit aktualisieren. Das fertiggestellte Objekt wird zur ILM-Bewertung zu Warteschlangen hinzugefügt.

Beispiele anfordern

Dieses Beispiel ermöglicht die Zeit des letzten Zugriffs für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Dieses Beispiel deaktiviert die Zeit des letzten Zugriffs für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN

Mit der Konfigurationsanforderung FÜR DIE BENACHRICHTIGUNG „BUCKET-Metadaten LÖSCHEN“ können Sie den Suchintegrationsdienst für einzelne Buckets deaktivieren, indem Sie die Konfigurations-XML löschen.

Sie haben die berechtigung s3:DeleteBucketMetadataNotification für einen Bucket oder als Account-Root, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Dieses Beispiel zeigt die Deaktivierung des Suchintegrationservice für einen Bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN

Die Konfigurationsanforderung FÜR GET Bucket-Metadaten-Benachrichtigungen ermöglicht es Ihnen, die Konfigurations-XML abzurufen, die zur Konfiguration der Suchintegration für einzelne Buckets verwendet wird.

Sie verfügen über die Berechtigung `s3:GetBucketMetadataNotification` oder als Account root, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Diese Anforderung ruft die Konfiguration der Metadatenbenachrichtigung für den Bucket ab `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwort

Der Response Body umfasst die Konfiguration der Metadaten-Benachrichtigung für den Bucket. Anhand der Konfiguration der Metadatenbenachrichtigung können Sie festlegen, wie der Bucket für die Suchintegration konfiguriert ist. So können Unternehmen ermitteln, welche Objekte indiziert sind 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 Konfiguration für die Metadatenbenachrichtigung enthält mindestens ein Regeln. Jede Regel gibt die Objekte an, die auf sie angewendet werden, und das Ziel, an dem StorageGRID Objekt-Metadaten senden soll. Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	<p>Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen</p> <p>Enthält mindestens ein Regelement.</p>	Ja.
Regel	<p>Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen.</p> <p>Regeln mit überlappenden Präfixen werden abgelehnt.</p> <p>Im MetadataNotificationConfiguration Element enthalten.</p>	Ja.
ID	<p>Eindeutige Kennung für die Regel.</p> <p>In das Element Regel aufgenommen.</p>	Nein
Status	<p>Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Präfix	<p>Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>In das Element Regel aufgenommen.</p>	Ja.

Name	Beschreibung	Erforderlich
Urne	<p>URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • es Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl.</p> <p>Urne ist im Element Ziel enthalten.</p>	Ja.

Antwortbeispiel

Die XML, die zwischen dem enthalten ist

```
<MetadataNotificationConfiguration></MetadataNotificationConfiguration>
```

tags zeigen, wie die Integration in einen Endpunkt zur Integration der Suchfunktion für den Bucket konfiguriert wird. In diesem Beispiel werden Objektmetadaten an einen Elasticsearch-Index mit dem Namen `current` gesendet. Und geben Sie den Namen ein `2017`. Das wird in einer AWS-Domäne mit dem Namen `records` gehostet.

```
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>
```

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

PUT Bucket-Metadaten-Benachrichtigungskonfiguration

Die Konfigurationsanforderung FÜR PUT Bucket-Metadaten-Benachrichtigungen ermöglicht es Ihnen, den Such-Integrationservice für einzelne Buckets zu aktivieren. Die XML-Konfiguration für die Metadatenbenachrichtigung, die Sie im Anforderungsindex angeben, gibt die Objekte an, deren Metadaten an den Zielsuchindex gesendet werden.

Sie haben die `s3:PutBucketMetadataNotification`-Berechtigung für einen Bucket oder als Account-Root, um diesen Vorgang abzuschließen.

Anfrage

Die Anforderung muss die Konfiguration der Metadatenbenachrichtigung in der Anfraentext enthalten. Jede Konfiguration für die Metadatenbenachrichtigung enthält mindestens ein Regeln. Jede Regel gibt die Objekte an, auf die sie angewendet wird, und das Ziel, an dem StorageGRID Metadaten senden soll.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix `/images` An ein Ziel und Objekte mit dem Präfix `/videos` Nach anderen.

Konfigurationen mit überlappenden Präfixen sind nicht gültig und werden beim Einreichen abgelehnt. Beispiel: Eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` Enthielt Und eine zweite Regel für Objekte mit dem Präfix `test2` Nicht erlaubt.

Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden. Der Endpunkt muss

vorhanden sein, wenn die Konfiguration der Metadatenbenachrichtigung gesendet wird oder die Anforderung als fehlschlägt 400 Bad Request. In der Fehlermeldung steht: 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>

```

In der Tabelle werden die Elemente in der XML-Konfiguration für die Metadatenbenachrichtigung beschrieben.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelement.	Ja.
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration Element enthalten.	Ja.
ID	Eindeutige Kennung für die Regel. In das Element Regel aufgenommen.	Nein
Status	Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt. In das Element Regel aufgenommen.	Ja.

Name	Beschreibung	Erforderlich
Präfix	<p>Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Urne	<p>URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • es Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl.</p> <p>Urne ist im Element Ziel enthalten.</p>	Ja.

Beispiele anfordern

Dieses Beispiel zeigt die Aktivierung der Integration von Suchvorgängen 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 sind die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/images` An ein Ziel gesendet wird, während die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/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-1:33333333: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 Suchintegrations-Service generierter JSON

Wenn Sie den Such-Integrationservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielpunkt gesendet, wenn Metadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden.

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden kann, wenn ein Objekt mit dem Schlüssel enthält `SGWS/Tagging.txt` Wird in einem Bucket mit dem Namen erstellt `test`. Der `test` Der Bucket ist nicht versioniert, daher der `versionId` Das 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"
  }
}

```

Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten

In der Tabelle sind alle Felder aufgeführt, die im JSON-Dokument enthalten sind, die beim Aktivierung der Suchintegration an den Zielendpunkt gesendet werden.

Der Dokumentname umfasst, falls vorhanden, den Bucket-Namen, den Objektnamen und die Version-ID.

Typ	Elementname	Beschreibung
Bucket- und Objektinformationen	Eimer	Name des Buckets
Bucket- und Objektinformationen	Taste	Name des Objektschlüssels
Bucket- und Objektinformationen	VersionID	Objektversion für Objekte in versionierten Buckets
Bucket- und Objektinformationen	Werden	Beispielsweise Bucket-Region <code>us-east-1</code>
System-Metadaten	Größe	Objektgröße (in Byte) wie für einen HTTP-Client sichtbar
System-Metadaten	md5	Objekt-Hash
Benutzer-Metadaten	Metadaten <i>key:value</i>	Alle Benutzer-Metadaten des Objekts als Schlüssel-Wert-Paare
Tags	tags <i>key:value</i>	Alle für das Objekt definierten Objekt-Tags als Schlüsselwert-Paare



Für Tags und Benutzer-Metadaten gibt StorageGRID Daten und Nummern an Elasticsearch als Strings oder als S3-Ereignisbenachrichtigungen weiter. Um Elasticsearch so zu konfigurieren, dass diese Strings als Daten oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen für die dynamische Feldzuordnung und die 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.

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

Storage-Nutzungsanforderung ABRUFEN

Der Antrag ZUR GET Storage-Nutzung gibt Ihnen die Gesamtzahl des verwendeten Storage durch ein Konto und für jeden mit dem Account verknüpften Bucket an.

Die Menge des von einem Konto und seinen Buckets verwendeten Speichers kann durch eine geänderte GET-Service-Anforderung beim abgerufen werden `x-ntap-sg-usage` Abfrageparameter. Die Nutzung des Bucket-Storage wird getrennt von DEN PUT- und LÖSCHANFRAGEN, die vom System verarbeitet werden, nachverfolgt. Es kann zu einer gewissen Verzögerung kommen, bevor die Nutzungswerte auf der Grundlage der Verarbeitung von Anfragen den erwarteten Werten entsprechen, insbesondere wenn das System unter hoher Belastung steht.

StorageGRID versucht standardmäßig, Nutzungsdaten mithilfe einer starken globalen Konsistenz abzurufen. Wenn eine starke globale Konsistenz nicht erreicht werden kann, versucht StorageGRID, die Verwendungsinformationen in einer starken Site-Konsistenz abzurufen.

Sie haben die `s3:ListAllMyBuckets`-Berechtigung, oder als Account-Root, um diese Operation abzuschließen.

Anforderungsbeispiel

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

Dieses Beispiel zeigt ein Konto, das vier Objekte und 12 Bytes Daten in zwei Buckets enthält. 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 zum bei `ObjectCount` Und `DataBytes` Werte in der Antwort. Löschmarkierungen werden dem nicht hinzugefügt `ObjectCount` Gesamt:

Verwandte Informationen

["Konsistenzkontrollen"](#)

Veraltete Bucket-Anforderungen für ältere Compliance

Möglicherweise müssen Sie die StorageGRID S3 REST-API zum Management von Buckets verwenden, die mit der älteren Compliance-Funktion erstellt wurden.

Compliance-Funktion veraltet

Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

Wenn Sie zuvor die Einstellung für globale Konformität aktiviert haben, ist die globale S3-Objektsperre in StorageGRID 11.6 aktiviert. Neue Buckets können nicht mehr mit aktivierter Compliance erstellt werden.

Trotzdem können Sie bei Bedarf die StorageGRID S3 REST-API verwenden, um alle vorhandenen, älteren, konformen Buckets zu managen.

- ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)
- ["Objektmanagement mit ILM"](#)
- ["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Veraltete Compliance-Anforderungen:

- ["Veraltet – PUT Bucket-Anforderung-Änderungen aus Compliance-Gründen"](#)

Das SGCompliance XML-Element ist veraltet. Zuvor könnten Sie dieses benutzerdefinierte StorageGRID-Element in das optionale XML-Anforderungsgremium VON PUT Bucket-Anforderungen integrieren, um einen konformen Bucket zu erstellen.

- ["Veraltet – BUCKET-Compliance ABRUFEN"](#)

Die ANFORDERUNG „GET Bucket-Compliance“ ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die derzeit für einen vorhandenen, älteren, konformen Bucket geltenden Compliance-Einstellungen zu bestimmen.

- ["Veraltet – EINHALTUNG VON PUT Bucket"](#)

Die PUT Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Bucket zu ändern, der die Compliance-Anforderungen erfüllt. Sie können beispielsweise einen vorhandenen Bucket auf „Legal Hold“ platzieren oder den Aufbewahrungszeitraum erhöhen.

Veraltet: PUT Bucket-Request-Änderungen aus Compliance-Gründen

Das SGCompliance XML-Element ist veraltet. Zuvor könnten Sie dieses benutzerdefinierte StorageGRID-Element in das optionale XML-Anforderungsgremium VON PUT Bucket-Anforderungen integrieren, um einen konformen Bucket zu erstellen.



Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

["Objektmanagement mit ILM"](#)

["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Mit aktivierter Compliance können keine neuen Buckets mehr erstellt werden. Die folgende Fehlermeldung wird zurückgegeben, wenn Sie versuchen, die Put Bucket-Anforderung zur Compliance-Erstellung eines neuen Compliance-Buckets zu verwenden:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Veraltet: GET Bucket-Compliance-Anforderung

Die ANFORDERUNG „GET Bucket-Compliance“ ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die derzeit für einen vorhandenen, älteren, konformen Bucket geltenden Compliance-Einstellungen zu bestimmen.



Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

["Objektmanagement mit ILM"](#)

["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Sie verfügen über die Berechtigung `s3:GetBucketCompliance` oder als Kontostamm, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

In dieser Beispielanforderung können Sie die Compliance-Einstellungen für den Bucket mit dem Namen `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

In der XML-Antwortantwort `<SGCompliance>` führt die für den Bucket verwendeten Compliance-Einstellungen auf. Dieses Beispiel zeigt die Compliance-Einstellungen für einen Bucket, in dem jedes Objekt ein Jahr lang (525,600 Minuten) aufbewahrt wird, beginnend mit der Aufnahme des Objekts in das Grid. Derzeit ist keine gesetzliche Aufbewahrungspflicht auf diesem Bucket vorhanden. 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
WiederholungPeriodMinuten	Die Länge des Aufbewahrungszeitraums für Objekte, die diesem Bucket hinzugefügt wurden, in Minuten Der Aufbewahrungszeitraum beginnt, wenn das Objekt in das Raster aufgenommen wird.
LegalAlte	<ul style="list-style-type: none"> • Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn der Legal Hold aufgehoben wurde, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Eimer steht derzeit nicht unter einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können nach Ablauf ihres Aufbewahrungszeitraums gelöscht werden.
Automatisches Löschen	<ul style="list-style-type: none"> • Wahr: Die Objekte in diesem Bucket werden automatisch gelöscht, sobald ihre Aufbewahrungsfrist abgelaufen ist, es sei denn, der Bucket unterliegt einer gesetzlichen Aufbewahrungspflichten. • False: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abgelaufen ist. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Fehlerantworten

Wenn der Bucket nicht für 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 Anforderung jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Bucket zu ändern, der die Compliance-Anforderungen erfüllt. Sie können beispielsweise einen vorhandenen Bucket auf „Legal Hold“ platzieren oder den Aufbewahrungszeitraum

erhöhen.



Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

["Objektmanagement mit ILM"](#)

["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Sie verfügen über die s3:PutBucketCompliance-Berechtigung oder als Account-Root, um diesen Vorgang abzuschließen.

Wenn Sie eine PUT Bucket-Compliance-Anforderung ausgeben, müssen Sie für jedes Feld der Compliance-Einstellungen einen Wert angeben.

Anforderungsbeispiel

In dieser Beispielanforderung werden die Compliance-Einstellungen für den Bucket mit dem Namen geändert `mybucket`. In diesem Beispiel befinden sich die Objekte in `mybucket` Wird nun für zwei Jahre (1,051,200 Minuten) statt für ein Jahr beibehalten, beginnend mit dem Zeitpunkt, an dem das Objekt in das Grid aufgenommen wird. Es gibt keine gesetzliche Aufbewahrungspflichten auf diesem Bucket. 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
WiederholungPeriodMinuten	Die Länge des Aufbewahrungszeitraums für Objekte, die diesem Bucket hinzugefügt wurden, in Minuten Der Aufbewahrungszeitraum beginnt, wenn das Objekt in das Raster aufgenommen wird. Wichtig Wenn Sie einen neuen Wert für <code>RetentionPeriodMinutes</code> angeben, müssen Sie einen Wert angeben, der der aktuellen Aufbewahrungsfrist des Buckets entspricht oder größer ist. Nachdem die Aufbewahrungsfrist des Buckets festgelegt wurde, können Sie diesen Wert nicht verringern, sondern nur erhöhen.

Name	Beschreibung
LegalAlte	<ul style="list-style-type: none"> • Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn der Legal Hold aufgehoben wurde, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Eimer steht derzeit nicht unter einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können nach Ablauf ihres Aufbewahrungszeitraums gelöscht werden.
Automatisches Löschen	<ul style="list-style-type: none"> • Wahr: Die Objekte in diesem Bucket werden automatisch gelöscht, sobald ihre Aufbewahrungsfrist abgelaufen ist, es sei denn, der Bucket unterliegt einer gesetzlichen Aufbewahrungspflichten. • False: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abgelaufen ist. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Konsistenzstufe 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 Grid zu aktualisieren. Standardmäßig verwendet StorageGRID die Konsistenzstufe **stark global**, um zu gewährleisten, dass alle Datacenter-Standorte und alle Storage-Nodes mit Bucket-Metadaten Lese-/Schreibzugriff für die geänderten Compliance-Einstellungen erhalten.

Wenn StorageGRID die Konsistenzstufe **strong-global** 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 Storage-Services so schnell wie möglich verfügbar gemacht werden. Wenn der Grid-Administrator nicht in der Lage ist, an jedem Standort ausreichend Storage-Nodes zur Verfügung zu stellen, wird Sie vom technischen Support möglicherweise dazu gebracht, die ausgefallene Anforderung erneut zu versuchen, indem Sie die Konsistenzstufe für * strong-Site* erzwingen.



Erzwingen Sie niemals die * Strong-site* Consistency Level für PUT Bucket Compliance, es sei denn, Sie wurden dazu durch den technischen Support angewiesen, und es sei denn, Sie verstehen die möglichen Folgen der Verwendung dieser Ebene.

Wenn die Consistency Level auf **strong-site** reduziert wird, garantiert StorageGRID, dass aktualisierte Compliance-Einstellungen Lese-nach-Write-Konsistenz nur für Client-Anfragen innerhalb einer Site haben. Das bedeutet, dass das StorageGRID System vorübergehend mehrere inkonsistente Einstellungen für diesen Bucket bietet, bis alle Standorte und Storage-Nodes verfügbar sind. Die inkonsistenten Einstellungen können zu unerwarteten und unerwünschten Verhaltensweisen führen. Wenn Sie beispielsweise einen Bucket unter „Legal Hold“ platzieren und Sie eine niedrigere Konsistenzstufe erzwingen, sind die vorherigen Compliance-Einstellungen (d. h. „Legal Hold off“) des Buckets für einige Datacenter-Standorte möglicherweise weiterhin wirksam. Aus diesem Grund können Objekte, die Ihrer Meinung nach in einer gesetzlichen Wartefrist liegen, nach Ablauf ihres Aufbewahrungszeitraums entweder durch den Benutzer oder durch AutoDelete gelöscht werden, sofern diese Option aktiviert ist.

Um die Verwendung der Konsistenzstufe * Strong-site* zu erzwingen, geben Sie die PUT Bucket Compliance-Anforderung erneut aus und schließen Sie die ein `Consistency-Control` HTTP-Request-Header, wie folgt:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Fehlerantworten

- Wenn der Bucket nicht für konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort 404 Not Found.
- Wenn `RetentionPeriodMinutes` in der Anforderung ist kleiner als der aktuelle Aufbewahrungszeitraum des Buckets, lautet der HTTP-Statuscode 400 Bad Request.

Verwandte Informationen

["Veraltet: PUT Bucket-Request-Änderungen aus Compliance-Gründen"](#)

Bucket- und Gruppenzugriffsrichtlinien

Verwendung von Bucket- und Gruppenzugriffsrichtlinien

StorageGRID verwendet die Richtliniensprache für Amazon Web Services (AWS), um S3-Mandanten die Kontrolle des Zugriffs auf Buckets und Objekte innerhalb dieser Buckets zu ermöglichen. Das StorageGRID System implementiert eine Untermenge der S3-REST-API-Richtliniensprache. Zugriffsrichtlinien für die S3 API werden in JSON geschrieben.

Zugriffsrichtlinien – Überblick

Von StorageGRID werden zwei Arten von Zugriffsrichtlinien unterstützt:

- **Bucket-Richtlinien**, die mit DER GET Bucket-Richtlinie konfiguriert sind, PUT Bucket-Richtlinie und S3-API-Operationen FÜR die Bucket-Richtlinie LÖSCHEN. Bucket-Richtlinien sind mit Buckets verknüpft, so dass sie so konfiguriert sind, dass sie den Zugriff durch Benutzer im Bucket-Eigentümerkonto oder andere Konten an den Bucket und die darin befindlichen Objekte steuern. Eine Bucket-Richtlinie gilt nur für einen Bucket und möglicherweise auch für mehrere Gruppen.
- **Gruppenrichtlinien**, die mit dem Tenant Manager oder der Mandantenmanagement-API konfiguriert sind. Gruppenrichtlinien sind einer Gruppe im Konto zugeordnet, sodass sie so konfiguriert sind, dass sie der Gruppe ermöglichen, auf bestimmte Ressourcen zuzugreifen, die dem Konto gehören. Eine Gruppenrichtlinie gilt nur für eine Gruppe und möglicherweise für mehrere Buckets.



Es gibt keine Unterschiede in der Priorität zwischen Gruppen- und Bucket-Richtlinien.

StorageGRID Bucket und Gruppenrichtlinien folgen einer bestimmten Grammatik, die von Amazon definiert wurde. Innerhalb jeder Richtlinie gibt es eine Reihe von Richtlinienerklärungen, und jede Aussage enthält die folgenden Elemente:

- Statement-ID (Sid) (optional)
- Wirkung
- Principal/NotPrincipal
- Ressource/Ressource

- Aktion/Notaktion
- Bedingung (optional)

Richtlinienaussagen werden mithilfe dieser Struktur erstellt, um Berechtigungen anzugeben: <Effekt> gewähren, um <Principal> <Aktion> auf <Ressource> durchzuführen, wenn <Bedingung> angewendet wird.

Jedes Richtlinienelement wird für eine bestimmte Funktion verwendet:

Element	Beschreibung
Sid	Das Sid-Element ist optional. Der Sid ist nur als Beschreibung für den Benutzer gedacht. Diese wird vom StorageGRID System gespeichert, aber nicht interpretiert.
Wirkung	Verwenden Sie das Effektelement, um festzustellen, ob die angegebenen Vorgänge zulässig oder verweigert werden. Sie müssen anhand der Schlüsselwörter für unterstütztes Aktionselement Operationen identifizieren, die für Buckets oder Objekte zugelassen (oder verweigert) werden.
Principal/NotPrincipal	Benutzer, Gruppen und Konten können auf bestimmte Ressourcen zugreifen und bestimmte Aktionen ausführen. Wenn in der Anfrage keine S3-Signatur enthalten ist, ist ein anonymer Zugriff durch Angabe des Platzhalterzeichens (*) als Principal zulässig. Standardmäßig hat nur das Konto-Root Zugriff auf Ressourcen, die dem Konto gehören. Sie müssen nur das Hauptelement in einer Bucket-Richtlinie angeben. Bei Gruppenrichtlinien ist die Gruppe, der die Richtlinie zugeordnet ist, das implizite Prinzipalelement.
Ressource/Ressource	Das Ressourcenelement identifiziert Buckets und Objekte. Sie können Buckets und Objekten über den ARN (Amazon Resource Name) Berechtigungen gewähren oder verweigern, um die Ressource zu identifizieren.
Aktion/Notaktion	Die Elemente Aktion und Wirkung sind die beiden Komponenten von Berechtigungen. Wenn eine Gruppe eine Ressource anfordert, wird ihnen entweder der Zugriff auf die Ressource gewährt oder verweigert. Der Zugriff wird verweigert, es sei denn, Sie weisen ausdrücklich Berechtigungen zu, aber Sie können explizites Ablehnen verwenden, um eine von einer anderen Richtlinie gewährte Berechtigung zu überschreiben.
Zustand	Das Bedingungelement ist optional. Unter Bedingungen können Sie Ausdrücke erstellen, um zu bestimmen, wann eine Richtlinie angewendet werden soll.

Im Element Aktion können Sie das Platzhalterzeichen (*) verwenden, um alle Vorgänge oder eine Untermenge von Vorgängen anzugeben. Diese Aktion entspricht beispielsweise Berechtigungen wie s3:GetObject, s3:PutObject und s3>DeleteObject.

```
s3:*Object
```

Im Element `Resource` können Sie die Platzhalterzeichen (*) und (?) verwenden. Während das Sternchen (*) mit 0 oder mehr Zeichen übereinstimmt, ist das Fragezeichen (?) Entspricht einem beliebigen Zeichen.

Im Hauptelement werden Platzhalterzeichen nicht unterstützt, außer zum Festlegen eines anonymen Zugriffs, der allen Personen die Berechtigung gewährt. Sie legen beispielsweise den Platzhalter (*) als `Principal`-Wert fest.

```
"Principal": "*"
```

Im folgenden Beispiel verwendet die Anweisung die Elemente „Effekt“, „Principal“, „Aktion“ und „Ressource“. Dieses Beispiel zeigt eine vollständige Bucket-Richtlinienanweisung, die den Principals, die Admin-Gruppe, mit dem Effekt „Zulassen“ erhält `federated-group/admin` Und der Finanzgruppe `federated-group/finance`, Berechtigungen zur Durchführung der Aktion `s3:ListBucket` Auf dem genannten Bucket `mybucket` Und der 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:iam:s3::mybucket",
        "arn:aws:iam:s3::mybucket/*"
      ]
    }
  ]
}
```

Die Bucket-Richtlinie hat eine Größenbeschränkung von 20,480 Byte, und die Gruppenrichtlinie hat ein Größenlimit von 5,120 Byte.

Einstellungen zur Konsistenzkontrolle für Richtlinien

Standardmäßig sind alle Aktualisierungen, die Sie an Gruppenrichtlinien vornehmen, letztendlich konsistent. Sobald eine Gruppenrichtlinie konsistent wird, können die Änderungen aufgrund von Richtlinien-Caching

weitere 15 Minuten dauern. Standardmäßig sind alle Updates an den Bucket-Richtlinien ebenfalls konsistent.

Sie können bei Bedarf die Konsistenzgarantien für Bucket-Richtlinienaktualisierungen ändern. Beispielsweise könnte eine Änderung an einer Bucket-Richtlinie aus Sicherheitsgründen so schnell wie möglich wirksam werden.

In diesem Fall können Sie entweder die einstellen `Consistency-Control` Kopfzeile in der ANFORDERUNG DER PUT Bucket-Richtlinie, oder Sie können die PUT-Bucket-Konsistenzanforderung verwenden. Wenn Sie die Consistency Control für diese Anfrage ändern, müssen Sie den Wert **all** verwenden, der die höchste Garantie für die Konsistenz von Lesen nach dem Schreiben bietet. Wenn Sie einen anderen Wert für Consistency Control in einer Kopfzeile für die PUT Bucket Consistency Request angeben, wird die Anforderung abgelehnt. Wenn Sie einen anderen Wert für eine PUT Bucket Policy Request angeben, wird der Wert ignoriert. Sobald eine Bucket-Richtlinie konsistent ist, können die Änderungen aufgrund des Richtlinien-Caching weitere 8 Sekunden dauern.



Wenn Sie die Konsistenzstufe auf **alle** setzen, um eine neue Bucket-Richtlinie früher wirksam zu machen, stellen Sie die Bucket-Level-Kontrolle sicher, dass sie wieder auf ihren ursprünglichen Wert zurückgestellt wird, wenn Sie fertig sind. Andernfalls wird für alle zukünftigen Bucket-Anforderungen die **all**-Einstellung verwendet.

Verwenden Sie ARN in den Richtlinienerklärungen

In den Richtlinienerklärungen wird das ARN in Haupt- und Ressourcenelementen verwendet.

- Verwenden Sie diese Syntax, um die S3-Ressource ARN anzugeben:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Verwenden Sie diese Syntax, um die Identitätsressource ARN (Benutzer und Gruppen) festzulegen:

```
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 zu entsprechen.
- Internationale Zeichen, die im Objektschlüssel angegeben werden können, sollten mit JSON UTF-8 oder mit JSON \U Escape Sequenzen codiert werden. Die prozentuale Kodierung wird nicht unterstützt.

["RFC 2141 URN Syntax"](#)

Der HTTP-Anforderungskörper für DEN PUT Bucket-Richtlinienvorgang muss mit charset=UTF-8 codiert werden.

Geben Sie Ressourcen in einer Richtlinie an

In Richtlinienausrechnungen können Sie mithilfe des Elements Ressourcen den Bucket oder das Objekt angeben, für das Berechtigungen zulässig oder verweigert werden.

- Jede Richtlinienanweisung erfordert ein Ressourcenelement. In einer Richtlinie werden Ressourcen durch das Element gekennzeichnet `Resource`, Oder alternativ `NotResource` Für Ausschluss.
- Sie legen Ressourcen mit einer S3-Ressource ARN fest. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Sie können Richtlinienvariablen auch 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.

Principals in einer Policy angeben

Verwenden Sie das Hauptelement, um das Benutzer-, Gruppen- oder Mandantenkonto zu identifizieren, das über die Richtlinienanweisung Zugriff auf die Ressource erlaubt/verweigert wird.

- Jede Richtlinienanweisung in einer Bucket-Richtlinie muss ein Principal Element enthalten. Richtlinienanweisungen in einer Gruppenrichtlinie benötigen das Hauptelement nicht, da die Gruppe als Hauptelement verstanden wird.
- In einer Richtlinie werden die Prinzipien durch das Element „Principal,“ oder alternativ „NotPrincipal“ für den Ausschluss gekennzeichnet.
- Kontobasierte Identitäten müssen mit einer ID oder einem ARN angegeben werden:

```
"Principal": { "AWS": "account_id" }  
"Principal": { "AWS": "identity_arn" }
```

- In diesem Beispiel wird die Mandanten-Account-ID 27233906934684427525 verwendet, die das Konto-Root und alle Benutzer im Konto enthält:

```
"Principal": { "AWS": "27233906934684427525" }
```

- Sie können nur das Konto-Root angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Sie können einen bestimmten föderierten Benutzer („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 Principal angeben:

```
"Principal": "*" 
```

- Um Mehrdeutigkeiten zu vermeiden, können Sie die Benutzer-UUID anstelle des Benutzernamens verwenden:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

Angenommen, Alex verlässt zum Beispiel die Organisation und den Benutzernamen Alex Wird gelöscht. Wenn ein neuer Alex der Organisation beitrifft und dem gleichen zugewiesen wird Alex Benutzername: Der neue Benutzer erbt möglicherweise unbeabsichtigt die dem ursprünglichen Benutzer gewährten Berechtigungen.

- Der Hauptwert kann einen Gruppen-/Benutzernamen angeben, der beim Erstellen einer Bucket-Richtlinie noch nicht vorhanden ist.

Legen Sie Berechtigungen in einer Richtlinie fest

In einer Richtlinie wird das Aktionselement verwendet, um Berechtigungen einer Ressource zuzulassen/zu verweigern. Es gibt eine Reihe von Berechtigungen, die Sie in einer Richtlinie festlegen können, die durch das Element „Aktion“ gekennzeichnet sind, oder alternativ durch „NotAction“ für den Ausschluss. Jedes dieser Elemente wird bestimmten S3-REST-API-Operationen zugeordnet.

In den Tabellen werden die Berechtigungen aufgeführt, die auf Buckets angewendet werden, sowie die Berechtigungen, die für Objekte gelten.



Amazon S3 nutzt jetzt die Berechtigung s3:PutReplicationConfiguration sowohl für DIE PUT- als AUCH DELETE-Bucket-Replizierungsaktionen. StorageGRID verwendet für jede Aktion separate Berechtigungen, die mit der ursprünglichen Amazon S3 Spezifikation übereinstimmt.



EIN LÖSCHEN wird ausgeführt, wenn ein PUT zum Überschreiben eines vorhandenen Werts verwendet wird.

Berechtigungen, die für Buckets gelten

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:CreateBucket	Put Bucket	
s3>DeleteBucket	Bucket LÖSCHEN	
s3>DeleteBucketMetadataBenachrichtigung	Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN	Ja.
s3>DeleteBucketPolicy	Bucket-Richtlinie LÖSCHEN	
s3>DeleteReplicationConfiguration	Bucket-Replizierung LÖSCHEN	Ja, separate Berechtigungen für PUT und DELETE*
s3:GetBucketAcl	Bucket-ACL ABRUFEN	
s3:GetBucketCompliance	GET Bucket-Compliance (veraltet)	Ja.
s3:GetBucketConsistency	Get Bucket-Konsistenz	Ja.
s3:GetBucketCORS	Bucket-Cors ABRUFEN	
s3:GetVerschlüsselungKonfiguration	Get Bucket-Verschlüsselung	
s3:GetBucketLastAccessTime	ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN	Ja.
s3:GetBucketLocation	Bucket-Speicherort ABRUFEN	
s3:GetBucketMetadataBenachrichtigung	Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN	Ja.
s3:GetBucketBenachrichtigung	Bucket-Benachrichtigung ABRUFEN	
s3:GetBucketObjectLockConfiguration	Konfiguration der Objektsperre ABRUFEN	
s3:GetBucketPolicy	Get Bucket-Richtlinie	
s3:GetBucketTagging	Get Bucket-Tagging	
s3:GetBucketVersionierung	Get Bucket-Versionierung	
s3:GetLifecycleKonfiguration	BUCKET-Lebenszyklus ABRUFEN	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:GetReplicationConfiguration	GET Bucket-Replizierung	
s3:ListAllMyBuchs	<ul style="list-style-type: none"> • GET Service • GET Storage-Auslastung 	Ja, für GET Storage Usage
s3:ListBucket	<ul style="list-style-type: none"> • Bucket ABRUFEN (Objekte auflisten) • EIMER • WIEDERHERSTELLUNG VON POSTOBJEKTEN 	
s3:ListBucketMultipartUploads	<ul style="list-style-type: none"> • Mehrteilige Uploads Auflisten • WIEDERHERSTELLUNG VON POSTOBJEKTEN 	
s3:ListBucketVersions	Get Bucket-Versionen	
s3:PutBucketCompliance	PUT Bucket-Compliance (veraltet)	Ja.
s3:PutBucketConsistency	PUT Bucket-Konsistenz	Ja.
s3:PutBucketCORS	<ul style="list-style-type: none"> • Bucket Cors† LÖSCHEN • Bucket-Cors EINGEBEN 	
s3:PutVerschlüsselungKonfiguration	<ul style="list-style-type: none"> • Bucket-Verschlüsselung LÖSCHEN • Bucket-Verschlüsselung 	
s3:PutBucketLastAccessTime	PUT Bucket-Zeit für den letzten Zugriff	Ja.
s3:PutBucketMetadataBenachrichtigung	PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Ja.
s3:PutBucketNotification	PUT Bucket-Benachrichtigung	
s3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> • Geben Sie Bucket mit dem EIN <code>x-amz-bucket-object-lock-enabled: true</code> Kopfzeile anfordern (erfordert auch die Berechtigung <code>s3:CreateBucket</code>) • PUT Objekt Lock-Konfiguration 	
s3:PutBucketPolicy	Bucket-Richtlinie	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PutBucketTagging	<ul style="list-style-type: none"> • Bucket-Tagging† löschen • PUT Bucket-Tagging 	
s3:PutBucketVersionierung	PUT Bucket-Versionierung	
s3:PutLifecycleKonfiguration	<ul style="list-style-type: none"> • Bucket-Lebenszyklus LÖSCHEN† • PUT Bucket-Lebenszyklus 	
s3:PutReplikationKonfiguration	PUT Bucket-Replizierung	Ja, separate Berechtigungen für PUT und DELETE*

Berechtigungen, die sich auf Objekte beziehen

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:AbortMehnteilaUpload	<ul style="list-style-type: none"> • Abbrechen Von Mehrteiligen Uploads • WIEDERHERSTELLUNG VON POSTOBJEKTEN 	
s3:BypassGovernanceAufbewahrung	<ul style="list-style-type: none"> • Objekt LÖSCHEN • LÖSCHEN Sie mehrere Objekte • AUFBEWAHRUNG von Objekten 	
s3>DeleteObject	<ul style="list-style-type: none"> • Objekt LÖSCHEN • LÖSCHEN Sie mehrere Objekte • WIEDERHERSTELLUNG VON POSTOBJEKTEN 	
s3>DeleteObjectTagging	Objekt-Tagging LÖSCHEN	
s3>DeleteObjectVersionTagging	Objekt-Tagging LÖSCHEN (eine bestimmte Version des Objekts)	
s3>DeleteObjectVersion	Objekt LÖSCHEN (eine bestimmte Version des Objekts)	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:GetObject	<ul style="list-style-type: none"> • GET Objekt • HEAD Objekt • WIEDERHERSTELLUNG VON POSTOBJEKTEN • Wählen Sie Objektinhalt 	
s3:GetObjectAcl	GET Objekt-ACL	
s3:GetObjectLegalOld	HOLD-Aufbewahrung für Objekte	
s3:GetObjectRetention	Aufbewahrung von Objekten	
s3:GetObjectTagging	Get Objekt-Tagging	
s3:GetObjectVersionTagging	GET Object Tagging (eine bestimmte Version des Objekts)	
s3:GetObjectVersion	GET Object (eine bestimmte Version des Objekts)	
s3:ListeMultipartUploadParts	Teile auflisten, Objekt WIEDERHERSTELLEN	
s3:PutObject	<ul style="list-style-type: none"> • PUT Objekt • PUT Objekt - Kopieren • WIEDERHERSTELLUNG VON POSTOBJEKTEN • Initiieren Von Mehrteiligen Uploads • Abschließen Von Mehrteiligen Uploads • Hochladen Von Teilen • Hochladen Von Teilen - Kopieren 	
s3:PutObjectLegalOld	LEGALE Aufbewahrung des Objekts EINGEBEN	
s3:PutObjectRetention	AUFBEWAHRUNG von Objekten	
s3:PutObjectTagging	PUT Objekt-Tagging	
s3:PutObjectVersionTagging	PUT Objekt-Tagging (eine bestimmte Version des Objekts)	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PutOverwrite Object	<ul style="list-style-type: none"> • PUT Objekt • PUT Objekt - Kopieren • PUT Objekt-Tagging • Objekt-Tagging LÖSCHEN • Abschließen Von Mehrteiligen Uploads 	Ja.
s3:RestoreObject	WIEDERHERSTELLUNG VON POSTOBJEKTEN	

Verwenden Sie PutOverwriteObject-Berechtigung

die s3:PutOverwriteObject-Berechtigung ist eine benutzerdefinierte StorageGRID-Berechtigung, die für Vorgänge gilt, die Objekte erstellen oder aktualisieren. Durch diese Berechtigung wird festgelegt, ob der Client die Daten, benutzerdefinierte Metadaten oder S3-Objekt-Tagging überschreiben kann.

Mögliche Einstellungen für diese Berechtigung sind:

- **Zulassen:** Der Client kann ein Objekt überschreiben. Dies ist die Standardeinstellung.
- **Deny:** Der Client kann ein Objekt nicht überschreiben. Wenn die Option „Ablehnen“ eingestellt ist, funktioniert die Berechtigung „PutOverwriteObject“ wie folgt:
 - Wenn ein vorhandenes Objekt auf demselben Pfad gefunden wird:
 - Die Daten, benutzerdefinierten Metadaten oder S3-Objekt-Tagging des Objekts können nicht überschrieben werden.
 - Alle laufenden Aufnahmevorgänge werden abgebrochen und ein Fehler wird zurückgegeben.
 - Wenn die S3-Versionierung aktiviert ist, verhindert die Einstellung Deny, dass PUT Objekt-Tagging oder DELETE Objekt-Tagging die TagSet für ein Objekt und seine nicht aktuellen Versionen ändert.
 - Wenn ein vorhandenes Objekt nicht gefunden wird, hat diese Berechtigung keine Wirkung.
- Wenn diese Berechtigung nicht vorhanden ist, ist der Effekt der gleiche, als ob Allow-were gesetzt wurden.



Wenn die aktuelle S3-Richtlinie Überschreiben zulässt und die PutOverwriteObject-Berechtigung auf Deny festgelegt ist, kann der Client die Daten, benutzerdefinierten Metadaten oder Objekt-Tagging eines Objekts nicht überschreiben. Wenn zusätzlich das Kontrollkästchen **Client-Änderung verhindern** aktiviert ist (**KONFIGURATION > Sicherheitseinstellungen > Netzwerk und Objekte**), setzt diese Einstellung die Einstellung der PutOverwriteObject-Berechtigung außer Kraft.

Legen Sie Bedingungen in einer Richtlinie fest

Die Bedingungen legen fest, wann eine Richtlinie in Kraft sein wird. Die Bedingungen bestehen aus Bedienern und Schlüsselwertpaaren.

Bedingungen Verwenden Sie Key-Value-Paare für die Auswertung. Ein Bedingungelement kann mehrere Bedingungen enthalten, und jede Bedingung kann mehrere Schlüsselwert-Paare enthalten. Der Bedingungsblock verwendet das folgende Format:

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

Im folgenden Beispiel verwendet die IPAddress-Bedingung den SourceIp-Bedingungsschlüssel.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

Unterstützte Bedingungsoperatoren

Bedingungsoperatoren werden wie folgt kategorisiert:

- Zeichenfolge
- Numerisch
- Boolesch
- IP-Adresse
- Null-Prüfung

Bedingungsoperatoren	Beschreibung
StringEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird beachtet).
StringNotEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird beachtet).
StringEquisgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird ignoriert).
StringNotEquisgnoreCase	Vergleicht einen Schlüssel mit einem String-Wert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird ignoriert).
StringLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen.
StringNotLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen.

Bedingungsoperatoren	Beschreibung
Ziffern	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf exakter Übereinstimmung basiert.
ZiffernNotequals	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf negatives Matching basiert.
NumericGreaterThan	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „größer als“-Übereinstimmung basiert.
ZahlungGreaterThanEquals	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „größer als oder gleich“-Übereinstimmung basiert.
NumericLessThan	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „weniger als“-Übereinstimmung basiert.
ZahlungWenigerThanEquals	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „kleiner als oder gleich“-Übereinstimmung basiert.
Bool	Vergleicht einen Schlüssel mit einem Booleschen Wert auf der Grundlage von „true“ oder „false“-Übereinstimmung.
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 negatierem Abgleich.
Null	Überprüft, ob im aktuellen Anforderungskontext ein Bedingungsschlüssel vorhanden ist.

Unterstützte Bedingungsschlüssel

Kategorie	Die entsprechenden Bedingungsschlüssel	Beschreibung
IP-Operatoren	aws:SourceIp	<p>Vergleicht mit der IP-Adresse, von der die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden</p> <p>Hinweis: wurde die S3-Anfrage über den Lastbalancer-Dienst auf Admin-Knoten und Gateways-Knoten gesendet, wird dies mit der IP-Adresse verglichen, die vor dem Load Balancer Service liegt.</p> <p>Hinweis: Wenn ein Drittanbieter-, nicht-transparenter Load Balancer verwendet wird, wird dies mit der IP-Adresse dieses Load Balancer verglichen. Alle <code>X-Forwarded-For</code> Kopfzeile wird ignoriert, da ihre Gültigkeit nicht ermittelt werden kann.</p>
Ressource/Identität	aws:Benutzername	Vergleicht mit dem Benutzernamen des Absenders, von dem die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden
s3:ListBucket und s3:ListBucketVersions Berechtigungen	s3:Trennzeichen	Vergleicht mit dem Parameter Trennzeichen, der in einer Anforderung GET Bucket oder GET Bucket Object Version angegeben ist.
s3:ListBucket und s3:ListBucketVersions Berechtigungen	s3:max-keys	Vergleicht den Parameter max-keys, der in einer Anforderung FÜR GET Bucket oder GET Bucket Object-Versionen angegeben ist.
s3:ListBucket und s3:ListBucketVersions Berechtigungen	s3:Präfix	Vergleicht mit dem Präfixparameter, der in einer Anforderung FÜR GET Bucket oder GET Bucket Object-Versionen angegeben ist.
s3:PutObject	s3:verbleibende Object-Lock-Retention-Tage	<p>Vergleicht mit dem in angegebenen Aufbewahrungsdatum <code>x-amz-object-lock-retain-until-date</code> Kopfzeile anfordern oder berechnet aus der Standardaufbewahrungsdauer des Buckets, um sicherzustellen, dass diese Werte innerhalb des zulässigen Bereichs für die folgenden Anforderungen liegen:</p> <ul style="list-style-type: none"> • PUT Objekt • PUT Objekt - Kopieren • Initiieren Von Mehrteiligen Uploads

Kategorie	Die entsprechenden Bedingungsschlüssel	Beschreibung
s3:PutObjectRetention	s3:verbleibende Object-Lock-Retention-Tage	Vergleicht mit dem in der ANFORDERUNG PUT Object Retention angegebenen Aufbewahrungsdatum, um sicherzustellen, dass dieser innerhalb des zulässigen Bereichs liegt.

Geben Sie Variablen in einer Richtlinie an

Sie können Variablen in Richtlinien verwenden, um die Richtlinieninformationen auszufüllen, wenn sie verfügbar sind. Sie können Richtlinienvariablen in verwenden `Resource` Element und in String-Vergleichen im `Condition` Element:

In diesem Beispiel die Variable `${aws:username}` Ist Teil des Ressourcenelements:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In diesem Beispiel die Variable `${aws:username}` Ist Teil des Bedingungswertes im Bedingungsblock:

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variabel	Beschreibung
<code>\${aws:SourceIp}</code>	Verwendet den SourceIp-Schlüssel als bereitgestellte Variable.
<code>\${aws:username}</code>	Verwendet den Benutzernamen-Schlüssel als bereitgestellte Variable.
<code>\${s3:prefix}</code>	Verwendet den Service-spezifischen Präfixschlüssel als bereitgestellte Variable.
<code>\${s3:max-keys}</code>	Verwendet die Service-spezifische max-keys als die angegebene Variable.
<code>\${*}</code>	Sonderzeichen. Verwendet das Zeichen als Literal * -Zeichen.
<code>\${?}</code>	Sonderzeichen. Verwendet den Charakter als Literal ? Zeichen.
<code>\${\$}</code>	Sonderzeichen. Verwendet das Zeichen als Literal USD Zeichen.

Erstellen von Richtlinien, die eine spezielle Handhabung erfordern

Manchmal kann eine Richtlinie Berechtigungen erteilen, die für die Sicherheit oder die Gefahr für einen fortgesetzten Betrieb gefährlich sind, z. B. das Sperren des Root-Benutzerkontos. Die StorageGRID S3-REST-API-Implementierung ist bei der Richtliniengültigkeit weniger restriktiv als Amazon, aber auch bei der Richtliniengültigkeit streng.

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Verweigern Sie sich selbst irgendwelche Berechtigungen für das Root-Konto	Eimer	Gültig und durchgesetzt, aber das Root-Benutzerkonto behält die Berechtigung für alle S3 Bucket-Richtlinienvorgänge bei	Gleich
Verweigern Sie selbst jegliche Berechtigungen für Benutzer/Gruppe	Gruppieren	Gültig und durchgesetzt	Gleich
Erlauben Sie einer fremden Kontogruppe jegliche Berechtigung	Eimer	Ungültiger Principal	Gültig, aber die Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben bei Richtliniengültigkeit durch eine Richtlinie einen nicht zugelassenen 405-Method-Fehler zurück
Berechtigung für ein ausländisches Konto oder einen Benutzer zulassen	Eimer	Gültig, aber die Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben bei Richtliniengültigkeit durch eine Richtlinie einen nicht zugelassenen 405-Method-Fehler zurück	Gleich
Alle Berechtigungen für alle Aktionen zulassen	Eimer	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405 Methode nicht erlaubten Fehler für das ausländische Konto Root und Benutzer zurück	Gleich
Alle Berechtigungen für alle Aktionen verweigern	Eimer	Gültig und durchgesetzt, aber das Root-Benutzerkonto behält die Berechtigung für alle S3 Bucket-Richtlinienvorgänge bei	Gleich

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Principal ist ein nicht existierender Benutzer oder eine Gruppe	Eimer	Ungültiger Principal	Gültig
Die Ressource ist ein nicht existierender S3-Bucket	Gruppieren	Gültig	Gleich
Principal ist eine lokale Gruppe	Eimer	Ungültiger Principal	Gültig
Policy gewährt einem nicht-Inhaberkonto (einschließlich anonymer Konten) Berechtigungen zum PUT von Objekten	Eimer	Gültig. Objekte sind Eigentum des Erstellerkontos, und die Bucket-Richtlinie gilt nicht. Das Ersteller-Konto muss über Objekt-ACLs Zugriffsrechte für das Objekt gewähren.	Gültig. Der Eigentümer der Objekte ist das Bucket-Owner-Konto. Bucket-Richtlinie gilt.

WORM-Schutz (Write Once, Read Many)

Sie können WORM-Buckets (Write-Once-Read-Many) erstellen, um Daten, benutzerdefinierte Objekt-Metadaten und S3-Objekt-Tagging zu sichern. SIE konfigurieren die WORM-Buckets, um das Erstellen neuer Objekte zu ermöglichen und Überschreibungen oder das 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 **CONFIGURATION > Security > Security settings > Network and Objects** und aktivieren Sie das Kontrollkästchen **Client-Änderung verhindern**.
- Wenden Sie die folgenden Regeln und S3-Richtlinien an:
 - Fügen Sie der S3-Richtlinie einen PutOverwriteObject DENY-Vorgang hinzu.
 - Fügen Sie der S3-Richtlinie einen DeleteObject DENY-Vorgang hinzu.
 - Fügen Sie der S3-Richtlinie einen PUT Object ALLOW-Vorgang hinzu.



Wenn DeleteObject in einer S3-Richtlinie VERWEIGERT wird, verhindert dies nicht, dass ILM Objekte löscht, wenn eine Regel wie „Zero Copies after 30 days“ vorhanden ist.



Selbst wenn alle diese Regeln und Richtlinien angewendet werden, schützen sie sich nicht vor gleichzeitigen Schreibvorgängen (siehe Situation A). Sie schützen vor sequenziellen Überschreibungen (siehe Situation B).

Situation A: Gleichzeitige Schreibvorgänge (nicht bewacht)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situation B: Sequentielle abgeschlossene Überschreibungen (bewacht gegen)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Verwandte Informationen

- ["Managen von Objekten durch StorageGRID ILM-Regeln"](#)
- ["Beispiel für Bucket-Richtlinien"](#)
- ["Beispiel für Gruppenrichtlinien"](#)
- ["Objektmanagement mit ILM"](#)
- ["Verwenden Sie ein Mandantenkonto"](#)

Beispiel für Bucket-Richtlinien

Mithilfe der Beispiele in diesem Abschnitt können Sie StorageGRID-Zugriffsrichtlinien für Buckets erstellen.

Bucket-Richtlinien geben die Zugriffsberechtigungen für den Bucket an, mit dem die Richtlinie verknüpft ist. Bucket-Richtlinien werden mithilfe der S3-PutBucketPolicy-API konfiguriert. Siehe ["Operationen auf Buckets"](#).

Eine Bucket-Richtlinie kann mithilfe der AWS CLI wie folgt konfiguriert werden:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

Beispiel: Lesezugriff auf einen Bucket zulassen

In diesem Beispiel darf jeder, auch anonym, Objekte im Bucket auflisten und get-Objektvorgänge an allen Objekten im Bucket durchführen. Alle anderen Operationen werden abgelehnt. Beachten Sie, dass diese Richtlinie möglicherweise nicht besonders nützlich ist, da niemand außer dem Konto root über Berechtigungen 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: Jeder in einem Konto Vollzugriff zulassen, und jeder in einem anderen Konto hat nur Lesezugriff auf einen Bucket

In diesem Beispiel ist jedem in einem bestimmten Konto der vollständige Zugriff auf einen Bucket gestattet, während jeder in einem anderen angegebenen Konto nur die Liste des Buckets und die Durchführung von GetObject-Operationen für Objekte im Bucket erlaubt ist, die mit dem beginnen `shared/` Objektschlüsselpräfix.



In StorageGRID sind Objekte, die von einem nicht-Inhaberkonto erstellt wurden (einschließlich anonymer Konten), Eigentum des Bucket-Inhaberkontos. Die Bucket-Richtlinie gilt für diese Objekte.

```

{
  "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: Lesezugriff für einen Bucket und vollständiger Zugriff durch angegebene Gruppe

In diesem Beispiel dürfen alle, einschließlich anonym, den Bucket auflisten und GET-Objektvorgänge für alle Objekte im Bucket durchführen, während nur Benutzer der Gruppe gehören Marketing Im angegebenen Konto ist Vollzugriff erlaubt.

```

{
  "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: Jeder Lese- und Schreibzugriff auf einen Bucket zulassen, wenn Client im IP-Bereich ist

In diesem Beispiel darf jeder, einschließlich anonym, den Bucket auflisten und beliebige Objektvorgänge an allen Objekten im Bucket durchführen, vorausgesetzt, dass die Anforderungen aus einem bestimmten IP-Bereich stammen (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: Vollständigen Zugriff auf einen Bucket zulassen, der ausschließlich von einem festgelegten föderierten Benutzer verwendet wird

In diesem Beispiel ist dem föderierten Benutzer Alex der vollständige Zugriff auf das erlaubt `examplebucket` Bucket und seine Objekte. Alle anderen Benutzer, einschließlich 'root', werden ausdrücklich allen Operationen verweigert. Beachten Sie jedoch, dass 'root' niemals die Berechtigungen 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 ist der `Deny` Effect für `PutOverwriteObject` und `DeleteObject` stellt sicher, dass niemand die Daten, benutzerdefinierte Metadaten und S3-Objekt-Tagging 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/*"
    }
  ]
}

```

Beispiel für Gruppenrichtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID-Zugriffsrichtlinien für Gruppen zu erstellen.

Gruppenrichtlinien legen die Zugriffsberechtigungen für die Gruppe fest, der die Richtlinie zugeordnet ist. Es gibt keine `Principal` Element in der Richtlinie, weil sie implizit ist. Gruppenrichtlinien werden mit dem Tenant Manager oder der API konfiguriert.

Beispiel: Legen Sie eine Gruppenrichtlinie mit Tenant Manager fest

Wenn Sie eine Gruppe im Tenant Manager hinzufügen oder bearbeiten, können Sie eine Gruppenrichtlinie auswählen, um festzulegen, über welche S3-Zugriffsberechtigungen die Mitglieder dieser Gruppe verfügen. Siehe ["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 über eine Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.
- **Schreibgeschützter Zugriff:** Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine schreibgeschützte Gruppenrichtlinie angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
- **Vollzugriff:** Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
- **Ransomware Mitigation:** Diese Beispielrichtlinie gilt für alle Buckets für diesen Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber Objekte aus Buckets, für die die Objektversionierung aktiviert ist, nicht dauerhaft löschen.

Mandanten-Manager-Benutzer mit der Berechtigung zum Verwalten aller Buckets können diese Gruppenrichtlinie überschreiben. Beschränken Sie die Berechtigung zum Verwalten aller Buckets auf vertrauenswürdige Benutzer und verwenden Sie die Multi-Faktor-Authentifizierung (MFA), sofern verfügbar.

- **Benutzerdefiniert:** Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.

Beispiel: Vollständigen Zugriff auf alle Buckets zulassen

In diesem Beispiel sind alle Mitglieder der Gruppe berechtigt, vollständigen Zugriff auf alle Buckets des Mandantenkontos zu erhalten, sofern nicht ausdrücklich von der Bucket-Richtlinie abgelehnt wurde.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Beispiel: Schreibgeschützter Zugriff auf alle Buckets für Gruppen zulassen

In diesem Beispiel haben alle Mitglieder der Gruppe schreibgeschützten Zugriff auf S3-Ressourcen, sofern nicht ausdrücklich von der Bucket-Richtlinie abgelehnt wird. Benutzer in dieser Gruppe können beispielsweise 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: Gruppenmitglieder haben vollen Zugriff auf ihre „folder“ in einem Bucket

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 der Privatsphäre 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}/*"
    }
  ]
}

```

Konfigurieren Sie die Sicherheit für DIE REST API

Sie sollten die für DIE REST API implementierten Sicherheitsmaßnahmen überprüfen und verstehen, wie Sie Ihr System sichern können.

So bietet StorageGRID Sicherheit für DIE REST-API

Sie sollten verstehen, wie das StorageGRID System die Sicherheit, Authentifizierung und Autorisierung für DIE REST-API implementiert.

StorageGRID setzt die folgenden Sicherheitsmaßnahmen ein.

- Die Client-Kommunikation mit dem Load Balancer-Service erfolgt über HTTPS, wenn HTTPS für den Load Balancer-Endpunkt konfiguriert ist.

Wenn Sie einen Endpunkt für den Load Balancer konfigurieren, kann HTTP optional aktiviert werden. Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

- Standardmäßig verwendet StorageGRID HTTPS für die Client-Kommunikation mit Storage-Nodes.

HTTP kann optional für diese Verbindungen aktiviert werden. Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

- Die Kommunikation zwischen StorageGRID und dem Client wird über TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Service und den Speicherknoten innerhalb des Grid wird verschlüsselt, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Clients müssen HTTP-Authentifizierungskopfzeilen an StorageGRID bereitstellen, um REST-API-Vorgänge durchzuführen.

Sicherheitszertifikate und Clientanwendungen

Clients können sich direkt mit den Storage-Nodes mit dem Load Balancer-Service auf Gateway-Nodes oder Admin-Nodes verbinden.

Clientanwendungen können in jedem Fall TLS-Verbindungen herstellen, indem sie entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID-System generiertes Zertifikat verwenden:

- Wenn Client-Anwendungen eine Verbindung zum Load Balancer-Service herstellen, verwenden sie dazu das Zertifikat, das für den spezifischen Load Balancer-Endpunkt konfiguriert wurde, der für die Verbindung verwendet wurde. Jeder Endpunkt verfügt über ein eigenes Zertifikat, entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein Zertifikat, das der Grid-Administrator bei der Konfiguration des Endpunkts in StorageGRID generiert hat.
- Wenn Client-Anwendungen eine direkte Verbindung zu einem Speicher-Node herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems für Speicher-Nodes generiert wurden (die von der Systemzertifikatsbehörde signiert werden). Oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird.

Die Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die unabhängig davon, welches Zertifikat sie zum Erstellen von TLS-Verbindungen verwenden, unterzeichnet hat.

Informationen zum Konfigurieren von Lastausgleichsendpunkten und Anweisungen zum Hinzufügen eines einzelnen benutzerdefinierten Serverzertifikats für TLS-Verbindungen direkt zu Storage-Nodes finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Zusammenfassung

Die folgende Tabelle zeigt, wie Sicherheitsprobleme in den S3 und Swift REST-APIs implementiert werden:

Sicherheitsproblem	Implementierung für REST-API
Verbindungssicherheit	TLS
Serverauthentifizierung	X.509-Serverzertifikat, das von der System-CA oder vom Administrator zur Verfügung gestellten benutzerdefinierten Serverzertifikat unterzeichnet wurde
Client-Authentifizierung	<ul style="list-style-type: none"> • S3: S3-Konto (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel) • Swift: Swift-Konto (Benutzername und Passwort)

Sicherheitsproblem	Implementierung für REST-API
Client-Autorisierung	<ul style="list-style-type: none"> • S3: Bucket-Eigentümerschaft und alle anwendbaren Richtlinien für die Zugriffssteuerung • Swift: Administratorrollenzugriff

Verwandte Informationen

["StorageGRID verwalten"](#)

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID System unterstützt eine begrenzte Anzahl von Chiffren-Suites, die Client-Anwendungen beim Einrichten einer TLS-Sitzung (Transport Layer Security) verwenden können. Um Chiffren zu konfigurieren, gehen Sie zu **CONFIGURATION > Security > Security settings** und wählen **TLS und SSH Policies** aus.

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.

Verwandte Informationen

["Mandantenkonten und -Verbindungen konfigurieren"](#)

Monitoring und Prüfung von Vorgängen

Überwachen von Objekteinspeisung und -Abruf

Die Überwachung von Objektaufnahmeraten und -Abruffraten sowie von Metriken für Objektanzahl, -Abfragen und -Verifizierung Sie können die Anzahl der erfolgreichen und fehlgeschlagenen Versuche von Client-Applikationen anzeigen, Objekte in StorageGRID zu lesen, zu schreiben und zu ändern.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).
2. Wählen Sie im Dashboard **Performance > S3-Operationen** oder **Performance > Swift-Operationen**.

In diesem Abschnitt wird die Anzahl der Client-Vorgänge zusammengefasst, die vom StorageGRID System durchgeführt werden. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.

3. Wählen Sie **KNOTEN**.
4. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Load Balancer**.

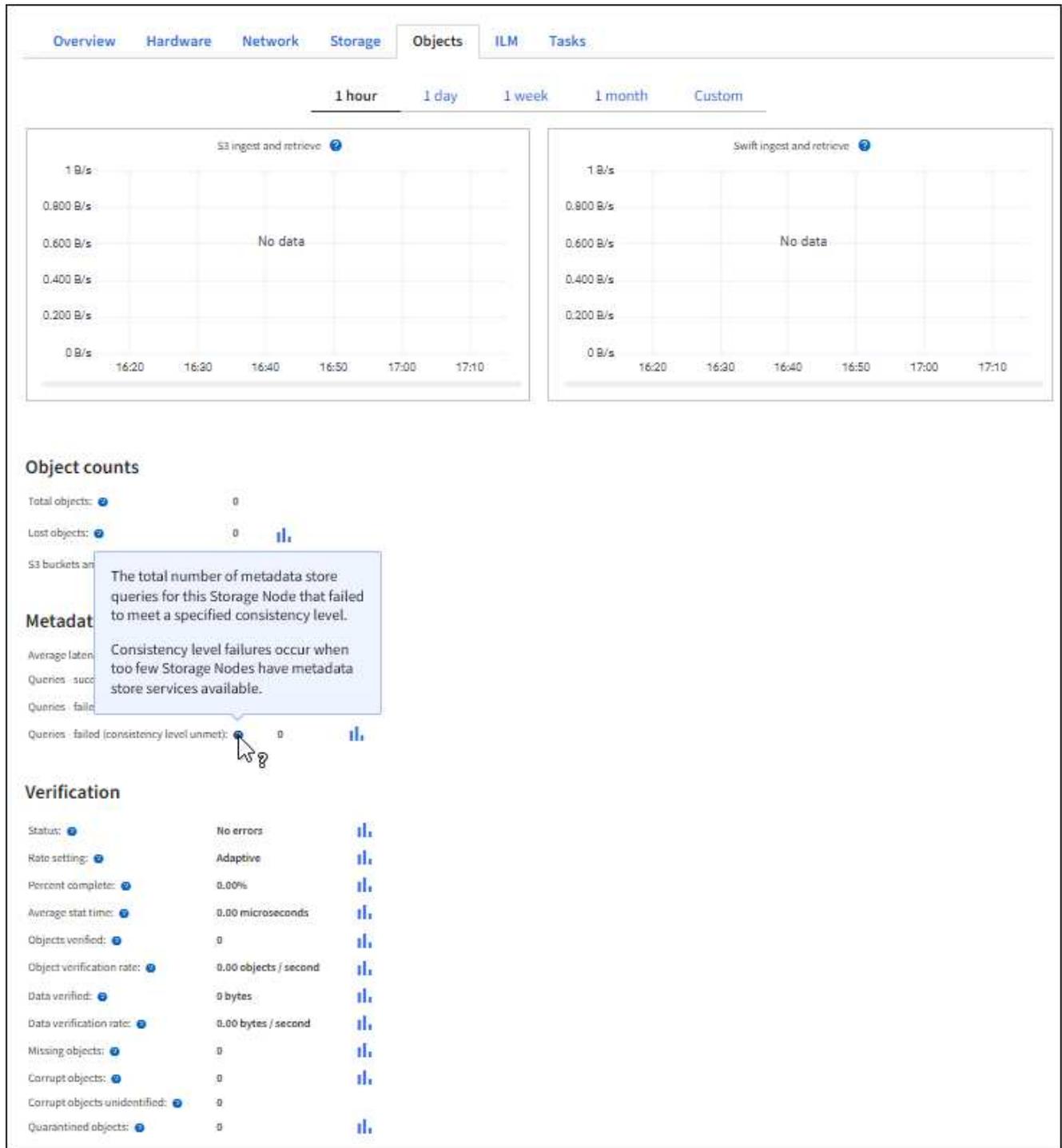
Die Diagramme zeigen Trends für den gesamten Client-Datenverkehr an Load Balancer-Endpunkte im Raster. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

5. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Objekte**.

Das Diagramm zeigt die Aufnahme- und Abrufraten Ihres gesamten StorageGRID Systems in Byte pro Sekunde sowie insgesamt Bytes. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

- Um Informationen zu einem bestimmten Speicherknoten anzuzeigen, wählen Sie den Knoten aus der Liste auf der linken Seite aus, und klicken Sie auf die Registerkarte **Objekte**.

Das Diagramm zeigt die Aufnahme- und Abrufraten des Objekts für diesen Speicherknoten. Die Registerkarte enthält außerdem Kennzahlen für Objektanzahl, Abfragen und Verifizierung. Sie können auf die Beschriftungen klicken, um die Definitionen dieser Metriken anzuzeigen.



- Wenn Sie noch mehr Details wünschen:

a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.

b. Wählen Sie **site > Übersicht > Haupt**.

Im Abschnitt API-Vorgänge werden zusammenfassende Informationen für das gesamte Raster angezeigt.

c. Wählen Sie **Storage Node > LDR > Client-Anwendung > Übersicht > Main** aus

Im Abschnitt „Vorgänge“ werden zusammenfassende Informationen für den ausgewählten Speicherknoten angezeigt.

Aufrufen und Prüfen von Prüfprotokollen

Audit-Meldungen werden von StorageGRID-Diensten generiert und in Text-Log-Dateien gespeichert. API-spezifische Audit-Meldungen in den Audit-Protokollen stellen kritische Daten zum Monitoring von Sicherheit, Betrieb und Performance bereit, die Ihnen bei der Bewertung des Systemzustands helfen können.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die `Passwords.txt` Datei:
- Sie kennen die IP-Adresse eines Admin-Knotens.

Über diese Aufgabe

Der Name der aktiven Audit-Log-Datei `audit.log`, Und es wird auf Admin-Knoten gespeichert.

Einmal am Tag wird die aktive `audit.log`-Datei 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`.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt `yyyy-mm-dd.txt.gz`, Die das ursprüngliche Datum bewahrt.

Dieses Beispiel zeigt die aktive `audit.log` Datei, Datei des Vortags (`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
```

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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält:

```
cd /var/local/audit/export
```

3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

S3-Vorgänge werden in den Audit-Protokollen protokolliert

Verschiedene Bucket-Vorgänge und Objektvorgänge werden in den StorageGRID-Prüfprotokollen verfolgt.

Bucket-Vorgänge werden in den Audit-Protokollen protokolliert

- Bucket LÖSCHEN
- Bucket-Tagging LÖSCHEN
- LÖSCHEN Sie mehrere Objekte
- Bucket ABRUFEN (Objekte auflisten)
- Get Bucket-Objektversionen
- Get Bucket-Tagging
- EIMER
- Put Bucket
- BUCKET-Compliance
- PUT Bucket-Tagging
- PUT Bucket-Versionierung

Objektvorgänge werden in den Audit-Protokollen protokolliert

- Abschließen Von Mehrteiligen Uploads
- Hochladen von Teilen (wenn die ILM-Regel das ausgeglichene oder strikte Aufnahmeverhalten verwendet)
- Hochladen von Teilen – Kopieren (wenn die ILM-Regel das ausgewogene oder strikte Aufnahmeverhalten verwendet)
- Objekt LÖSCHEN
- GET Objekt
- HEAD Objekt
- WIEDERHERSTELLUNG VON POSTOBJEKTEN
- PUT Objekt
- PUT Objekt - Kopieren

Verwandte Informationen

["Operationen auf Buckets"](#)

["Operationen für Objekte"](#)

Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen

Die Konfiguration von HTTP-Verbindungen kann sich auf die Performance des StorageGRID-Systems auswirken. Die Konfigurationen unterscheiden sich je nachdem, ob die HTTP-Verbindung aktiv oder inaktiv ist oder Sie mehrere Verbindungen gleichzeitig haben.

Sie können die Performance-Vorteile für die folgenden Arten von HTTP-Verbindungen identifizieren:

- Inaktive HTTP-Verbindungen
- Aktive HTTP-Verbindungen
- Gleichzeitige HTTP-Verbindungen

Vorteile, wenn inaktive HTTP-Verbindungen offen gehalten werden

Sie sollten HTTP-Verbindungen auch dann offen halten, wenn Client-Anwendungen inaktiv sind, um Client-Anwendungen die Ausführung folgender Transaktionen über die offene Verbindung zu ermöglichen. Basierend auf Systemmessungen und Integrationserfahrungen sollten Sie eine inaktive HTTP-Verbindung für maximal 10 Minuten offen halten. StorageGRID schließt möglicherweise automatisch eine HTTP-Verbindung, die länger als 10 Minuten im Ruhezustand bleibt.

Open- und Idle-HTTP-Verbindungen bieten folgende Vorteile:

- Niedrigere Latenz von dem Zeitpunkt, zu dem das StorageGRID System feststellt, dass eine HTTP-Transaktion durchgeführt werden muss, bis zum Zeitpunkt, zu dem das StorageGRID System die Transaktion ausführen kann

Die geringere Latenz ist der Hauptvorteil, insbesondere aufgrund der für die Einrichtung von TCP/IP- und TLS-Verbindungen benötigten Zeit.

- Erhöhte Datenübertragungsrate durch Priming des TCP/IP Slow-Start-Algorithmus mit zuvor durchgeführten Transfers
- Sofortige Benachrichtigung über mehrere Klassen von Fehlerbedingungen, die die Verbindung zwischen Client-Anwendung und StorageGRID-System unterbrechen

Die Bestimmung, wie lange eine Leerlaufverbindung offen bleiben-soll, ist ein Kompromiss zwischen den Vorteilen des langsamen Starts, der mit der bestehenden Verbindung verbunden ist, und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

Vorteile von aktiven HTTP-Verbindungen

Bei Verbindungen direkt zu Storage Nodes sollten Sie die Dauer einer aktiven HTTP-Verbindung auf maximal 10 Minuten begrenzen, selbst wenn die HTTP-Verbindung kontinuierlich Transaktionen durchführt.

Die Bestimmung der maximalen Dauer, die eine Verbindung offen halten-sollte, ist ein Kompromiss zwischen den Vorteilen der Verbindungspersistenz und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

Bei Client-Verbindungen zu Storage-Nodes bietet die Beschränkung aktiver HTTP-Verbindungen folgende Vorteile:

- Ermöglicht einen optimalen Lastausgleich über das StorageGRID System hinweg.

Im Laufe der Zeit ist eine HTTP-Verbindung möglicherweise nicht mehr optimal, da sich die Anforderungen für den Lastausgleich ändern. Das System führt den besten Lastenausgleich durch, wenn Client-Anwendungen für jede Transaktion eine separate HTTP-Verbindung herstellen, jedoch die wesentlich wertvolleren Gewinne, die mit persistenten Verbindungen verbunden sind, zunichte machen.

- Ermöglicht Client-Anwendungen, HTTP-Transaktionen an LDR-Dienste mit verfügbarem Speicherplatz zu leiten.
- Ermöglicht das Starten von Wartungsvorgängen.

Einige Wartungsverfahren beginnen erst, nachdem alle laufenden HTTP-Verbindungen abgeschlossen sind.

Bei Client-Verbindungen zum Load Balancer-Service kann eine Begrenzung der Dauer offener Verbindungen nützlich sein, um einige Wartungsverfahren zeitnah starten zu können. Wenn die Dauer der Clientverbindungen nicht begrenzt ist, kann es mehrere Minuten dauern, bis aktive Verbindungen automatisch beendet werden.

Vorteile gleichzeitiger HTTP-Verbindungen

Sie sollten mehrere TCP/IP-Verbindungen zum StorageGRID-System offen halten, um Parallelität zu ermöglichen, was die Performance steigert. Die optimale Anzahl paralleler Verbindungen hängt von einer Vielzahl von Faktoren ab.

Gleichzeitige HTTP-Verbindungen bieten die folgenden Vorteile:

- Geringere Latenz

Transaktionen können sofort gestartet werden, anstatt auf die Durchführung anderer Transaktionen zu warten.

- Erhöhter Durchsatz

Das StorageGRID System kann parallele Transaktionen durchführen und den aggregierten Transaktionsdurchsatz erhöhen.

Client-Anwendungen sollten mehrere HTTP-Verbindungen einrichten. Wenn eine Client-Anwendung eine Transaktion durchführen muss, kann sie eine vorhandene Verbindung auswählen und sofort verwenden, die derzeit keine Transaktion verarbeitet.

Die Topologie jedes StorageGRID-Systems weist einen unterschiedlichen Spitzendurchsatz für gleichzeitige Transaktionen und Verbindungen auf, bevor die Performance abnimmt. Spitzendurchsatz hängt von Faktoren wie Computing-Ressourcen, Netzwerkressourcen, Storage-Ressourcen und WAN-Links ab. Ebenfalls ausschlaggebend ist die Anzahl der Server und Services sowie die Anzahl der vom StorageGRID System unterstützten Applikationen.

StorageGRID Systeme unterstützen oft mehrere Client-Applikationen. Beachten Sie dies, wenn Sie die maximale Anzahl gleichzeitiger Verbindungen bestimmen, die von einer Client-Anwendung verwendet wird. Wenn die Client-Anwendung aus mehreren Softwareeinheiten besteht, die jeweils Verbindungen zum StorageGRID-System herstellen, sollten Sie alle Verbindungen zwischen den Einheiten hinzufügen. In den folgenden Situationen müssen Sie möglicherweise die maximale Anzahl gleichzeitiger Verbindungen anpassen:

- Die Topologie des StorageGRID Systems beeinflusst die maximale Anzahl gleichzeitiger Transaktionen und Verbindungen, die das System unterstützen kann.

- Client-Applikationen, die über ein Netzwerk mit begrenzter Bandbreite mit dem StorageGRID-System interagieren, müssen möglicherweise das Maß an Parallelität verringern, um sicherzustellen, dass einzelne Transaktionen in einem angemessenen Zeitraum durchgeführt werden.
- Wenn viele Client-Applikationen das StorageGRID System gemeinsam nutzen, muss möglicherweise der Grad an Parallelität reduziert werden, um das Überschreiten der Systemgrenzen zu vermeiden.

Trennung von HTTP-Verbindungspools für Lese- und Schreibvorgänge

Es können separate Pools von HTTP-Verbindungen für Lese- und Schreibvorgänge genutzt werden, inklusive Kontrolle darüber, wie viele aus einem Pool jeweils verwendet werden. Separate Pools von HTTP-Verbindungen ermöglichen eine bessere Kontrolle von Transaktionen und einen besseren Lastausgleich.

Client-Applikationen können Lasten erzeugen, die sich auf Abruf dominant (Lesen) oder stark speichern (Schreiben). Mit separaten Pools von HTTP-Verbindungen für Lese- und Schreibtransaktionen können Sie den Umfang der einzelnen Pools für Lese- und Schreibtransaktionen anpassen.

Swift REST API verwenden (veraltet)

Übersicht über die Swift REST API

Client-Applikationen können die OpenStack Swift API zur Schnittstelle mit dem StorageGRID System nutzen.



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

StorageGRID unterstützt die folgenden spezifischen Versionen von Swift und HTTP.

Element	Version
Swift-Spezifikation	OpenStack Swift Objekt Storage API v1 ab November 2015
HTTP	1.1 Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35). Hinweis: StorageGRID unterstützt HTTP/1.1-Pipelining nicht.

Verwandte Informationen

["OpenStack: Objekt-Storage-API"](#)

Geschichte der Unterstützung von Swift API in StorageGRID

Bei Änderungen an der Unterstützung des StorageGRID-Systems für die Swift REST-API sollten Sie auf dieser hinweisen.

Freigabe	Kommentare
11.7	Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.
11.6	Kleine redaktionelle Änderungen.
11.5	Schwache Konsistenzkontrolle entfernt. Stattdessen wird die verfügbare Konsistenzstufe verwendet.
11.4	Unterstützung für TLS 1.3 hinzugefügt. Beschreibung der Wechselbeziehung zwischen ILM und KonsistenzEinstellung hinzugefügt
11.3	Aktualisierte PUT-Objektvorgänge zur Beschreibung der Auswirkungen von ILM-Regeln, die synchrone Platzierung bei der Aufnahme verwenden (die ausgewogenen und strengen Optionen für das Aufnahmeverhalten) Eine zusätzliche Beschreibung der Client-Verbindungen, die Load Balancer-Endpunkte oder Hochverfügbarkeitsgruppen verwenden. TLS 1.1-Chiffren werden nicht mehr unterstützt.
11.2	Kleine redaktionelle Änderungen des Dokuments.
11.1	Zusätzlicher Support für die Verwendung von HTTP für Swift-Client-Verbindungen zu Grid-Nodes. Die Definitionen der Konsistenzkontrollen wurden aktualisiert.
11.0	Hinzugefügter Support für 1,000 Container für jedes Mandantenkonto.
10.3	Administrative Aktualisierungen und Korrekturen des Dokuments. Abschnitte zum Konfigurieren von benutzerdefinierten Serverzertifikaten entfernt.
10.2	Unterstützung der Swift API durch das StorageGRID System zu Beginn. Die derzeit unterstützte Version ist OpenStack Swift Object Storage API v1.

So implementiert StorageGRID Swift REST API

Eine Client-Applikation kann mithilfe von Swift REST-API-Aufrufen eine Verbindung zu Storage-Nodes und Gateway-Nodes herstellen, um Container zu erstellen und Objekte zu speichern und abzurufen. Dadurch können serviceorientierte Applikationen, die für OpenStack Swift entwickelt wurden, mit lokalem Objekt-Storage des StorageGRID Systems verbunden werden.

Swift Objekt-Management

Nach der Aufnahme von Swift Objekten im StorageGRID System werden sie von den Regeln für Information Lifecycle Management (ILM) der aktiven ILM-Richtlinie des Systems gemanagt. Der "[ILM-Regeln](#)" Und "[ILM-Richtlinie](#)" Legen Sie fest, wie StorageGRID Kopien von Objektdaten erstellt und verteilt und wie diese Kopien über einen längeren Zeitraum gemanagt werden. Eine ILM-Regel kann beispielsweise für Objekte in bestimmten Swift Containern gelten und möglicherweise angeben, dass mehrere Objektkopien für eine bestimmte Anzahl von Jahren in mehreren Datacentern gespeichert werden.

Wenden Sie sich an Ihren NetApp Professional Services Berater oder StorageGRID Administrator, wenn Sie Informationen darüber benötigen, wie sich die ILM-Regeln und -Richtlinien des Grids auf die Objekte in Ihrem Swift Mandantenkonto auswirken.

In Konflikt stehende Clientanforderungen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt und nicht darauf, wann Swift-Clients einen Vorgang starten.

Konsistenzgarantien und -Kontrollen

Standardmäßig bietet StorageGRID Lese-/Nachher-Konsistenz für neu erstellte Objekte und schließlich die Konsistenz von Objekt-Updates und HEAD-Operationen. Alle "GET" Nach erfolgreichem Abschluss "PUT" Kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen sind schließlich konsistent. Überschreibungen dauern in der Regel nur wenige Sekunden oder Minuten, können jedoch bis zu 15 Tage in Anspruch nehmen.

StorageGRID ermöglicht Ihnen außerdem die Kontrolle der Konsistenz einzelner Container. Konsistenzkontrollen sorgen für ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg, wie von Ihrer Anwendung gefordert.

Empfehlungen für die Implementierung von Swift REST API

Bei der Implementierung der Swift REST API zur Verwendung mit StorageGRID sollten Sie diese Empfehlungen beachten.

Empfehlungen für Köpfe zu nicht vorhandenen Objekten

Wenn Ihre Anwendung regelmäßig prüft, ob ein Objekt an einem Pfad vorhanden ist, wo Sie nicht erwarten, dass das Objekt tatsächlich existiert, sollten Sie die Konsistenzkontrolle „available“ verwenden. Sie sollten z. B. die Konsistenzkontrolle „Available“ verwenden, wenn Ihre Anwendung EINEN HEAD-Vorgang an einem Speicherort ausführt, bevor Sie einen PUT-Vorgang an diesen Ort ausführen.

Andernfalls werden möglicherweise 500 Fehler des internen Servers angezeigt, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.

Sie können die Konsistenzsteuerung „available“ für jeden Container mithilfe des festlegen "PUT Container-Konsistenzanforderung". Sie können die Konsistenzsteuerung „available“ für jeden Container mithilfe von anzeigen "ABRUFEN der Container-Konsistenzanforderung".

Empfehlungen für Objektnamen

Bei Containern, die in StorageGRID 11.4 oder höher erstellt wurden, ist keine Beschränkung der Objektnamen auf die Performance-Best Practices mehr erforderlich. Sie können jetzt beispielsweise Zufallswerte für die ersten vier Zeichen von Objektnamen verwenden.

Befolgen Sie bei Containern, die in Versionen vor StorageGRID 11.4 erstellt wurden, weiterhin diese Empfehlungen für Objektnamen:

- Als die ersten vier Zeichen von Objektnamen sollten keine Zufallswerte verwendet werden. Dies steht im Gegensatz zu der früheren AWS Empfehlung für Namenspräfixe. Stattdessen sollten Sie nicht-zufällige, nicht-eindeutige Präfixe verwenden, wie z. B. image.

- Wenn Sie die frühere Empfehlung von AWS befolgen, zufällige und eindeutige Zeichen in Namenspräfixen zu verwenden, sollten Sie die Objektnamen mit einem Verzeichnisnamen vorschreiben. Verwenden Sie dieses Format:

```
mycontainer/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

```
mycontainer/f8e3-image3132.jpg
```

Empfehlungen für „Range reads“

Wenn der "[Globale Option zum Komprimieren gespeicherter Objekte](#)" Ist aktiviert, sollten Swift-Client-Anwendungen die Ausführung VON GET-Objektoperationen vermeiden, die einen Bereich von Bytes angeben, die zurückgegeben werden sollen. Diese Vorgänge „range Read“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. GET-Objektvorgänge, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es sehr ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.



Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Mandantenkonten und -Verbindungen konfigurieren

Wenn StorageGRID konfiguriert wird, um Verbindungen von Client-Applikationen zu akzeptieren, müssen ein oder mehrere Mandantenkonten erstellt und die Verbindungen eingerichtet werden.

Erstellen und Konfigurieren von Swift Mandantenkonten

Bevor Swift API-Clients Objekte auf StorageGRID speichern und abrufen können, ist ein Swift-Mandantenkonto erforderlich. Jedes Mandantenkonto hat seine eigene Konto-ID, Gruppen und Benutzer sowie Container und Objekte.

Swift-Mandantenkonten werden von einem StorageGRID Grid-Administrator mit dem Grid Manager oder der Grid Management API erstellt.

Wenn "[Erstellen eines Swift-Mandantenkontos](#)" Der Grid-Administrator gibt die folgenden Informationen an:

- "[Anzeigename für die Serviceeinheit](#)" (Die Konto-ID des Mandanten wird automatisch zugewiesen und kann nicht geändert werden)
- Optional: A "[Storage-Kontingent für das Mandantenkonto](#)" — die maximale Anzahl von Gigabyte, Terabyte oder Petabyte, die für die Objekte des Mieters verfügbar sind. Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.

- Wenn "[Single Sign On \(SSO\)](#)" Wird nicht für das StorageGRID-System verwendet, unabhängig davon, ob das Mandantenkonto seine eigene Identitätsquelle verwendet oder die Identitätsquelle des Grids gemeinsam verwendet und das anfängliche Passwort für den lokalen Root-Benutzer des Mandanten verwendet.
- Wenn SSO aktiviert ist, verfügt die föderierte Gruppe über Root-Zugriffsberechtigungen zum Konfigurieren des Mandantenkontos.

Nachdem ein Swift-Mandantenkonto erstellt wurde, können Benutzer mit der Root-Zugriffsberechtigung auf den Tenant Manager zugreifen, um Aufgaben wie die folgenden durchzuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) und Erstellen lokaler Gruppen und Benutzer
- Monitoring der Storage-Auslastung



Swift-Benutzer müssen über die Root-Zugriffsberechtigung für verfügen "[Rufen Sie den Mandantenmanager auf](#)". Die Berechtigung Root-Zugriff erlaubt Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

Wie Client-Verbindungen konfiguriert werden können

Ein Grid-Administrator trifft Konfigurationsmöglichkeiten, die Einfluss darauf haben, wie Swift-Clients sich mit StorageGRID verbinden, um Daten zu speichern und abzurufen. Die spezifischen Informationen, die benötigt werden, um eine Verbindung herzustellen, hängen von der gewählten Konfiguration ab.

Client-Applikationen können Objekte speichern oder abrufen, indem sie eine Verbindung zum Load Balancer-Service auf Admin-Nodes oder Gateway-Nodes herstellen oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability) mit Admin-Nodes oder Gateway-Nodes herstellen.



Alle Applikationen, die zur Lastverteilung von StorageGRID abhängig sind, sollten sich über den Load Balancer anschließen.

- Storage-Nodes mit oder ohne externen Load Balancer

Bei der Konfiguration von StorageGRID kann ein Grid-Administrator den Grid-Manager oder die Grid-Management-API verwenden, um die folgenden Schritte auszuführen, die alle optional sind:

1. Konfigurieren von Endpunkten für den Load Balancer Service.

Sie müssen Endpunkte konfigurieren, um den Load Balancer Service verwenden zu können. Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes verteilt eingehende Netzwerkverbindungen von Client-Anwendungen auf Storage-Nodes. Beim Erstellen eines Load Balancer-Endpunkts gibt der StorageGRID-Administrator eine Portnummer an, ob der Endpunkt HTTP- oder HTTPS-Verbindungen akzeptiert, der Client-Typ (S3 oder Swift), der den Endpunkt verwendet, und das für HTTPS-Verbindungen zu verwendende Zertifikat (falls zutreffend). Swift unterstützt diese "[endpunkttypen](#)".

2. Konfigurieren Sie Nicht Vertrauenswürdige Client-Netzwerke.

Wenn ein StorageGRID-Administrator das Clientnetzwerk eines Node so konfiguriert, dass es nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen im Clientnetzwerk an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind.

3. Konfigurieren Sie Hochverfügbarkeitsgruppen.

Wenn ein Administrator eine HA-Gruppe erstellt, werden die Netzwerkschnittstellen mehrerer Admin-Nodes oder Gateway-Nodes in einer aktiv-Backup-Konfiguration platziert. Client-Verbindungen werden mithilfe der virtuellen IP-Adresse der HA-Gruppe hergestellt.

Siehe "[Konfigurationsoptionen für HA-Gruppen](#)" Finden Sie weitere Informationen.

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Client-Applikationen stellen mithilfe der IP-Adresse eines Grid-Node und der Port-Nummer eines Service auf diesem Node eine Verbindung zu StorageGRID her. Bei Konfiguration von Hochverfügbarkeitsgruppen (High Availability, HA) können Client-Applikationen eine Verbindung über die virtuelle IP-Adresse der HA-Gruppe herstellen.

Zum Erstellen von Client-Verbindungen erforderliche Informationen

Die Tabelle fasst die verschiedenen Möglichkeiten zusammen, wie Clients eine Verbindung zu StorageGRID sowie zu den für die einzelnen Verbindungstypen verwendeten IP-Adressen und Ports herstellen können.

Siehe "[IP-Adressen und Ports für Client-Verbindungen](#)" Weitere Informationen erhalten Sie von Ihrem StorageGRID-Administrator.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	• Endpunkt-Port des Load Balancer
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	• Endpunkt-Port des Load Balancer
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	• Endpunkt-Port des Load Balancer
Storage-Node	LDR	IP-Adresse des Speicherknoten	Swift-Standardports: • HTTPS: 18083 • HTTP: 18085

Beispiel

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen Swift-Client mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Nodes zu verbinden:

- `https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.6 lautet und die Portnummer eines Swift Load Balancer Endpunkts 10444 ist, kann ein Swift-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.6:10444`

Ein DNS-Name kann für die IP-Adresse konfiguriert werden, die Clients zum Herstellen der Verbindung mit StorageGRID verwenden. Wenden Sie sich an Ihren Netzwerkadministrator vor Ort.

Entscheiden Sie sich für die Verwendung von HTTPS- oder HTTP-Verbindungen

Wenn Client-Verbindungen mit einem Load Balancer-Endpunkt hergestellt werden, müssen Verbindungen über das Protokoll (HTTP oder HTTPS) hergestellt werden, das für diesen Endpunkt angegeben wurde. Um HTTP für Clientverbindungen zu Storage Nodes zu verwenden, müssen Sie die Verwendung von HTTP aktivieren.

Wenn Clientanwendungen eine Verbindung zu Storage Nodes herstellen, müssen sie standardmäßig für alle Verbindungen verschlüsseltes HTTPS verwenden. Optional können Sie weniger sichere HTTP-Verbindungen aktivieren, indem Sie den auswählen "[Aktivieren Sie HTTP für Storage Node-Verbindungen](#)" Option im Grid Manager. Eine Client-Anwendung kann beispielsweise HTTP verwenden, wenn die Verbindung zu einem Speicherknoten in einer nicht produktiven Umgebung getestet wird.



Seien Sie vorsichtig, wenn Sie HTTP für ein Produktionsraster aktivieren, da Anfragen und Antworten unverschlüsselt gesendet werden.

Wenn die Option **HTTP für Storage Node-Verbindungen aktivieren** ausgewählt ist, müssen Clients für HTTP unterschiedliche Ports verwenden als für HTTPS.

Testen Sie Ihre Verbindung in der Swift API-Konfiguration

Mit der Swift CLI können Sie die Verbindung zum StorageGRID System testen und überprüfen, ob Sie Objekte lesen und in das System schreiben können.

Bevor Sie beginnen

- Sie müssen Python-swiftclient, den Swift-Befehlszeilen-Client, heruntergeladen und installiert haben.

["SwiftStack: python-wiftclient"](#)

- Im StorageGRID System müssen Sie ein Swift Mandantenkonto haben.

Über diese Aufgabe

Wenn Sie keine Sicherheit konfiguriert haben, müssen Sie die hinzufügen `--insecure` Flag auf jeden dieser Befehle.

Schritte

1. Fragen Sie die Info-URL für Ihre StorageGRID Swift Implementierung:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Dies reicht aus, um zu testen, ob Ihre Swift-Implementierung funktionsfähig ist. Um die Kontenkonfiguration durch Speichern eines Objekts weiter zu testen, fahren Sie mit den zusätzlichen Schritten fort.

2. Legen Sie ein Objekt in den Container:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Holen Sie sich den Container, um das Objekt zu überprüfen:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Löschen Sie das Objekt:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Löschen Sie den Container:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0`
delete test_container
```

Verwandte Informationen

["Erstellen und Konfigurieren von Swift Mandantenkonten"](#)

["Konfigurieren Sie die Sicherheit für DIE REST API"](#)

Von Swift UNTERSTÜTZTE REST-API-Operationen

Das StorageGRID System unterstützt die meisten Operationen in der OpenStack Swift API. Informieren Sie sich vor der Integration von Swift REST API Clients mit StorageGRID über die Implementierungsdetails für Konto-, Container- und

Objektvorgänge.

Von StorageGRID unterstützte Vorgänge

Die folgenden Swift-API-Operationen werden unterstützt:

- ["Konto-Operationen"](#)
- ["Container-Operationen"](#)
- ["Objekt-Operationen"](#)

Gemeinsame Answerheader für alle Vorgänge

Das StorageGRID-System implementiert alle gemeinsamen Header für unterstützte Vorgänge, wie sie von der OpenStack Swift Objekt-Storage-API v1 definiert wurden.

Verwandte Informationen

["OpenStack: Objekt-Storage-API"](#)

Unterstützte Swift-API-Endpunkte

StorageGRID unterstützt die folgenden Swift-API-Endpunkte: Die Info-URL, die auth-URL und die Storage-URL.

Info-URL

Sie können die Funktionen und Einschränkungen der StorageGRID-Swift-Implementierung bestimmen, indem Sie eine GET-Anfrage an die Swift-Basis-URL mit dem /info-Pfad senden.

```
https://FQDN | Node IP:Swift Port/info/
```

In der Anfrage:

- *FQDN* Ist der vollständig qualifizierte Domain-Name.
- *Node IP* Ist die IP-Adresse für den Storage-Node oder den Gateway-Node im StorageGRID-Netzwerk.
- *Swift Port* Ist die Portnummer, die für Swift-API-Verbindungen auf dem Storage-Node oder Gateway-Node verwendet wird.

Die folgende Info-URL würde beispielsweise Informationen von einem Storage-Node mit der IP-Adresse von 10.99.106.103 anfordern und Port 18083 verwenden.

```
https://10.99.106.103:18083/info/
```

Die Antwort umfasst die Funktionen der Swift-Implementierung als JSON-Wörterbuch. Ein Client-Tool kann die JSON-Antwort analysieren, um die Funktionen der Implementierung zu bestimmen und sie als Einschränkungen für nachfolgende Storage-Vorgänge zu verwenden.

Die StorageGRID-Implementierung von Swift ermöglicht nicht authentifizierten Zugriff auf die Info-URL.

Auth-URL

Ein Client kann die Swift auth URL verwenden, um sich als Benutzer eines Mandantenkontos zu authentifizieren.

`https://FQDN | Node IP:Swift Port/auth/v1.0/`

Sie müssen die Mandanten-Konto-ID, den Benutzernamen und das Passwort als Parameter in angeben `X-Auth-User` Und `X-Auth-Key` Anforderungs-Header wie folgt:

`X-Auth-User: Tenant_Account_ID:Username`

`X-Auth-Key: Password`

In den Kopfzeilen der Anfrage:

- `Tenant_Account_ID` Ist die Account-ID, die StorageGRID beim Erstellen des Swift-Mandanten zugewiesen hat. Dies ist die gleiche Mandantenkonto-ID, die auf der Anmeldeseite des Mandanten-Managers verwendet wird.
- `Username` Ist der Name eines im Mandanten-Manager erstellten Benutzers. Dieser Benutzer muss einer Gruppe angehören, die über die Swift Administrator-Berechtigung verfügt. Der Root-Benutzer des Mandanten kann nicht für die Verwendung der Swift REST API konfiguriert werden.

Wenn Identity Federation für das Mandantenkonto aktiviert ist, geben Sie den Benutzernamen und das Passwort des föderierten Benutzers vom LDAP-Server an. Geben Sie alternativ den Domännennamen des LDAP-Benutzers an. Beispiel:

`X-Auth-User: Tenant_Account_ID:Username@Domain_Name`

- `Password` Ist das Passwort für den Mandantenbenutzer. Benutzerpasswörter werden im Mandanten-Manager erstellt und gemanagt.

Als Antwort auf eine erfolgreiche Authentifizierungsanforderung werden eine Storage-URL und ein auth-Token zurückgegeben:

`X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID`

`X-Auth-Token: token`

`X-Storage-Token: token`

Das Token ist standardmäßig für 24 Stunden ab der Erzeugung gültig.

Token werden für ein bestimmtes Mandantenkonto generiert. Ein gültiges Token für ein Konto ermächtigt einen Benutzer nicht, auf ein anderes Konto zuzugreifen.

Storage-URL

Eine Client-Applikation kann Swift-REST-API-Aufrufe ausstellen, um unterstützte Konto-, Container- und Objektvorgänge mit einem Gateway-Node oder Storage-Node durchzuführen. Storage-Anforderungen werden an die in der Authentifizierungsantwort zurückgegebene Storage-URL adressiert. Die Anforderung muss auch die Kopfzeile von `X-Auth-Token` und den Wert enthalten, der von der auth-Anforderung zurückgegeben wurde.

`https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID`

`[/container] [/object]`

`X-Auth-Token: token`

Einige Kopf für Speicherantwort, die Nutzungsstatistiken enthalten, geben möglicherweise keine genauen Zahlen für kürzlich geänderte Objekte wieder. Es kann einige Minuten dauern, bis genaue Zahlen in diesen Kopfzeilen angezeigt werden.

Die folgenden Antwortkopfzeilen für Konto- und Container-Vorgänge sind Beispiele für solche, die Nutzungsstatistiken enthalten:

- X-Account-Bytes-Used
- X-Account-Object-Count
- X-Container-Bytes-Used
- X-Container-Object-Count

Verwandte Informationen

["Mandantenkonten und -Verbindungen konfigurieren"](#)

["Konto-Operationen"](#)

["Container-Operationen"](#)

["Objekt-Operationen"](#)

Konto-Operationen

Die folgenden Swift-API-Vorgänge werden bei Accounts durchgeführt.

GET Konto

Dieser Vorgang ruft die Containerliste ab, die mit den Statistiken zur Konto- und Kontonutzung verknüpft ist.

Der folgende Parameter für die Anfrage ist erforderlich:

- Account

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden unterstützten Abfrageparameter sind optional:

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Prefix

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer „HTTP/1.1 204 No Content“-Antwort zurück, wenn das Konto gefunden wurde und keine Container oder die Containerliste leer ist; oder eine „HTTP/1.1 200 OK“-Antwort, wenn das Konto gefunden wurde und die Containerliste nicht leer ist:

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

HEAD Konto

Mit dieser Operation werden Kontoinformationen und Statistiken von einem Swift-Konto abgerufen.

Der folgende Parameter für die Anfrage ist erforderlich:

- Account

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Bei einer erfolgreichen Ausführung werden die folgenden Header mit einer „HTTP/1.1 204 No Content“-Antwort zurückgegeben:

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Verwandte Informationen

["Monitoring und Prüfung von Vorgängen"](#)

Container-Operationen

StorageGRID unterstützt maximal 1,000 Container pro Swift Konto. Die folgenden Swift-API-Vorgänge werden auf Containern durchgeführt.

Container LÖSCHEN

Durch diesen Vorgang wird ein leerer Container aus einem Swift-Konto in einem StorageGRID-System entfernt.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Kopfzeilen mit einer HTTP/1.1 204 No Content-Antwort zurück:

- Content-Length
- Content-Type
- Date
- X-Trans-Id

GET Container

Dieser Vorgang ruft die dem Container zugeordnete Objektliste sowie die Containerstatistiken und Metadaten in einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden unterstützten Abfrageparameter sind optional:

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path
- Prefix

Eine erfolgreiche Ausführung liefert die folgenden Header mit einer "HTTP/1.1 200 success" oder einer "HTTP/1.1 204 No Content"-Antwort:

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

KOPF Behälter

Dieser Vorgang ruft Containerstatistiken und Metadaten aus einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Kopfzeilen mit einer HTTP/1.1 204 No Content-Antwort zurück:

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

Legen Sie den Behälter

Durch diesen Vorgang wird ein Container für ein Konto in einem StorageGRID-System erstellt.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer "HTTP/1.1 201 created" oder "HTTP/1.1 202 Accepted" (falls der Container bereits unter diesem Konto existiert) Antwort zurück:

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

Container-Name muss im StorageGRID-Namespace eindeutig sein. Wenn der Container unter einem anderen Konto vorhanden ist, wird der folgende Header zurückgegeben: „HTTP/1.1 409-Konflikt“.

Verwandte Informationen

["Monitoring und Prüfung von Vorgängen"](#)

Objekt-Operationen

Die folgenden Swift-API-Vorgänge werden an Objekten durchgeführt. Diese Vorgänge können im nachverfolgt werden ["StorageGRID Prüfprotokoll"](#).

Delete Objekt

Durch diesen Vorgang werden der Inhalt und die Metadaten eines Objekts aus dem StorageGRID System gelöscht.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Bei einer erfolgreichen Ausführung werden die folgenden Antwortheadern mit einem zurückgegeben HTTP/1.1 204 No Content Antwort:

- Content-Length
- Content-Type
- Date
- X-Trans-Id

Bei der Verarbeitung einer LÖSCHOBJEKTANFORDERUNG versucht StorageGRID, alle Kopien des Objekts sofort von allen gespeicherten Speicherorten zu entfernen. Wenn erfolgreich, gibt StorageGRID sofort eine Antwort an den Client zurück. Wenn nicht innerhalb von 30 Sekunden alle Kopien entfernt werden können (z. B. weil ein Speicherort vorübergehend nicht verfügbar ist), stellt StorageGRID die Kopien in eine Warteschlange zur Entfernung und zeigt dann den Erfolg des Clients an.

Weitere Informationen finden Sie unter ["So werden Objekte gelöscht"](#).

GET Objekt

Dieser Vorgang ruft den Objekthalt ab und ruft die Objektmetadaten von einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden Anfragezeilen sind optional:

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Bei einer erfolgreichen Ausführung werden die folgenden Kopfzeilen mit einem zurückgegeben HTTP/1.1 200 OK Antwort:

- Accept-Ranges
- Content-Disposition, Nur wenn zurückgegeben Content-Disposition Es wurden Metadaten festgelegt
- Content-Encoding, Nur wenn zurückgegeben Content-Encoding Es wurden Metadaten festgelegt
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

HEAD Objekt

Dieser Vorgang ruft Metadaten und Eigenschaften eines aufgenommene Objekts von einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer HTTP/1.1 200 OK-Antwort zurück:

- Accept-Ranges
- Content-Disposition, Nur wenn zurückgegeben Content-Disposition Es wurden Metadaten festgelegt
- Content-Encoding, Nur wenn zurückgegeben Content-Encoding Es wurden Metadaten festgelegt
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

PUT Objekt

Durch diesen Vorgang wird ein neues Objekt mit Daten und Metadaten erstellt oder ein vorhandenes Objekt durch Daten und Metadaten in einem StorageGRID System ersetzt.

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 tib (5,497,558,138,880 Byte).



Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt und nicht darauf, wann Swift-Clients einen Vorgang starten.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden Anfragezeilen sind optional:

- Content-Disposition

- Content-Encoding

Verwenden Sie keine Schrottbearbeitungen `Content-Encoding` Wenn die ILM-Regel für ein Objekt Objekte nach der Größe filtert und synchrone Platzierung bei der Aufnahme verwendet wird (die ausgewogenen oder strengen Optionen für das Aufnahmeverhalten).

- Transfer-Encoding

Verwenden Sie keine komprimierten oder chunked `Transfer-Encoding` Wenn die ILM-Regel für ein Objekt Objekte nach der Größe filtert und synchrone Platzierung bei der Aufnahme verwendet wird (die ausgewogenen oder strengen Optionen für das Aufnahmeverhalten).

- Content-Length

Wenn eine ILM-Regel Objekte nach Größe filtert und bei der Aufnahme synchrone Platzierung verwendet, müssen Sie angeben `Content-Length`.



Wenn Sie diese Richtlinien für nicht befolgen `Content-Encoding`, `Transfer-Encoding`, und `Content-Length`, `StorageGRID` muss das Objekt speichern, bevor es die Objektgröße bestimmen kann und die ILM-Regel anwenden kann. Das heißt, `StorageGRID` muss standardmäßig vorläufige Kopien eines Objekts bei der Aufnahme erstellen. Das heißt, `StorageGRID` muss die `Dual-Commit`-Option für das Ingest-Verhalten verwenden.

Weitere Informationen zur synchronen Platzierung und zu ILM-Regeln finden Sie unter "[Datensicherungsoptionen für die Aufnahme](#)".

- Content-Type

- ETag

- X-Object-Meta-`<name\>` (Objektbezogene Metadaten)

Wenn Sie die Option **User Defined Creation Time** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie den Wert in einem benutzerdefinierten Header namens `speichern X-Object-Meta-Creation-Time`. Beispiel:

```
X-Object-Meta-Creation-Time: 1443399726
```

Dieses Feld wird seit dem 1. Januar 1970 als Sekunden ausgewertet.

- X-Storage-Class: `reduced_redundancy`

Diese Kopfzeile wirkt sich darauf aus, wie viele Objektkopien `StorageGRID` erstellt werden, wenn die ILM-Regel, die mit einem aufgenommenen Objekt übereinstimmt, ein Aufnahmeverhalten der `Dual-Commit` oder `Balance` angibt.

- **Dual Commit:** Wenn die ILM-Regel die `Dual Commit`-Option für das Aufnahmeverhalten angibt, erstellt `StorageGRID` bei Aufnahme des Objekts eine einzelne Interimskopie (`Single Commit`).
- **Ausgeglichen:** Wenn die ILM-Regel die Option `ausgeglichen` angibt, erstellt `StorageGRID` nur eine Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann.

Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung.

Der `reduced_redundancy` Kopfzeile eignet sich am besten, wenn die ILM-Regel, die dem Objekt entspricht, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `reduced_redundancy` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

Verwenden der `reduced_redundancy` Header wird unter anderen Umständen nicht empfohlen, da dies das Risiko für den Verlust von Objektdaten während der Aufnahme erhöht. Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.



Da nur eine Kopie zu einem beliebigen Zeitpunkt repliziert werden kann, sind Daten einem ständigen Verlust ausgesetzt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Beachten Sie, dass Sie angeben `reduced_redundancy` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer "HTTP/1.1 201 created"-Antwort zurück:

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Trans-Id

OPTIONEN anfordern

Die `OPTIONEN` Request überprüft die Verfügbarkeit eines einzelnen Swift Service. Die `OPTIONSANFORDERUNG` wird vom in der URL angegebenen Speicherknoten oder Gateway-Node verarbeitet.

OPTIONEN

Client-Anwendungen können zum Beispiel eine `OPTIONSANFORDERUNG` an den Swift-Port auf einem Storage Node stellen, ohne Swift-Authentifizierungsdaten bereitzustellen, um zu ermitteln, ob der Storage-Node verfügbar ist. Sie können diese Anforderung zum Monitoring verwenden oder um externen Lastausgleich zu ermöglichen, wenn ein Storage-Node ausfällt.

Bei Verwendung mit der Info-URL oder der Speicher-URL gibt die `OPTIONSMETHODE` eine Liste der unterstützten Verben für die angegebene URL zurück (z. B. KOPF, GET, OPTIONEN und PUT). Die `OPTIONSMETHODE` kann nicht mit der AuthentifizURL verwendet werden.

Der folgende Parameter für die Anfrage ist erforderlich:

- Account

Die folgenden Anfrageparameter sind optional:

- Container
- Object

Bei einer erfolgreichen Ausführung werden die folgenden Header mit einer „HTTP/1.1 204 No Content“-Antwort zurückgegeben. Für die ANFORDERUNG VON OPTIONEN an die Speicher-URL ist nicht erforderlich, dass das Ziel vorhanden ist.

- Allow (Eine Liste der unterstützten Verben für die angegebene URL, z. B. „KOPF“, „ABRUFEN“, „OPTIONEN“, Und PUT)
- Content-Length
- Content-Type
- Date
- X-Trans-Id

Verwandte Informationen

["Unterstützte Swift-API-Endpunkte"](#)

Fehlerantworten bei Swift-API-Operationen

Das Verständnis möglicher Fehlerantworten kann Ihnen bei der Fehlerbehebung helfen.

Wenn während eines Vorgangs Fehler auftreten, werden möglicherweise die folgenden HTTP-Statuscodes zurückgegeben:

Swift-Fehlername	HTTP-Status
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadaValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadaTooLarge	400 Fehlerhafte Anfrage
AccessDenied	403 Verbotene
ContainerNotEmpty, ContainerAlreadyExists	409 Konflikt
Interner Fehler	500 Fehler Des Internen Servers
InvalidRange	416 Angeforderter Bereich Nicht Zu Unterprüfbar
MethodenAlled	405 Methode Nicht Zulässig

Swift-Fehlername	HTTP-Status
MissingContentLänge	411 Länge Erforderlich
Nicht gefunden	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
ResourceNotFound	404 Nicht Gefunden
Nicht Autorisiert	401 Nicht Autorisiert
Nicht verarbeitbarEntity	422 Nicht Verarbeitbare Einheit

StorageGRID Swift REST-API-Operationen

Speziell für das StorageGRID System wurden Vorgänge zur Swift REST API hinzugefügt.

ABRUFEN der Container-Konsistenzanforderung

"[Konsistenzkontrollen](#)" Sorgen Sie für ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage-Nodes und Standorte hinweg. Die GET Container-Konsistenzanforderung ermöglicht es Ihnen, die auf einen bestimmten Container angewendete Konsistenzstufe zu bestimmen.

Anfrage

HTTP-Header anfordern	Beschreibung
X-Auth-Token	Gibt das Swift-Authentifizierungs-Token für das Konto an, das für die Anforderung verwendet werden soll.
X-ntap-sg-Konsistenz	Gibt den Anforderungstyp an, wobei <code>true</code> = GET Containerkonsistenz, und <code>false</code> = get Container.
Host	Der Hostname, auf den die Anforderung gerichtet ist.

Anforderungsbeispiel

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Antwort

HTTP-Kopfzeile für Antwort	Beschreibung
Datum	Datum und Uhrzeit der Antwort.
Verbindung	Ob die Verbindung zum Server offen oder geschlossen ist.
X-Trans-ID	Die eindeutige Transaktions-ID für die Anforderung.
Inhaltslänge	Die Länge des Reaktionskörpers.
X-ntap-sg-Konsistenz	<p>Die auf den Container angewendete Konsistenzkontrollebene. Folgende Werte werden unterstützt:</p> <p>Alle: Alle Knoten erhalten die Daten sofort oder die Anfrage schlägt fehl.</p> <p>Strong-global: Garantiert Lese-After-Write-Konsistenz für alle Kundenanfragen über alle Standorte hinweg.</p> <p>Strong-site: Garantiert Lese-After-Write Konsistenz für alle Kundenanfragen innerhalb einer Site.</p> <p>Read-after-New-write: (Standard) bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.</p> <p>Verfügbar: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.</p>

Antwortbeispiel

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

PUT Container-Konsistenzanforderung

Die PUT Container-Konsistenzanforderung ermöglicht es Ihnen, die Konsistenzstufe für die Operationen anzugeben, die auf einem Container ausgeführt werden. Standardmäßig werden neue Container mithilfe der Konsistenzstufe „read-after-New-write“ erstellt.

Anfrage

HTTP-Header anfordern	Beschreibung
X-Auth-Token	Swift Authentifizierungs-Token für das Konto zur Verwendung für die Anforderung.
X-ntap-sg-Konsistenz	<p>Die Konsistenzkontrollebene gilt für Container-Operationen. Folgende Werte werden unterstützt:</p> <p>Alle: Alle Knoten erhalten die Daten sofort oder die Anfrage schlägt fehl.</p> <p>Strong-global: Garantiert Lese-After-Write-Konsistenz für alle Kundenanfragen über alle Standorte hinweg.</p> <p>Strong-site: Garantiert Lese-After-Write Konsistenz für alle Kundenanfragen innerhalb einer Site.</p> <p>Read-after-New-write: (Standard) bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.</p> <p>Verfügbar: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.</p>
Host	Der Hostname, auf den die Anforderung gerichtet ist.

Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung zu beeinträchtigen

Beide Ihre Wahl "**Konsistenzkontrolle**" Ihre ILM-Regel wirkt sich darüber hinaus auf den Schutz von Objekten aus. Diese Einstellungen können interagieren.

Die beim Speichern eines Objekts verwendete Konsistenzsteuerung wirkt sich beispielsweise auf die anfängliche Platzierung von Objekt-Metadaten aus, während der "**Aufnahmeverhalten**" Die für die ILM-Regel ausgewählt wurde, wirkt sich auf die anfängliche Platzierung von Objektkopien aus. Da StorageGRID Zugriff auf die Metadaten eines Objekts und seine Daten benötigt, um Kundenanforderungen zu erfüllen, kann die Auswahl der passenden Sicherungsstufen für Konsistenz und Aufnahme-Verhalten eine bessere Erstsicherung und zuverlässigere Systemantworten ermöglichen.

Beispiel für die Interaktion von Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel:** Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe:** "strong-global" (Objektmetadaten werden sofort auf alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt

Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „strong-site“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten an den Remote Standort repliziert wurden, aber bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Anforderungsbeispiel

```
PUT /v1/28544923908243208806/_Swift_container_  
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29  
x-ntap-sg-consistency: strong-site  
Host: test.com
```

Antwort

HTTP-Kopfzeile für Antwort	Beschreibung
Date	Datum und Uhrzeit der Antwort.
Connection	Ob die Verbindung zum Server offen oder geschlossen ist.
X-Trans-Id	Die eindeutige Transaktions-ID für die Anforderung.
Content-Length	Die Länge des Reaktionskörpers.

Antwortbeispiel

```
HTTP/1.1 204 No Content  
Date: Sat, 29 Nov 2015 01:02:18 GMT  
Connection: CLOSE  
X-Trans-Id: 1936575373  
Content-Length: 0
```

Konfigurieren Sie die Sicherheit für DIE REST API

Sie sollten die für DIE REST API implementierten Sicherheitsmaßnahmen überprüfen

und verstehen, wie Sie Ihr System sichern können.

So bietet StorageGRID Sicherheit für DIE REST-API

Sie sollten verstehen, wie das StorageGRID System die Sicherheit, Authentifizierung und Autorisierung für DIE REST-API implementiert.

StorageGRID setzt die folgenden Sicherheitsmaßnahmen ein.

- Die Client-Kommunikation mit dem Load Balancer-Service erfolgt über HTTPS, wenn HTTPS für den Load Balancer-Endpunkt konfiguriert ist.

Wenn Sie "[Konfigurieren Sie einen Endpunkt für den Load Balancer](#)", HTTP kann optional aktiviert werden. Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen.

- Standardmäßig verwendet StorageGRID HTTPS für die Client-Kommunikation mit Storage-Nodes.

Optional "[Aktivieren Sie HTTP für diese Verbindungen](#)". Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen.

- Die Kommunikation zwischen StorageGRID und dem Client wird über TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Service und den Speicherknoten innerhalb des Grid wird verschlüsselt, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Clients müssen HTTP-Authentisierungskopfzeilen an StorageGRID bereitstellen, um REST-API-Vorgänge durchzuführen.

Sicherheitszertifikate und Clientanwendungen

Clients können sich direkt mit den Storage-Nodes mit dem Load Balancer-Service auf Gateway-Nodes oder Admin-Nodes verbinden.

Clientanwendungen können in jedem Fall TLS-Verbindungen herstellen, indem sie entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID-System generiertes Zertifikat verwenden:

- Wenn Client-Anwendungen eine Verbindung zum Load Balancer-Service herstellen, verwenden sie dazu das Zertifikat, das für den spezifischen Load Balancer-Endpunkt konfiguriert wurde, der für die Verbindung verwendet wurde. Jeder Endpunkt verfügt über ein eigenes Zertifikat, entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein Zertifikat, das der Grid-Administrator bei der Konfiguration des Endpunkts in StorageGRID generiert hat.
- Wenn Client-Anwendungen eine direkte Verbindung zu einem Speicher-Node herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems für Speicher-Nodes generiert wurden (die von der Systemzertifikatbehörde signiert werden). Oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird.

Die Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die unabhängig davon, welches Zertifikat sie zum Erstellen von TLS-Verbindungen verwenden, unterzeichnet hat.

Siehe "[Konfigurieren der Lastausgleichsendpunkte](#)" Und "[Hinzufügen eines einzelnen benutzerdefinierten Serverzertifikats](#)" Für TLS-Verbindungen direkt zu Storage-Nodes.

Zusammenfassung

Die folgende Tabelle zeigt, wie Sicherheitsprobleme in den S3 und Swift REST-APIs implementiert werden:

Sicherheitsproblem	Implementierung für REST-API
Verbindungssicherheit	TLS
Serverauthentifizierung	X.509-Serverzertifikat, das von der System-CA oder vom Administrator zur Verfügung gestellten benutzerdefinierten Serverzertifikat unterzeichnet wurde
Client-Authentifizierung	<ul style="list-style-type: none">• S3: S3-Konto (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel)• Swift: Swift-Konto (Benutzername und Passwort)
Client-Autorisierung	<ul style="list-style-type: none">• S3: Bucket-Eigentümerschaft und alle anwendbaren Richtlinien für die Zugriffssteuerung• Swift: Administratorrollenzugriff

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID System unterstützt eine begrenzte Anzahl von Chiffren-Suites, die Client-Anwendungen beim Einrichten einer TLS-Sitzung (Transport Layer Security) verwenden können. Um Chiffren zu konfigurieren, gehen Sie zu **CONFIGURATION > Security > Security settings** und wählen **TLS und SSH Policies** aus.

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.

Verwandte Informationen

["Mandantenkonten und -Verbindungen konfigurieren"](#)

Monitoring und Prüfung von Vorgängen

Kunden können Workloads und die Effizienz für Client-Vorgänge überwachen, indem sie Transaktionstrends für das gesamte Grid oder bestimmte Nodes anzeigen. Sie können Audit-Meldungen zur Überwachung von Client-Vorgängen und -Transaktionen verwenden.

Überwachen von Objekteinspeisung und -Abruf

Die Überwachung von Objektaufnahmeraten und -Abruffraten sowie von Metriken für Objektanzahl, -Abfragen und -Verifizierung Sie können die Anzahl der erfolgreichen und fehlgeschlagenen Versuche von Client-Applikationen anzeigen, Objekte in StorageGRID zu lesen, zu schreiben und zu ändern.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an "[Unterstützter Webbrowser](#)".
2. Wählen Sie im Dashboard **Performance > S3-Operationen** oder **Performance > Swift-Operationen**.

In diesem Abschnitt wird die Anzahl der Client-Vorgänge zusammengefasst, die vom StorageGRID System durchgeführt werden. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.

3. Wählen Sie **KNOTEN**.
4. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Load Balancer**.

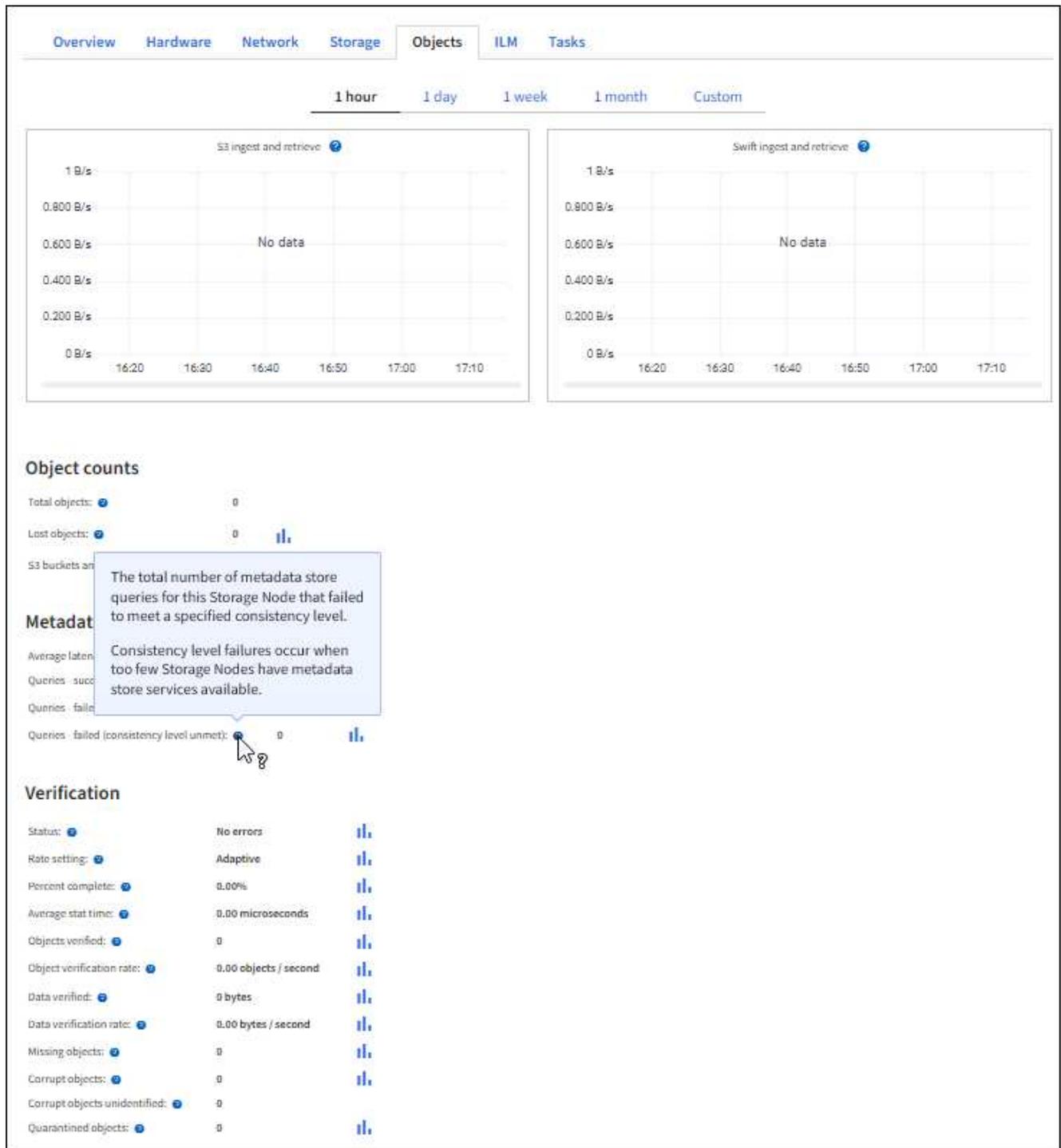
Die Diagramme zeigen Trends für den gesamten Client-Datenverkehr an Load Balancer-Endpunkte im Raster. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

5. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Objekte**.

Das Diagramm zeigt die Aufnahme- und Abrufzeiten Ihres gesamten StorageGRID Systems in Byte pro Sekunde sowie insgesamt Bytes. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

6. Um Informationen zu einem bestimmten Speicherknoten anzuzeigen, wählen Sie den Knoten aus der Liste auf der linken Seite aus, und klicken Sie auf die Registerkarte **Objekte**.

Das Diagramm zeigt die Aufnahme- und Abrufzeiten des Objekts für diesen Speicherknoten. Die Registerkarte enthält außerdem Kennzahlen für Objektanzahl, Abfragen und Verifizierung. Sie können auf die Beschriftungen klicken, um die Definitionen dieser Metriken anzuzeigen.



7. Wenn Sie noch mehr Details wünschen:

- Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- Wählen Sie **site > Übersicht > Haupt**.

Im Abschnitt API-Vorgänge werden zusammenfassende Informationen für das gesamte Raster angezeigt.

- Wählen Sie **Storage Node > LDR > Client-Anwendung > Übersicht > Main** aus

Im Abschnitt „Vorgänge“ werden zusammenfassende Informationen für den ausgewählten Speicherknoten angezeigt.

Aufrufen und Prüfen von Prüfprotokollen

Audit-Meldungen werden von StorageGRID-Diensten generiert und in Text-Log-Dateien gespeichert. API-spezifische Audit-Meldungen in den Audit-Protokollen stellen kritische Daten zum Monitoring von Sicherheit, Betrieb und Performance bereit, die Ihnen bei der Bewertung des Systemzustands helfen können.

Bevor Sie beginnen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Über diese Aufgabe

Der "[Aktive Audit-Protokolldatei](#)" ist benannt `audit.log`, und es wird auf Admin-Knoten gespeichert.

Einmal am Tag wird die aktive `audit.log`-Datei gespeichert und eine neue `audit.log`-Datei gestartet. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format `yyyy-mm-dd.txt`.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt `yyyy-mm-dd.txt.gz`, die das ursprüngliche Datum bewahrt.

Dieses Beispiel zeigt die aktive `audit.log`-Datei, die Datei des Vortags (`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
```

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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als `root` angemeldet sind, ändert sich die Eingabeaufforderung von `$` bis `#`.

2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält: `cd /var/local/audit/export`
3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt

Alle erfolgreichen Storage-LÖSCHUNGS-, GET-, HEAD-, POST- und PUT-Vorgänge werden in der nachverfolgt "[StorageGRID Prüfprotokoll](#)". Fehler werden weder protokolliert noch Info-, Auth- oder OPTIONSANFRAGEN.

Die Informationen werden für die folgenden Swift-Vorgänge nachverfolgt.

Konto-Operationen

- "GET Konto"
- "HEAD Konto"

Container-Operationen

- "Container LÖSCHEN"
- "GET Container"
- "KOPF Behälter"
- "Legen Sie den Behälter"

Objekt-Operationen

- "Delete Objekt"
- "GET Objekt"
- "HEAD Objekt"
- "PUT Objekt"

Monitoring und Fehlerbehebung

Überwachen Sie das StorageGRID-System

Überwachen eines StorageGRID-Systems: Übersicht

Befolgen Sie diese Anweisungen, um ein StorageGRID-System zu überwachen und mögliche Probleme zu bewerten.

In diesen Anweisungen wird die Verwendung von Grid Manager zum Überwachen eines StorageGRID-Systems beschrieben. Sie erfahren, welche Informationen Sie regelmäßig überwachen sollten, wie Sie Warnmeldungen und ältere Alarme verwalten, wie Sie SNMP für das Monitoring verwenden und wie Sie zusätzliche StorageGRID-Daten erhalten, einschließlich Metriken und Diagnosen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Dieser muss unbedingt vorhanden sein "[Bestimmte Zugriffsberechtigungen](#)".



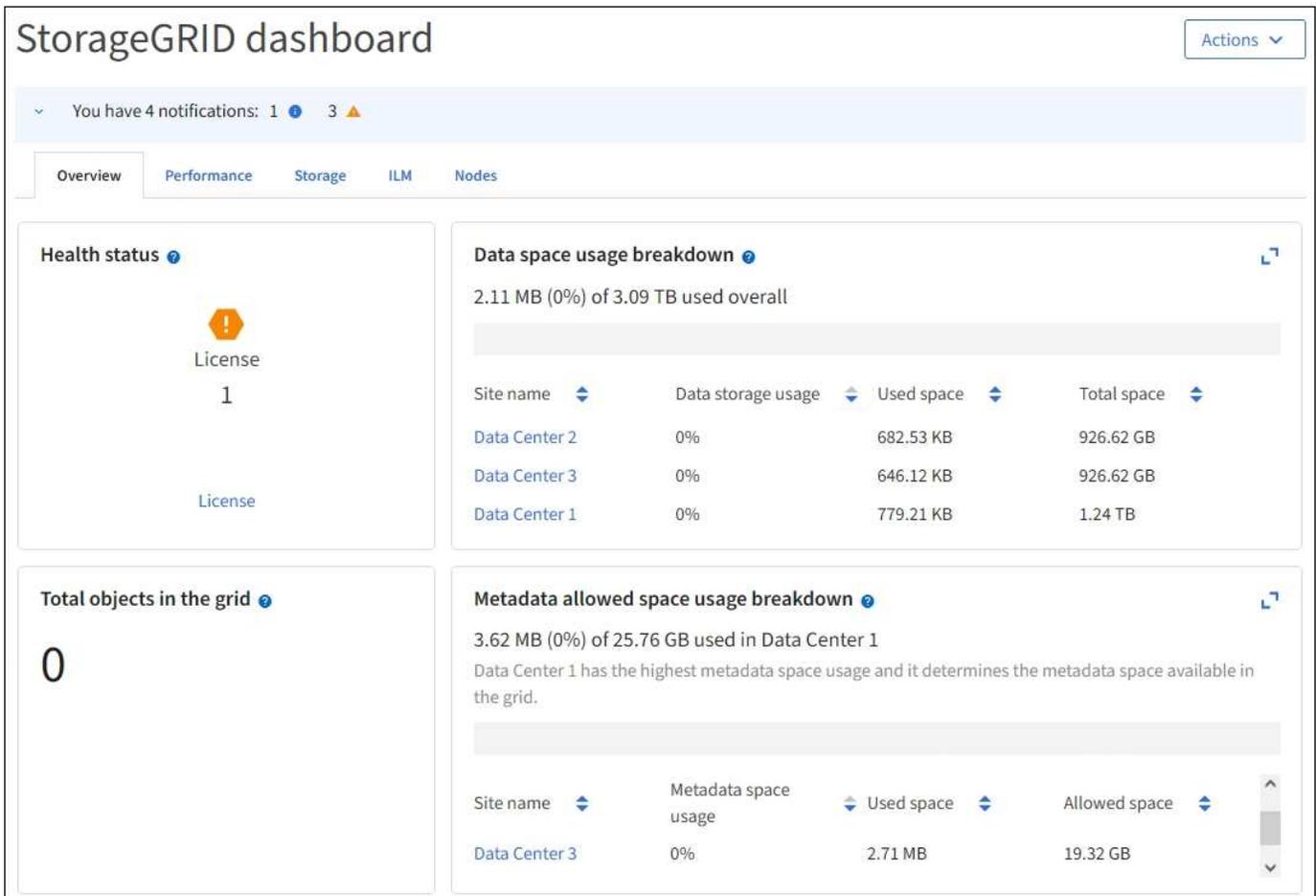
Um die Einheiten für die im Grid-Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown oben rechts im Grid-Manager aus, und wählen Sie dann **Benutzereinstellungen** aus.

Das Dashboard anzeigen und verwalten

Über das Dashboard können Sie Systemaktivitäten auf einen Blick überwachen. Sie können benutzerdefinierte Dashboards erstellen, um die Implementierung von StorageGRID zu überwachen.



Um die Einheiten für die im Grid-Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown oben rechts im Grid-Manager aus, und wählen Sie dann **Benutzereinstellungen** aus.



Dashboard anzeigen

Die Konsole besteht aus Registerkarten mit spezifischen Informationen zum StorageGRID System. Jede Registerkarte enthält Informationskategorien, die auf Karten angezeigt werden.

Sie können das vom System bereitgestellte Dashboard wie dargestellt verwenden. Außerdem können Sie benutzerdefinierte Dashboards erstellen, die nur die Registerkarten und Karten enthalten, die für die Überwachung Ihrer Implementierung von StorageGRID relevant sind.

Die vom System bereitgestellten Dashboard-Registerkarten enthalten Karten mit den folgenden Informationstypen:

Im vom System bereitgestellten Dashboard	Enthält
Überblick	Allgemeine Informationen über das Raster, wie aktive Warnmeldungen, Speicherplatznutzung und Gesamtobjekte in der Tabelle.
Leistung	Speichernutzung, im Zeitverlauf verwendeter Storage, S3- oder Swift-Vorgänge, Anfragedauer, Fehlerrate.
Storage	Nutzung von Mandantenkontingenten und logischer Speicherplatznutzung. Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten.

Im vom System bereitgestellten Dashboard	Enthält
ILM	Information Lifecycle Management-Warteschlange und Evaluierungsrate.
Knoten	CPU-, Daten- und Arbeitsspeicherverbrauch pro Node S3- oder Swift-Vorgänge pro Node. Verteilung von Knoten zu Standort.

Einige der Karten können für eine einfachere Anzeige maximiert werden. Wählen Sie das Symbol Maximieren  In der oberen rechten Ecke der Karte. Um eine maximierte Karte zu schließen, wählen Sie das Minimieren-Symbol  Oder wählen Sie **Schließen**.

Managen von Dashboards

Wenn Sie Root-Zugriff haben (siehe "[Berechtigungen für Admin-Gruppen](#)") 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 zur Erstellung benutzerdefinierter Dashboards.
- Legen Sie ein aktives Dashboard für einen Benutzer fest. Das aktive Dashboard kann entweder das vom System bereitgestellte Dashboard oder ein benutzerdefiniertes Dashboard sein.
- Legen Sie ein Standard-Dashboard fest, das allen Benutzern angezeigt wird, es sei denn, sie aktivieren ihr eigenes Dashboard.
- Bearbeiten Sie einen Dashboard-Namen.
- Bearbeiten Sie ein Dashboard, um Registerkarten und Karten hinzuzufügen oder zu entfernen. Sie können mindestens 1 und maximal 20 Registerkarten haben.
- Entfernen Sie ein Dashboard.



Wenn Sie neben dem Root-Zugriff über eine andere Berechtigung verfügen, können Sie nur ein aktives Dashboard einrichten.

Um Dashboards zu verwalten, wählen Sie **actions > Manage Dashboards**.



Dashboards konfigurieren

Um ein neues Dashboard durch Klonen des aktiven Dashboards zu erstellen, wählen Sie **actions > Clone Active Dashboard**.

Um ein vorhandenes Dashboard zu bearbeiten oder zu klonen, wählen Sie **actions > Manage Dashboards**.



Das vom System bereitgestellte Dashboard kann nicht bearbeitet oder entfernt werden.

Folgende Möglichkeiten stehen beim Konfigurieren eines Dashboards zur Verfügung:

- Registerkarten hinzufügen oder entfernen
- Benennen Sie die Registerkarten um und geben Sie neue eindeutige Namen
- Karten für jede Registerkarte hinzufügen, entfernen oder neu anordnen (ziehen)
- Wählen Sie die Größe der einzelnen Karten aus, indem Sie oben auf der Karte **S**, **M**, **L** oder **XL** auswählen

Configure dashboard

Overview Performance Storage ILM Nodes + Add tab

Tab name
Overview

Select cards

S M L

Health status

License
1
License

M L XL

Data space usage breakdown

3.50 MB (0%) of 3.09 TB used overall

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

Zeigen Sie die Seite Knoten an

Anzeigen der Seite Knoten: Übersicht

Wenn Sie detailliertere Informationen über das StorageGRID-System benötigen, als das Dashboard bietet, können Sie auf der Seite Nodes Metriken für das gesamte Grid, jeden Standort im Raster und jeden Node an einem Standort anzeigen.

In der Tabelle Nodes werden Zusammenfassungsinformationen für das gesamte Raster, jeden Standort und jeden Node aufgeführt. Wenn ein Knoten getrennt ist oder eine aktive Warnmeldung hat, wird neben dem Knotennamen ein Symbol angezeigt. Wenn der Knoten verbunden ist und keine aktiven Warnmeldungen enthält, wird kein Symbol angezeigt.



Wenn ein Knoten nicht mit dem Raster verbunden ist, z. B. während eines Upgrades oder eines getrennten Status, sind bestimmte Metriken möglicherweise nicht verfügbar oder von den Gesamtsummen des Standorts und des Rasters ausgeschlossen. Nachdem sich ein Node wieder mit dem Grid verbunden hat, warten Sie einige Minuten, bis sich die Werte stabilisieren.



Um die Einheiten für die im Grid-Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown oben rechts im Grid-Manager aus, und wählen Sie dann **Benutzereinstellungen** aus.

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 12

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
^ DC1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	6%
DC1-ARC1	Archive Node	—	—	1%
DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%

Symbole für Verbindungsstatus

Wenn ein Knoten vom Raster getrennt wird, wird neben dem Knotennamen eines der folgenden Symbole angezeigt.

Symbol	Beschreibung	Handeln erforderlich
	<p>Nicht verbunden - Unbekannt</p> <p>Aus einem unbekanntem Grund ist die Verbindung zu einem Node unterbrochen, oder Dienste auf dem Node wurden unerwartet heruntergefahren. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren.</p> <p>Die Warnung * kann nicht mit Node* kommunizieren. Andere Warnmeldungen können ebenfalls aktiv sein.</p>	<p>Erfordert sofortige Aufmerksamkeit. "Wählen Sie jede Warnmeldung aus" Und befolgen Sie die empfohlenen Maßnahmen.</p> <p>Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten.</p> <p>Hinweis: Ein Knoten kann während des verwalteten Herunterfahrens als Unbekannt erscheinen. In diesen Fällen können Sie den Status Unbekannt ignorieren.</p>

Symbol	Beschreibung	Handeln erforderlich
	<p>Nicht verbunden - Administrativ unten</p> <p>Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden.</p> <p>Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist möglicherweise auch aktiv.</p> <p>Aufgrund des zugrunde liegenden Problems sind diese Nodes oft ohne Eingriff wieder online.</p>	<p>Ermitteln Sie, ob Warnmeldungen Auswirkungen auf diesen Node haben.</p> <p>Wenn eine oder mehrere Warnungen aktiv sind, "Wählen Sie jede Warnmeldung aus" Und befolgen Sie die empfohlenen Maßnahmen.</p>

Wenn ein Knoten vom Raster getrennt wird, wird möglicherweise eine zugrunde liegende Warnmeldung angezeigt, aber nur das Symbol „not connected“ wird angezeigt. Um die aktiven Warnmeldungen für einen Node anzuzeigen, wählen Sie den Node aus.

Warnungssymbole

Wenn eine aktive Warnmeldung für einen Node vorhanden ist, wird neben dem Node-Namen eines der folgenden Symbole angezeigt:

 **Kritisch:** Es existiert eine anormale Bedingung, die den normalen Betrieb eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen.

 **Major:** Es gibt einen anormalen Zustand, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für einen kritischen Alarm nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet.

 **Minor:** Das System funktioniert normal, aber es gibt einen ungewöhnlichen Zustand, der die Fähigkeit des Systems beeinflussen könnte, wenn es weitergeht. Sie sollten kleinere Warnmeldungen überwachen und beheben, die nicht von selbst geklärt werden, um sicherzustellen, dass sie nicht zu einem schwerwiegenden Problem führen.

Zeigt Details zu einem System, Standort oder Node an

Um die in der Tabelle Knoten angezeigten Informationen zu filtern, geben Sie einen Suchstring in das Feld **Suche** ein. Sie können nach Systemnamen, Anzeigenamen oder Typ suchen (z. B. **gat** eingeben, um alle Gateway-Knoten schnell zu finden).

So zeigen Sie Informationen für das Raster, den Standort oder den Knoten an:

- Wählen Sie den Grid-Namen aus, um eine Zusammenfassung der Statistiken für Ihr gesamtes StorageGRID System anzuzeigen.
- Wählen Sie einen bestimmten Datacenter-Standort aus, um eine aggregierte Zusammenfassung der

Statistiken für alle Nodes an diesem Standort anzuzeigen.

- Wählen Sie einen bestimmten Node aus, um detaillierte Informationen zu diesem Node anzuzeigen.

Zeigen Sie die Registerkarte Übersicht an

Die Registerkarte Übersicht enthält grundlegende Informationen zu den einzelnen Knoten. Es werden zudem alle Meldungen angezeigt, die derzeit den Node betreffen.

Die Registerkarte Übersicht wird für alle Knoten angezeigt.

Node-Informationen

Im Abschnitt „Knoteninformationen“ der Registerkarte „Übersicht“ werden grundlegende Informationen zum Knoten aufgeführt.

NYC-ADM1 (Primary Admin Node) [↗](#)

Overview Hardware Network Storage Load balancer Tasks

Node information [?](#)

Display name: NYC-ADM1

System name: DC1-ADM1

Type: Primary Admin Node

ID: 3adb1aa8-9c7a-4901-8074-47054aa06ae6

Connection state: ✔ Connected

Software version: 11.7.0

IP addresses: 10.96.105.85 - eth0 (Grid Network)

[Show additional IP addresses](#) ▼

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 "[Benennen Sie Grid, Standort und Nodes um](#)" Vorgehensweise 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**: Node-Typ - Admin-Node, primärer Admin-Node, Storage-Node, Gateway-Node oder Archiv-Node.



Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

- **ID:** Die eindeutige Kennung für den Knoten, die auch als UUID bezeichnet wird.
- **Verbindungsstatus:** Einer von drei Zuständen. Das Symbol für den schwersten Zustand wird angezeigt.

- * Unbekannt* : Aus einem unbekanntem Grund ist der Knoten nicht mit dem Grid verbunden, oder ein oder mehrere Dienste sind unerwartet ausgefallen. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen, der Strom ist ausgefallen oder ein Dienst ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.



Ein Node wird möglicherweise während des verwalteten Herunterfahrens als „Unbekannt“ angezeigt. In diesen Fällen können Sie den Status Unbekannt ignorieren.

- **Administrativ nach unten** : Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist möglicherweise auch aktiv.

- * Verbunden* : Der Knoten ist mit dem Raster verbunden.

- **Verwendeter Speicher:** Nur für Speicherknoten.
 - **Objektdateien:** Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdateien, der auf dem Speicherknoten verwendet wurde.
 - **Objektmetadaten:** Der Prozentsatz des insgesamt zulässigen Speicherplatzes für Objektmetadaten, die auf dem Speicherknoten verwendet wurden.
- **Software-Version:** Die Version von StorageGRID, die auf dem Knoten installiert ist.
- **HA-Gruppen:** Nur für Admin-Node und Gateway-Nodes. 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.

Meldungen

Im Abschnitt „Warnmeldungen“ der Registerkarte „Übersicht“ sind alle aufgeführt ["Warnmeldungen, die sich derzeit auf diesen Knoten auswirken, die nicht stummgeschaltet wurden"](#). Wählen Sie den Namen der Warnmeldung aus, um weitere Details und empfohlene Aktionen anzuzeigen.

Alerts

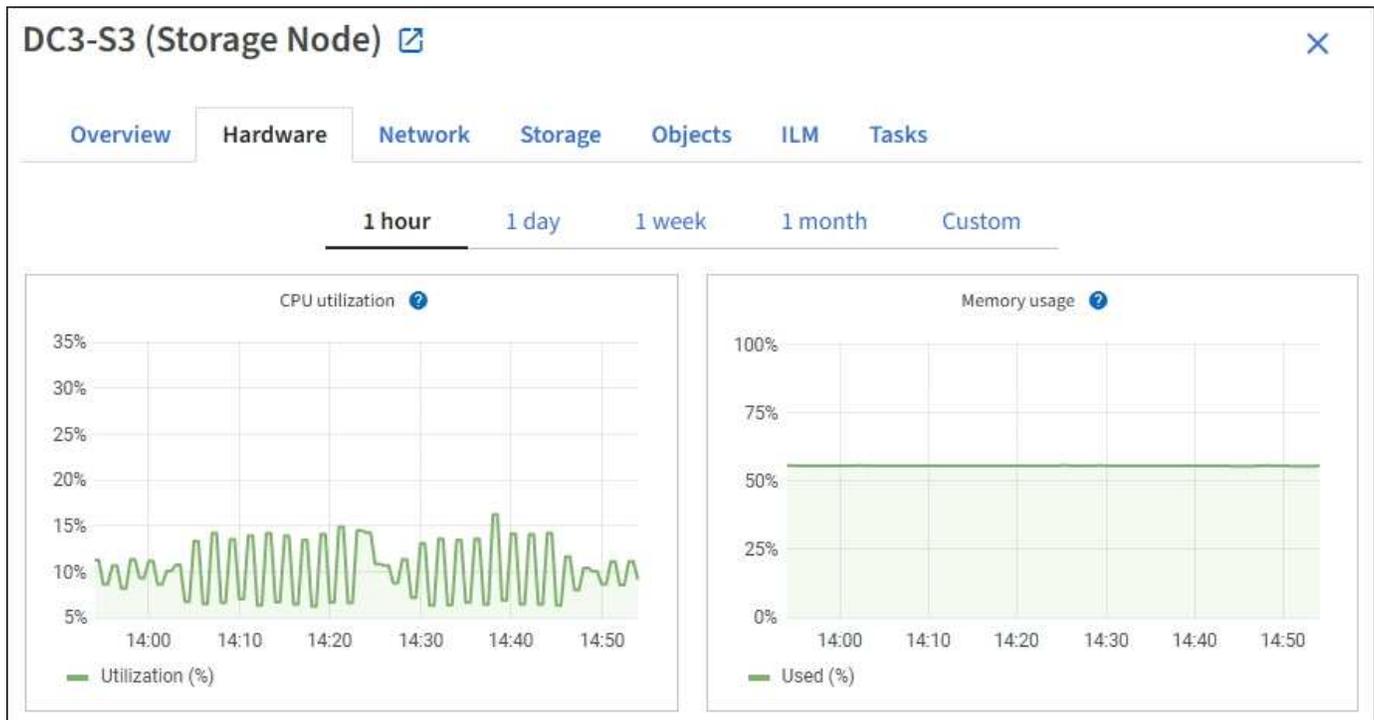
Alert name	Severity	Time triggered	Current values
Low installed node memory	Critical	11 hours ago	Total RAM size: 8.37 GB
The amount of installed memory on a node is low.			

Warnmeldungen sind auch für enthalten "Status der Node-Verbindung".

Zeigen Sie die Registerkarte Hardware an

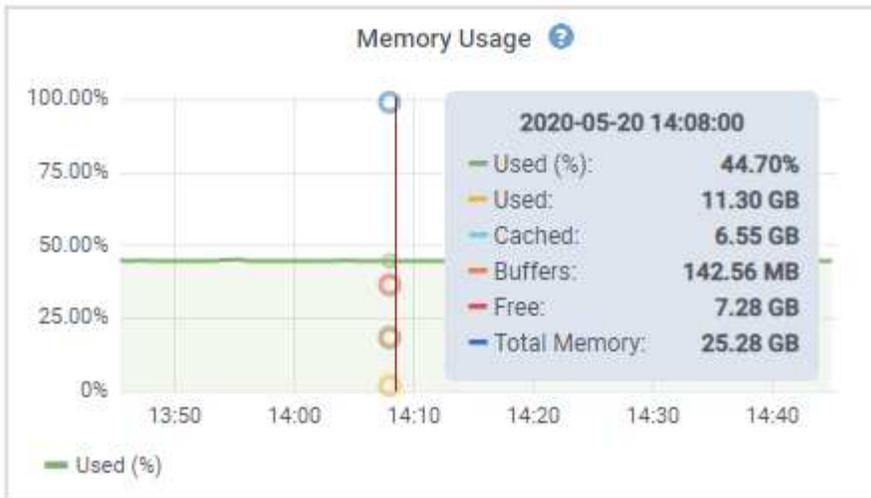
Auf der Registerkarte Hardware werden für jeden Node CPU-Auslastung und Arbeitsspeicherauslastung sowie zusätzliche Hardware-Informationen über Appliances angezeigt.

Die Registerkarte Hardware wird für alle Nodes angezeigt.



Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.

Um Details zur CPU-Auslastung und Speicherauslastung anzuzeigen, setzen Sie den Mauszeiger auf die einzelnen Diagramme.



Wenn der Knoten ein Appliance-Node ist, enthält diese Registerkarte auch einen Abschnitt mit weiteren Informationen zur Appliance-Hardware.

Zeigen Sie Informationen zu Appliance Storage Nodes an

Auf der Seite Nodes werden Informationen zum Servicestatus sowie alle Computing-, Festplattengeräte- und Netzwerkressourcen für jeden Appliance Storage Node aufgeführt. Außerdem können Sie den Arbeitsspeicher, die Storage-Hardware, die Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen und empfangen und übertragen Daten.

Schritte

1. Wählen Sie auf der Seite Knoten einen Appliance-Speicherknoten aus.
2. Wählen Sie **Übersicht**.

Im Abschnitt Node-Informationen auf der Registerkarte Übersicht werden zusammenfassende Informationen für den Node, z. B. Name, Typ, ID und Verbindungsstatus des Node, angezeigt. Die Liste der IP-Adressen umfasst den Namen der Schnittstelle für jede Adresse:

- **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das 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-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
- **mtc**: Einer der physischen 1-GbE-Ports auf der Appliance. Eine oder mehrere mtc-Schnittstellen bilden die StorageGRID Admin-Netzwerkschnittstelle (eth1). Für den Techniker im Rechenzentrum können Sie andere mtc-Schnittstellen zur temporären lokalen Konnektivität zur Verfügung stellen.

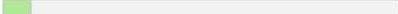
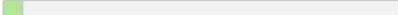
[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:
Object data  7% [?](#)
Object metadata  5% [?](#)

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

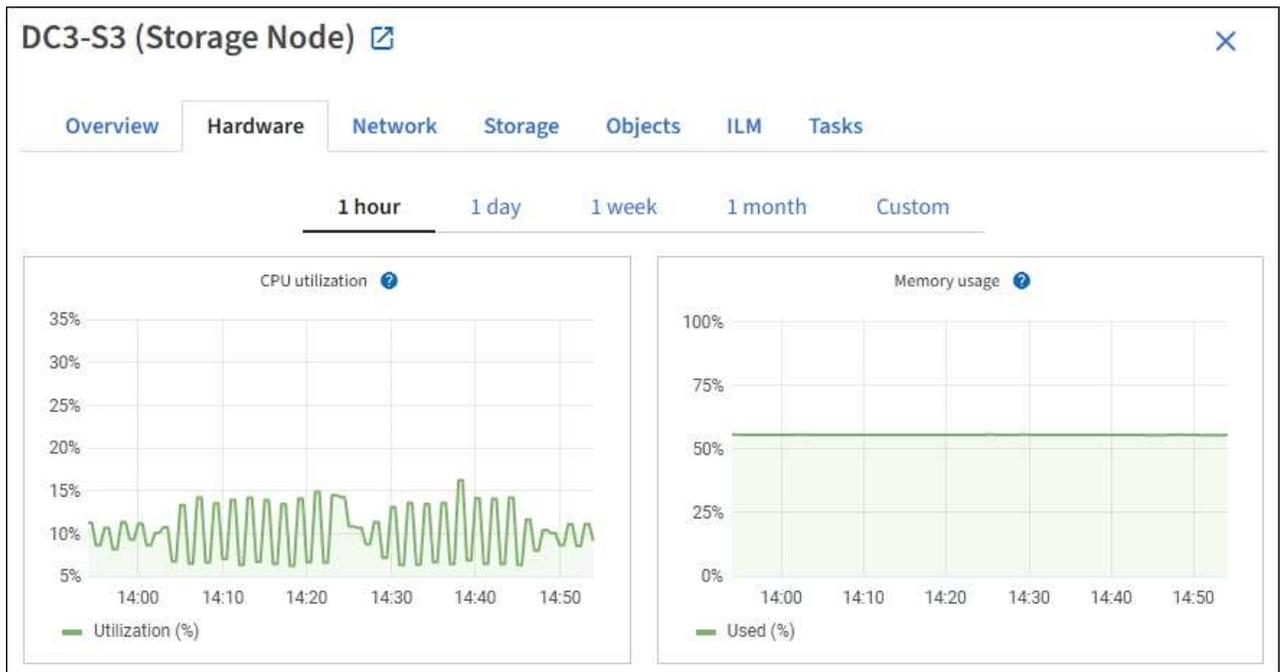
Interface ↕	IP address ↕
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ↕	Severity ? ↕	Time triggered ↕	Current values
ILM placement unachievable ↗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Im Abschnitt „Meldungen“ der Registerkarte „Übersicht“ werden alle aktiven Meldungen für den Node angezeigt.

3. Wählen Sie **Hardware**, um weitere Informationen über das Gerät anzuzeigen.
 - a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.



- b. Blättern Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen, z. B. den Modellnamen der Appliance, Controller-Namen, Seriennummern und IP-Adressen und den Status der einzelnen Komponenten.



Einige Felder, wie BMC IP- und Computing-Hardware des Rechencontrollers, werden nur für Geräte mit dieser Funktion angezeigt.

Komponenten für Storage-Shelfs und Erweiterungs-Shelfs, wenn sie Teil der Installation sind, werden in einer separaten Tabelle unter der Appliance-Tabelle aufgeführt.

StorageGRID Appliance

Appliance model: ?	SG5660	
Storage controller name: ?	StorageGRID-SGA-Lab11	
Storage controller A management IP: ?	10.224.2.192	
Storage controller WWID: ?	600a098000a4a707000000005e8ed5fd	
Storage appliance chassis serial number: ?	1142FG000135	
Storage controller firmware version: ?	08.40.60.01	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	2.00 TB	
Storage RAID mode: ?	RAID6	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller serial number: ?	SV54365519	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	

Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?
SN SV13304553	0	Nominal	N/A

Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer für diese StorageGRID Appliance wird in SANtricity OS angezeigt.
Name des Storage Controllers	Der Name dieser StorageGRID-Appliance wird in SANtricity OS angezeigt.
Storage Controller A Management-IP	IP-Adresse für Management Port 1 auf Storage Controller A Sie verwenden diese IP, um auf das SANtricity Betriebssystem zuzugreifen, um Storage-Probleme zu beheben.

Feld in der Appliance-Tabelle	Beschreibung
Storage-Controller B Management-IP	<p>IP-Adresse für Management Port 1 auf Storage Controller B Sie verwenden diese IP, um auf das SANtricity Betriebssystem zuzugreifen, um Storage-Probleme zu beheben.</p> <p>Einige Appliance-Modelle besitzen keinen Storage Controller B.</p>
WWID des Storage Controller	Die weltweite Kennung des im SANtricity OS gezeigten Storage Controllers.
Seriennummer des Storage-Appliance-Chassis	Die Seriennummer des Gehäuses des Geräts.
Version der Storage Controller-Firmware	Die Version der Firmware auf dem Storage Controller für dieses Gerät.
Storage-Hardware	<p>Der Gesamtstatus der Hardware des Storage Controllers. Wenn SANtricity System Manager einen Status als Warnung für die Storage-Hardware meldet, meldet das StorageGRID System diesen Wert ebenfalls.</p> <p>Wenn der Status „needs Aufmerksamkeit“ lautet, überprüfen Sie zuerst den Storage Controller mit SANtricity OS. Stellen Sie dann sicher, dass keine weiteren Alarme vorhanden sind, die für den Rechencontroller gelten.</p>
Anzahl der Laufwerke bei Ausfall des Storage-Controllers	Die Anzahl der Laufwerke, die nicht optimal sind.
Storage Controller A	Der Status von Speicher-Controller A.
Storage Controller B	Der Status von Storage Controller B. Einige Appliance-Modelle besitzen keinen Storage Controller B.
Netzteil A für Storage-Controller	Der Status von Netzteil A für den Storage Controller.
Netzteil B für Storage Controller	Der Status von Netzteil B für den Speicher-Controller.
Typ des Speicherdatenspeichers	Der Laufwerkstyp in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe der Speicherdatenlaufwerk	<p>Die effektive Größe eines Datenlaufwerks.</p> <p>Hinweis: Für Knoten mit Erweiterungs-Shelfs, verwenden Sie das Datenlaufwerk-Größe für jedes Shelf Stattdessen. Die effektive Laufwerksgröße kann je nach Shelf abweichen.</p>
Storage RAID-Modus	Der für die Appliance konfigurierte RAID-Modus.

Feld in der Appliance-Tabelle	Beschreibung
Storage-Konnektivität	Der Status der Storage-Konnektivität.
Gesamtnetzteil	Der Status aller Netzteile für das Gerät.
BMC IP für Computing Controller	Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie eine Verbindung zur BMC-Schnittstelle herstellen, um die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird nicht für Gerätemodelle angezeigt, die keinen BMC enthalten.
Seriennummer des Computing-Controllers	Die Seriennummer des Compute-Controllers.
Computing-Hardware	Der Status der Compute-Controller-Hardware Dieses Feld wird nicht für Appliance-Modelle angezeigt, die über keine separate Computing-Hardware und Speicher-Hardware verfügen.
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute-Controllers.
Temperatur im Computing-Controller-Chassis	Der Temperaturstatus des Compute-Controllers.

+

Spalte in der Tabelle „Storage Shelves“	Beschreibung
Seriennummer des Shelf Chassis	Die Seriennummer für das Storage Shelf-Chassis.
Shelf-ID	Die numerische Kennung für das Storage-Shelf. <ul style="list-style-type: none"> • 99: Storage Controller Shelf • 0: Erstes Erweiterungs-Shelf • 1: Zweites Erweiterungs-Shelf <p>Hinweis: Erweiterungseinschübe gelten nur für das SG6060.</p>
Der Shelf-Status	Der Gesamtstatus des Storage Shelf.
IOM-Status	Der Status der ein-/Ausgangsmodule (IOMs) in beliebigen Erweiterungs-Shelves. K. A., wenn es sich nicht um ein Erweiterungs-Shelf handelt

Spalte in der Tabelle „Storage Shelves“	Beschreibung
Netzteilstatus	Der Gesamtstatus der Netzteile für das Storage Shelf.
Status der Schublade	Der Zustand der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Lüfter im Storage Shelf.
Laufwerksschächte	Die Gesamtzahl der Laufwerksschächte im Storage-Shelf.
Datenlaufwerke	Die Anzahl der Laufwerke im Storage Shelf, die für den Datenspeicher verwendet werden.
Größe des Datenlaufwerks	Die effektive Größe eines Datenlaufwerks im Storage Shelf.
Cache-Laufwerke	Die Anzahl der Laufwerke im Storage Shelf, die als Cache verwendet werden.
Größe des Cache-Laufwerks	Die Größe des kleinsten Cache-Laufwerks im Storage-Shelf. Normalerweise haben Cache-Laufwerke dieselbe Größe.
Konfigurationsstatus	Der Konfigurationsstatus des Storage Shelf.

a. Bestätigen Sie, dass alle Status „Nominal“ sind.

Wenn der Status nicht „Nominal“ lautet, überprüfen Sie alle aktuellen Warnmeldungen. Weitere Informationen zu einigen dieser Hardware-Werte finden Sie auch mit SANtricity System Manager. Informationen zur Installation und Wartung des Geräts finden Sie in den Anweisungen.

4. Wählen Sie **Netzwerk**, um Informationen für jedes Netzwerk anzuzeigen.

Das Diagramm „Netzwerkverkehr“ 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 festzustellen, ob die 10/25-GbE-Netzwerkanschlüsse auf dem Gerät für den aktiven/Backup-Modus oder den LACP-Modus konfiguriert wurden.



Die in der Tabelle aufgeführten Werte gehen davon aus, dass alle vier Links verwendet werden.

Verbindungsmodus	Bond-Modus	Einzelne HIC-Verbindungsgeschwindigkeit (Schluck1, 2, Schluck3, Schluck4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0,eth2)
Aggregat	LACP	25	100
Fest	LACP	25	50
Fest	Aktiv/Backup	25	25
Aggregat	LACP	10	40
Fest	LACP	10	20
Fest	Aktiv/Backup	10	10

Siehe "[Netzwerkverbindungen konfigurieren](#)" Weitere Informationen zum Konfigurieren der 10/25-GbE-Ports.

b. Lesen Sie den Abschnitt Netzwerkkommunikation.

Die Tabellen „Empfangen und Senden“ zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Übertragungs-Metriken.

Network communication

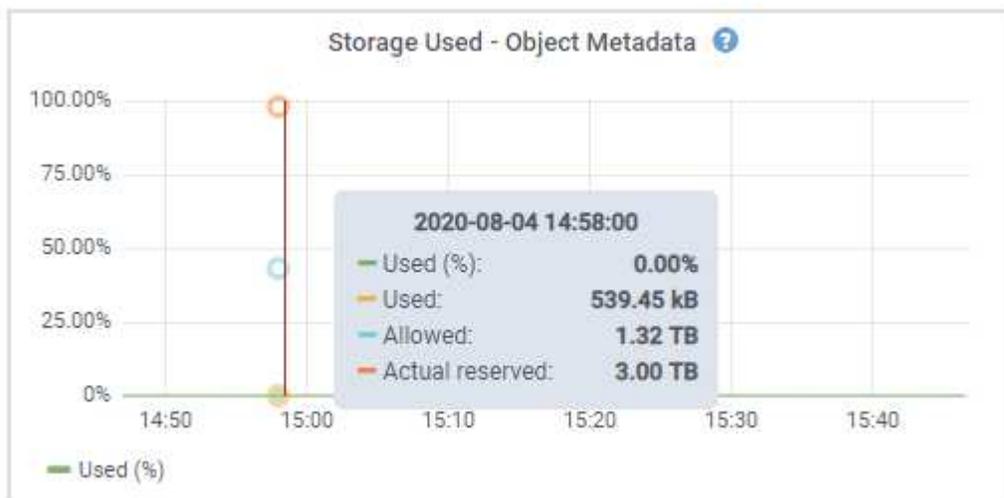
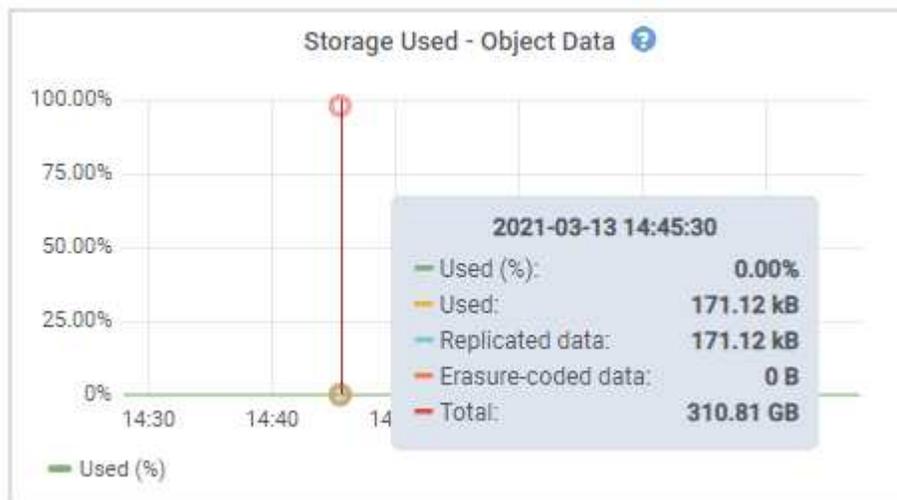
Receive

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

5. Wählen Sie **Storage** aus, um Diagramme anzuzeigen, die den Prozentsatz des im Zeitverlauf für Objektdaten und Objektmetadaten verwendeten Speichers sowie Informationen zu Festplattengeräten, Volumes und Objektspeichern anzeigen.



- a. Blättern Sie nach unten, um die verfügbaren Speichermengen für jedes Volume und jeden

Objektspeicher anzuzeigen.

Der weltweite Name jeder Festplatte stimmt mit der WWID (World-Wide Identifier) des Volumes überein, die angezeigt wird, wenn Sie die Standard-Volume-Eigenschaften in SANtricity OS (der mit dem Storage Controller der Appliance verbundenen Managementsoftware) anzeigen.

Um Ihnen bei der Auswertung von Datenträger-Lese- und Schreibstatistiken zu Volume-Mount-Punkten zu helfen, entspricht der erste Teil des Namens, der in der Spalte **Name** der Tabelle Disk Devices (d. h. *sdc*, *sdd*, *sde* usw.) in der Spalte **Gerät** der Tabelle Volumes angezeigt wird.

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

Zeigen Sie Informationen zu Appliance Admin Nodes und Gateway Nodes an

Auf der Seite Nodes werden Informationen zum Servicestatus sowie alle Computing-, Festplatten- und Netzwerkressourcen für jede Service-Appliance, die als Admin-Node oder Gateway-Node verwendet wird,

aufgeführt. Außerdem können Sie Arbeitsspeicher, Storage-Hardware, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen, Daten empfangen und übertragen.

Schritte

1. Wählen Sie auf der Seite Knoten einen Appliance Admin Node oder einen Appliance Gateway Node aus.
2. Wählen Sie **Übersicht**.

Im Abschnitt Node-Informationen auf der Registerkarte Übersicht werden zusammenfassende Informationen für den Node, z. B. Name, Typ, ID und Verbindungsstatus des Node, angezeigt. Die Liste der IP-Adressen umfasst den Namen der Schnittstelle für jede Adresse:

- **Adlb** und **adlli**: Wird angezeigt, wenn Active/Backup Bonding für die Admin Network Interface verwendet wird
- **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das 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-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
- **mtc**: Einer der physischen 1-GbE-Ports auf der Appliance. Eine oder mehrere mtc-Schnittstellen bilden die Admin-Netzwerkschnittstelle (eth1). Für den Techniker im Rechenzentrum können Sie andere mtc-Schnittstellen zur temporären lokalen Konnektivität zur Verfügung stellen.

10-224-6-199-ADM1 (Primary Admin Node)

Overview Hardware Network Storage Load balancer Tasks SANtricity System Manager

Node information

Name: 10-224-6-199-ADM1
Type: Primary Admin Node
ID: 6fdc1890-ca0a-4493-acdd-72ed317d95fb
Connection state: ✔ Connected
Software version: 11.6.0 (build 20210926.1321.6687ee3)
IP addresses: 172.16.6.199 - eth0 (Grid Network)
10.224.6.199 - eth1 (Admin Network)
47.47.7.241 - eth2 (Client Network)

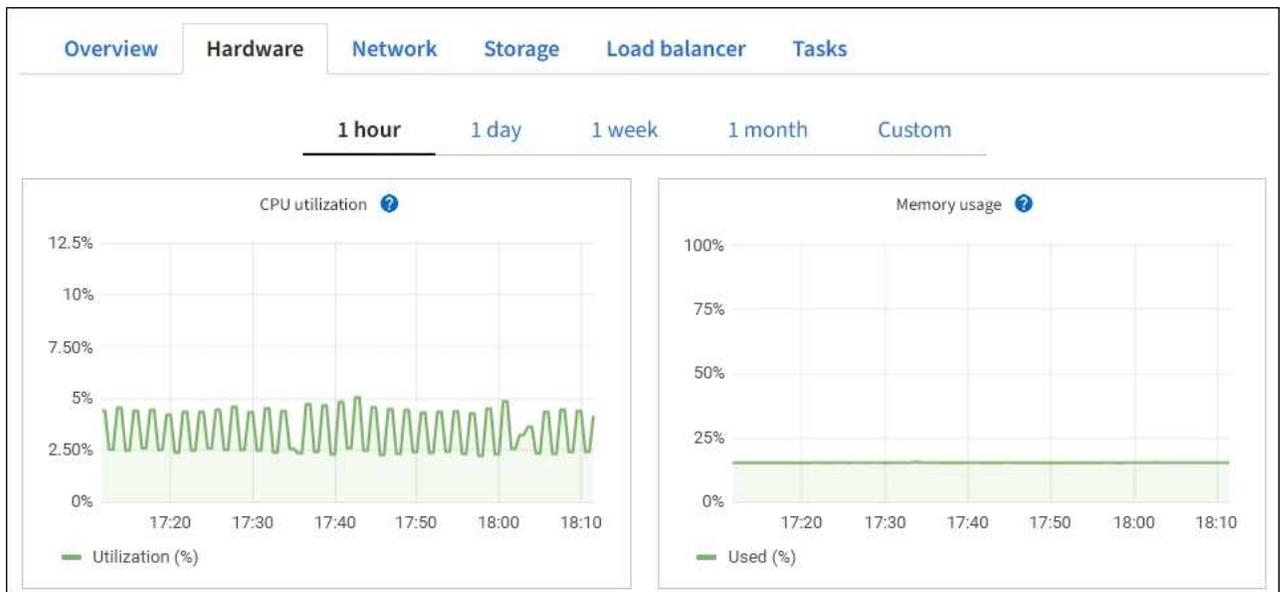
[Hide additional IP addresses](#)

Interface	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

Im Abschnitt „Meldungen“ der Registerkarte „Übersicht“ werden alle aktiven Meldungen für den Node angezeigt.

3. Wählen Sie **Hardware**, um weitere Informationen über das Gerät anzuzeigen.

- a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.



- b. Blättern Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen, z. B. den Modellnamen, die Seriennummer, die Controller-Firmware-Version und den Status jeder Komponente.

StorageGRID Appliance

Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer für diese StorageGRID Appliance.
Anzahl der Laufwerke bei Ausfall des Storage-Controllers	Die Anzahl der Laufwerke, die nicht optimal sind.
Typ des Speicherdatenspeichers	Der Laufwerkstyp in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe der Speicherdatenlaufwerk	Die effektive Größe eines Datenlaufwerks.
Storage RAID-Modus	Der RAID-Modus für die Appliance.
Gesamtnetzteil	Der Status aller Netzteile im Gerät.
BMC IP für Computing Controller	<p>Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie eine Verbindung zur BMC-Schnittstelle herstellen, um die Appliance-Hardware zu überwachen und zu diagnostizieren.</p> <p>Dieses Feld wird nicht für Gerätemodelle angezeigt, die keinen BMC enthalten.</p>

Feld in der Appliance-Tabelle	Beschreibung
Seriennummer des Computing-Controllers	Die Seriennummer des Compute-Controllers.
Computing-Hardware	Der Status der Compute-Controller-Hardware
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute-Controllers.
Temperatur im Computing-Controller-Chassis	Der Temperaturstatus des Compute-Controllers.

a. Bestätigen Sie, dass alle Status „Nominal“ sind.

Wenn der Status nicht „Nominal“ lautet, überprüfen Sie alle aktuellen Warnmeldungen.

4. Wählen Sie **Netzwerk**, um Informationen für jedes Netzwerk anzuzeigen.

Das Diagramm „Netzwerkverkehr“ 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 festzustellen, ob die vier 40/100-GbE-Netzwerkanschlüsse auf der Appliance für den aktiven/Backup-Modus oder den LACP-Modus konfiguriert wurden.



Die in der Tabelle aufgeführten Werte gehen davon aus, dass alle vier Links verwendet werden.

Verbindungsmodus	Bond-Modus	Einzelne HIC-Verbindungsgeschwindigkeit (Schluck1, 2, Schluck3, Schluck4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0, eth2)
Aggregat	LACP	100	400
Fest	LACP	100	200
Fest	Aktiv/Backup	100	100
Aggregat	LACP	40	160
Fest	LACP	40	80
Fest	Aktiv/Backup	40	40

b. Lesen Sie den Abschnitt Netzwerkkommunikation.

Die Tabellen „Empfangen und Senden“ zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Übertragungstabellen.

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

5. Wählen Sie **Storage** aus, um Informationen zu den Festplattengeräten und Volumes auf der Services Appliance anzuzeigen.

DO-REF-DC1-GW1 (Gateway Node) ✕

Overview Hardware Network **Storage** Load balancer Tasks

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 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	84.63 GB	Unknown

Verwandte Informationen

["SG100- und SG1000-Services-Appliances"](#)

Zeigen Sie die Registerkarte Netzwerk an

Auf der Registerkarte Netzwerk wird ein Diagramm angezeigt, in dem der empfangene und gesendete Netzwerkdatenverkehr über alle Netzwerkschnittstellen auf dem Node, am Standort oder im Raster angezeigt wird.

Die Registerkarte Netzwerk wird für alle Nodes, jeden Standort und das gesamte Raster angezeigt.

Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.

Für Nodes bietet die Tabelle Netzwerkschnittstellen Informationen zu den physischen Netzwerkports jedes Node. Die Netzwerkkommunikationstabelle enthält Details zu den Empfangs- und Übertragungsvorgängen jedes Knotens sowie alle vom Treiber gemeldeten Fehlerzähler.

DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

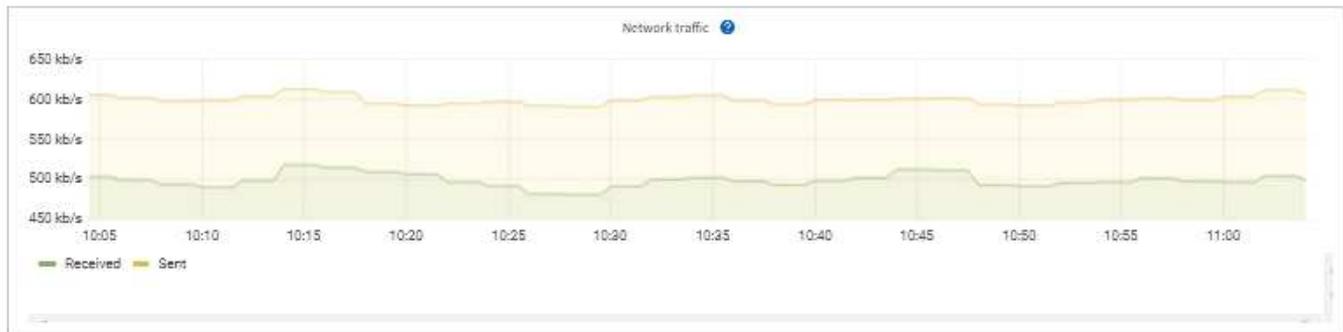
1 hour

1 day

1 week

1 month

Custom



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

Verwandte Informationen

["Überwachen Sie Netzwerkverbindungen und Performance"](#)

Öffnen Sie die Registerkarte „Speicher“

Die Registerkarte „Storage“ fasst Storage-Verfügbarkeit und andere Storage-Metriken zusammen.

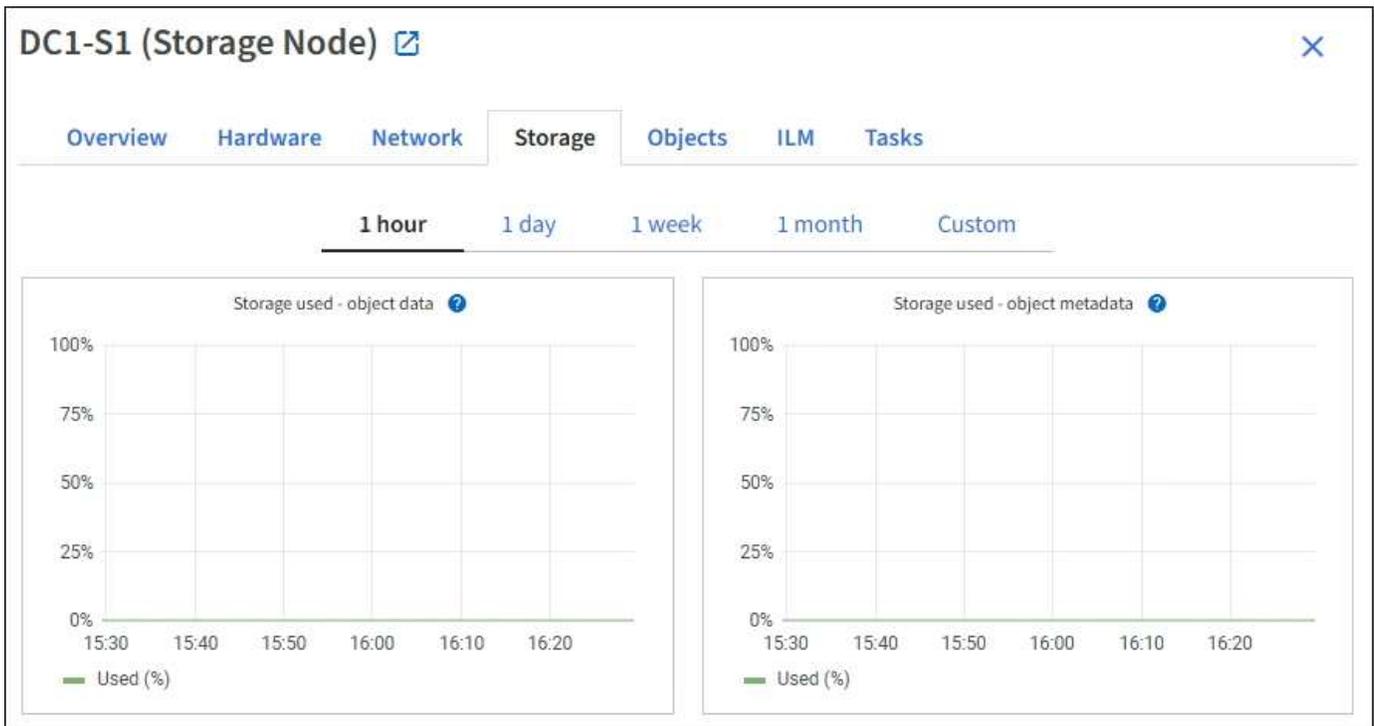
Die Registerkarte Storage wird für alle Nodes, jeden Standort und das gesamte Raster angezeigt.

Verwendete Diagramme im Storage

Für Storage-Nodes, jeden Standort und das gesamte Raster enthält die Registerkarte Storage Diagramme, die zeigen, wie viel Storage von Objektdaten und Objekt-Metadaten im Laufe der Zeit verwendet wurde.



Wenn ein Knoten nicht mit dem Raster verbunden ist, z. B. während eines Upgrades oder eines getrennten Status, sind bestimmte Metriken möglicherweise nicht verfügbar oder von den Gesamtsummen des Standorts und des Rasters ausgeschlossen. Nachdem sich ein Node wieder mit dem Grid verbunden hat, warten Sie einige Minuten, bis sich die Werte stabilisieren.



Festplattengeräte, Volumes und Objektspeichern Tabellen

Für alle Nodes enthält die Registerkarte Storage Details zu den Festplattengeräten und Volumes auf dem Node. Für Speicherknoten bietet die Objektspeichertabelle Informationen über jedes 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

Verwandte Informationen

["Monitoring der Storage-Kapazität"](#)

Verwenden Sie die Registerkarte Aufgabe, um einen Grid-Knoten neu zu starten

Auf der Registerkarte Task können Sie den ausgewählten Knoten neu starten. Die Registerkarte Task wird für alle Knoten angezeigt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).

- Sie haben die Berechtigung **Wartung** oder **Stammzugriff**.
- Sie haben die **Provisionierungs-Passphrase**.

Über diese Aufgabe

Auf der Registerkarte **Task** können Sie einen Knoten neu starten. Für Geräteknoten können Sie die Registerkarte **Aufgabe** auch verwenden, um das Gerät in den **Wartungsmodus** zu versetzen.

- Beim Neubooten eines Grid-Node auf der Registerkarte **Task** wird der Befehl zum Neubooten auf dem Ziel-Node ausgegeben. Beim Neubooten eines Node wird der Node heruntergefahren und neu gestartet. Alle Dienste werden automatisch neu gestartet.

Wenn Sie einen Storage-Node neu booten möchten, beachten Sie Folgendes:

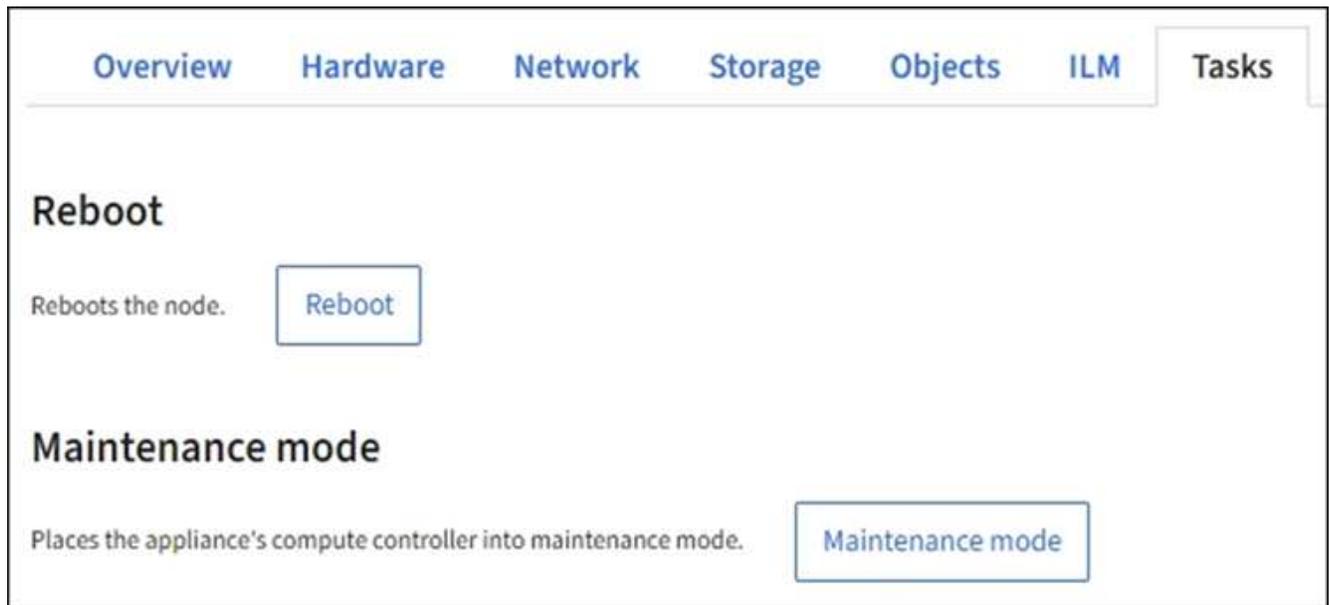
- Wenn eine ILM-Regel ein Aufnahmeverhalten von Dual-Commit angibt oder die Regel einen Ausgleich angibt und nicht sofort alle erforderlichen Kopien erstellen kann, werden neu aufgenommenen Objekte sofort von StorageGRID auf zwei Storage-Nodes am selben Standort übertragen und ILM wird später ausgewertet. Wenn Sie zwei oder mehr Storage-Nodes an einem bestimmten Standort neu starten möchten, können Sie während des Neustarts möglicherweise nicht auf diese Objekte zugreifen.
 - Um sicherzustellen, dass Sie während des Neubootens eines Storage-Node auf alle Objekte zugreifen können, beenden Sie die Verarbeitung von Objekten an einem Standort etwa eine Stunde lang, bevor Sie den Node neu booten.
- Möglicherweise müssen Sie eine StorageGRID Appliance in den **Wartungsmodus** versetzen, um bestimmte Verfahren durchzuführen, z. B. das Ändern der Link-Konfiguration oder den Austausch eines Storage Controllers. Anweisungen hierzu finden Sie unter "[Stellen Sie das Gerät in den Wartungsmodus](#)".



In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den **Wartungsmodus** versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.

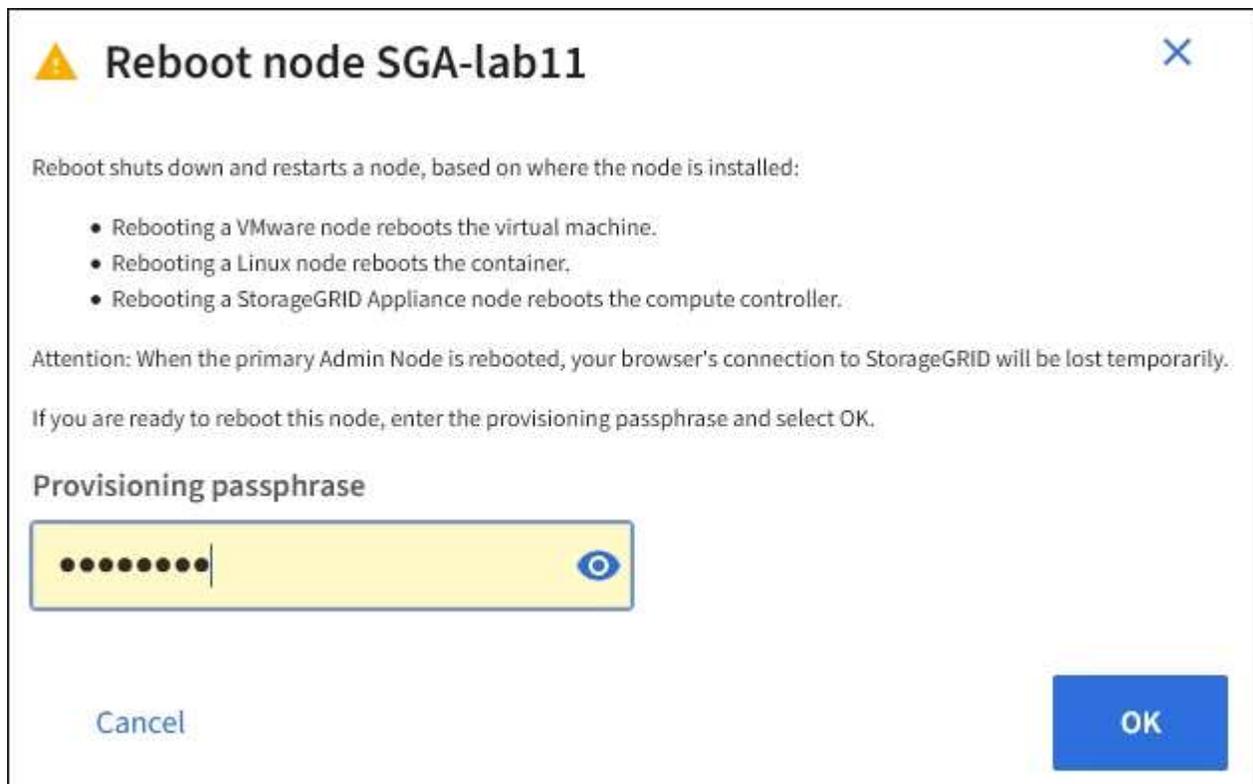
Schritte

1. Wählen Sie **KNOTEN**.
2. Wählen Sie den Grid-Node aus, den Sie neu booten möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.



4. Wählen Sie **Neustart**.

Ein Bestätigungsdialogfeld wird angezeigt.



Wenn Sie den primären Admin-Knoten neu starten, wird im Bestätigungsdialogfeld darauf hingewiesen, dass die Verbindung Ihres Browsers zum Grid Manager vorübergehend verloren geht, wenn Dienste beendet werden.

5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

6. Warten Sie, bis der Node neu gebootet wird.

Es kann einige Zeit dauern, bis Dienste heruntergefahren werden.

Wenn der Knoten neu gestartet wird, wird das graue Symbol (Administrativ Down) auf der linken Seite der Seite **Nodes** angezeigt. Wenn alle Dienste wieder gestartet wurden und der Knoten erfolgreich mit dem Raster verbunden ist, sollte die Seite **Nodes** einen normalen Status anzeigen (keine Symbole links neben dem Knotennamen), was darauf hinweist, dass keine Alarme aktiv sind und der Knoten mit dem Raster verbunden ist.

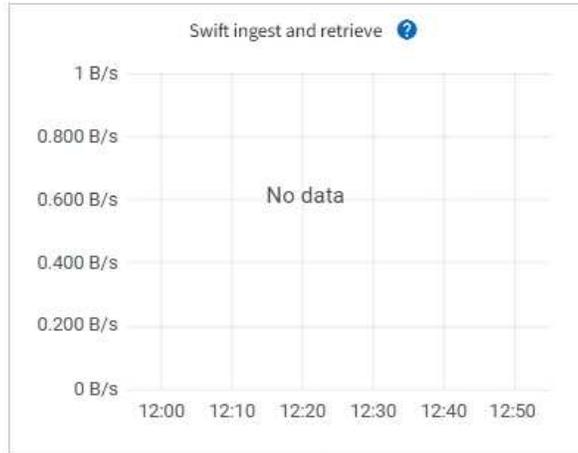
Zeigen Sie die Registerkarte Objekte an

Die Registerkarte Objekte enthält Informationen zu "S3" Und "Swift" Einspielraten und Abrufen.

Für jeden Storage-Node, jeden Standort und das gesamte Raster wird die Registerkarte Objekte angezeigt. Für Storage-Nodes bietet die Registerkarte Objekte außerdem die Anzahl der Objekte und Informationen zu Metadatenabfragen und zur Hintergrundüberprüfung.

- Overview
- Hardware
- Network
- Storage
- Objects
- ILM
- Tasks

- 1 hour
- 1 day
- 1 week
- 1 month
- Custom



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	

Zeigen Sie die Registerkarte ILM an

Die Registerkarte ILM enthält Informationen zu ILM-Vorgängen (Information Lifecycle Management).

Die ILM-Registerkarte wird für jeden Storage-Node, jeden Standort und das gesamte Grid angezeigt. Auf der Registerkarte ILM wird für jeden Standort und das Grid ein Diagramm der ILM-Warteschlange im Laufe der Zeit angezeigt. In dieser Registerkarte wird auch die voraussichtliche Zeit zum Abschluss eines vollständigen ILM-Scans aller Objekte bereitgestellt.

Für Storage-Nodes bietet die Registerkarte ILM Details zur ILM-Bewertung und zur Hintergrundüberprüfung codierten Objekten.

DC2-S1 (Storage Node) [↗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) **ILM** [Tasks](#)

Evaluation

Awaiting - all: ?	0 objects	
Awaiting - client: ?	0 objects	
Evaluation rate: ?	0.00 objects / second	
Scan rate: ?	0.00 objects / second	

Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-09-09 17:36:44 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Verwandte Informationen

["Überwachung des Information Lifecycle Management"](#)

["StorageGRID verwalten"](#)

Zeigen Sie die Registerkarte Load Balancer an

Die Registerkarte Load Balancer enthält Performance- und Diagnosediagramme zum Betrieb des Load Balancer Service.

Die Registerkarte Load Balancer wird für Admin-Nodes und Gateway-Nodes, jeden Standort und das gesamte Raster angezeigt. Die Registerkarte Load Balancer bietet für jeden Standort eine zusammengefasste Zusammenfassung der Statistiken für alle Nodes an diesem Standort. Die Registerkarte Load Balancer bietet für das gesamte Raster eine zusammengefasste Zusammenfassung der Statistiken für alle Standorte.

Wenn kein I/O durch den Lastausgleichsdienst ausgeführt wird oder kein Load Balancer konfiguriert ist, werden in den Diagrammen „Keine Daten“ angezeigt.



Datenverkehr anfordern

Dieses Diagramm zeigt einen Mittelwert, der durch 3 Minuten bewegt wird und den Durchsatz der Daten zwischen den Endpunkten des Load Balancer und den Clients, die die Anforderungen erstellen, in Bits pro Sekunde übertragen wird.



Dieser Wert wird beim Abschluss jeder Anfrage aktualisiert. Aus diesem Grund kann sich der Wert von dem Echtzeitdurchsatz bei niedrigen Anfrageraten oder bei sehr langen Anforderungen unterscheiden. Auf der Registerkarte „Netzwerk“ finden Sie eine realistischere Ansicht des aktuellen Netzwerkverhaltens.

Eingehende Anfragerate

Dieses Diagramm zeigt einen 3-minütigen, sich bewegenden Durchschnitt der Anzahl neuer Anfragen pro Sekunde, aufgeschlüsselt nach Anfragetyp (GET, PUT, HEAD und DELETE). Dieser Wert wird aktualisiert, wenn die Kopfzeilen einer neuen Anfrage validiert wurden.

Durchschnittliche Anfragedauer (fehlerfrei)

Dieses Diagramm zeigt einen 3-minütigen versch. Durchschnitt der Anfragedauer und ist nach Anforderungstyp aufgeschlüsselt (GET, PUT, HEAD und DELETE). Jede Anforderungsdauer beginnt, wenn eine Anforderungs-Kopfzeile vom Lastbalancer-Dienst analysiert wird und endet, wenn der vollständige Antwortkörper an den Client zurückgesendet wird.

Fehlerantwortrate

Dieses Diagramm zeigt einen Mittelwert, der durch 3 Minuten verschoben wird und der Anzahl der Fehlerantworten, die an Clients pro Sekunde zurückgegeben werden, aufgeschlüsselt nach dem Fehlercode.

Verwandte Informationen

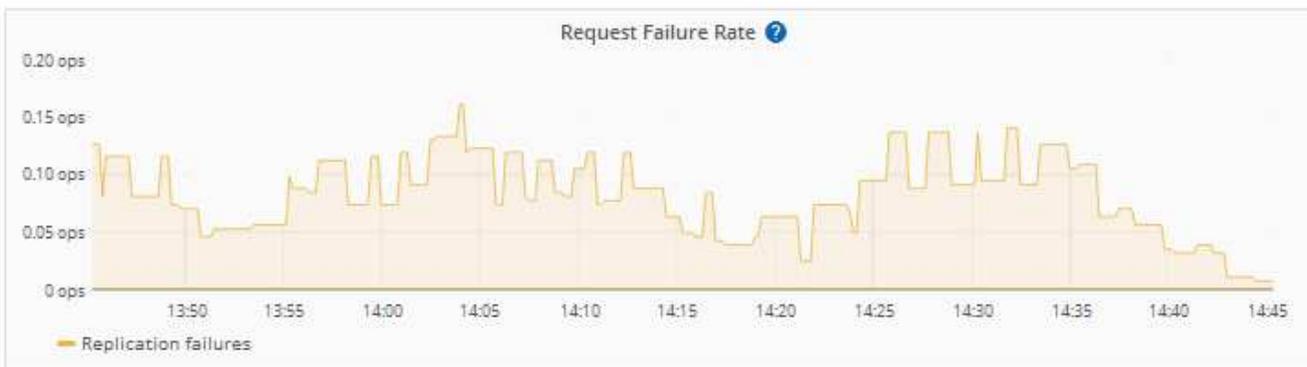
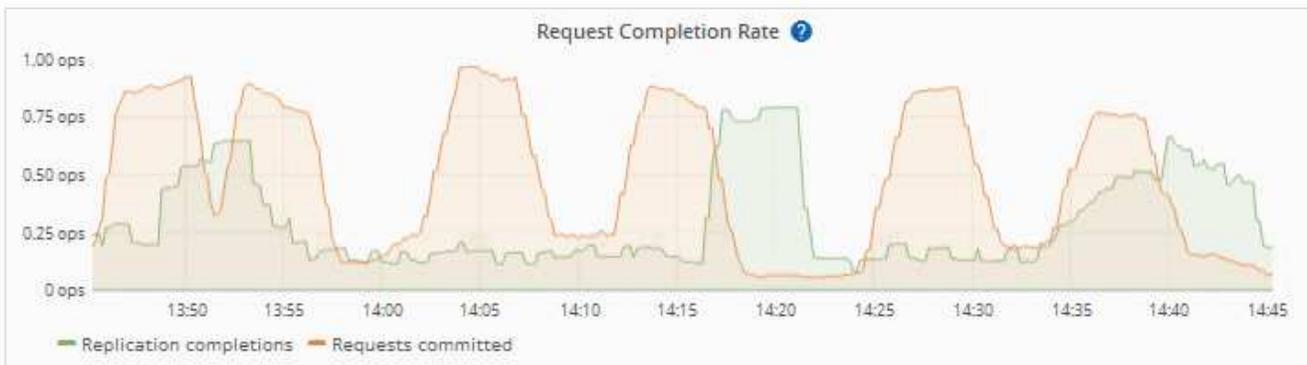
["Monitoring von Lastverteilungsvorgängen"](#)

["StorageGRID verwalten"](#)

Zeigen Sie die Registerkarte Plattformdienste an

Die Registerkarte Plattformdienste enthält Informationen über alle S3-Plattform-Servicevorgänge an einem Standort.

Die Registerkarte Plattformdienste wird für jede Site angezeigt. Diese Registerkarte enthält Informationen zu S3-Plattformdiensten wie CloudMirror-Replizierung und den Suchintegrationsdienst. In Diagrammen auf dieser Registerkarte werden Metriken angezeigt, z. B. die Anzahl der ausstehenden Anfragen, die Abschlussrate der Anfrage und die Rate bei Ausfällen von Anfragen.



Weitere Informationen zu S3-Platformservices, einschließlich Details zur Fehlerbehebung, finden Sie im ["Anweisungen für die Administration von StorageGRID"](#).

Zeigen Sie die Registerkarte SANtricity System Manager an

Über die Registerkarte SANtricity System Manager auf der Seite Knoten im Grid-Manager können Sie auf SANtricity System Manager zugreifen, ohne den Managementport der Storage Appliance konfigurieren oder anschließen zu müssen. Sie können diese Registerkarte verwenden, um Informationen zur Hardware-Diagnose und -Umgebung sowie Probleme im Zusammenhang mit den Laufwerken zu überprüfen.



Die Registerkarte SANtricity System Manager wird nur für Nodes von Storage-Appliances angezeigt, die die E-Series Hardware verwenden.

Mit SANtricity System Manager sind folgende Vorgänge möglich:

- Anzeige von Performance-Daten wie Performance auf Storage-Array-Ebene, I/O-Latenz, CPU-Auslastung des Storage-Controllers und Durchsatz
- Überprüfen Sie den Status der Hardwarekomponenten.
- Durchführung von Support-Funktionen, einschließlich Anzeige von Diagnosedaten und Konfiguration der E-Series AutoSupport



Informationen zur Konfiguration eines Proxys für E-Series AutoSupport mit SANtricity System Manager finden Sie unter "[Senden Sie AutoSupport Nachrichten aus der E-Series über StorageGRID](#)".

Um über den Grid-Manager auf den SANtricity System Manager zuzugreifen, müssen Sie über eine Administratorberechtigung oder eine Root-Berechtigung für die Storage-Appliance verfügen.



Sie müssen über SANtricity-Firmware 8.70 oder höher verfügen, um mit dem Grid Manager auf SANtricity System Manager zuzugreifen.



Der Zugriff auf den SANtricity System Manager über den Grid Manager erlaubt in der Regel nur die Überwachung der Appliance-Hardware und die Konfiguration der E-Series AutoSupport. Viele Funktionen und Vorgänge in SANtricity System Manager, beispielsweise ein Firmware-Upgrade, gelten nicht für die Überwachung Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie stets die Hardware-Wartungsanweisungen für Ihr Gerät.

Die Registerkarte zeigt die Startseite von SANtricity System Manager an.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open [SANtricity System Manager](#) in a new browser tab.

The screenshot displays the SANtricity System Manager interface for a StorageGRID-NetApp SGA-108. The top navigation bar includes 'Overview', 'Hardware', 'Network', 'Storage', 'Objects', 'ILM', 'Events', 'Tasks', and 'SANtricity System Manager'. The main content area shows a green checkmark indicating 'Your storage array is optimal.' Below this is a 'STORAGE ARRAY LEVEL PERFORMANCE' section featuring an IOPS graph. The graph shows IOPS (Reads) and IOPS (Writes) over time, with a 'Live updating' indicator. Below the graph are buttons for 'IOPS', 'MiB/s', and 'CPU'. At the bottom, there are sections for 'CAPACITY' (showing 0% free) and 'STORAGE HIERARCHY' (showing 1 Shelf, 18 Volumes, and 1 Host).



Über den Link SANtricity System Manager können Sie den SANtricity System Manager in einem neuen Browser-Fenster öffnen und so die Ansicht erleichtern.

Wenn Sie Details zur Performance und Kapazitätsauslastung auf Speicher-Array-Ebene anzeigen möchten,

setzen Sie den Mauszeiger auf die einzelnen Diagramme.

Weitere Informationen zum Anzeigen der Informationen, auf die über die Registerkarte SANtricity System Manager zugegriffen werden kann, finden Sie unter "[NetApp E-Series und SANtricity Dokumentation](#)".

Verwandte Informationen

- "[Warten Sie die SG6000-Appliance](#)"
- "[SG5700 Appliance warten](#)"

Informationen, die Sie regelmäßig überwachen sollten

Was und wann zu überwachen

Das StorageGRID System funktioniert auch dann weiter, wenn Fehler auftreten oder Teile des Grids nicht verfügbar sind, sollten Sie potenzielle Probleme überwachen und beheben, bevor sie die Effizienz oder Verfügbarkeit des Grids beeinträchtigen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben spezifische Zugriffsberechtigungen.

Über Überwachungsaufgaben

Ein überlastetes System generiert große Datenmengen. Die folgende Liste enthält Anleitungen zu den wichtigsten Informationen, die fortlaufend überwacht werden müssen.

Was überwacht werden soll	Frequenz
" Systemstatus "	Täglich
Tarif " Objekt- und Metadatenkapazität des Storage-Node " Wird verbraucht	Wöchentlich
" Information Lifecycle Management-Operationen "	Wöchentlich
" Netzwerk- und Systemressourcen "	Wöchentlich
" Mandantenaktivität "	Wöchentlich
" Lastverteilung "	Nach der Erstkonfiguration und nach Konfigurationsänderungen
" Netzverbundverbindungen "	Wöchentlich
" Verfügbarkeit von Software-Hotfixes und Software-Upgrades "	Monatlich
" Kapazität des externen Archiv-Storage-Systems "	Wöchentlich

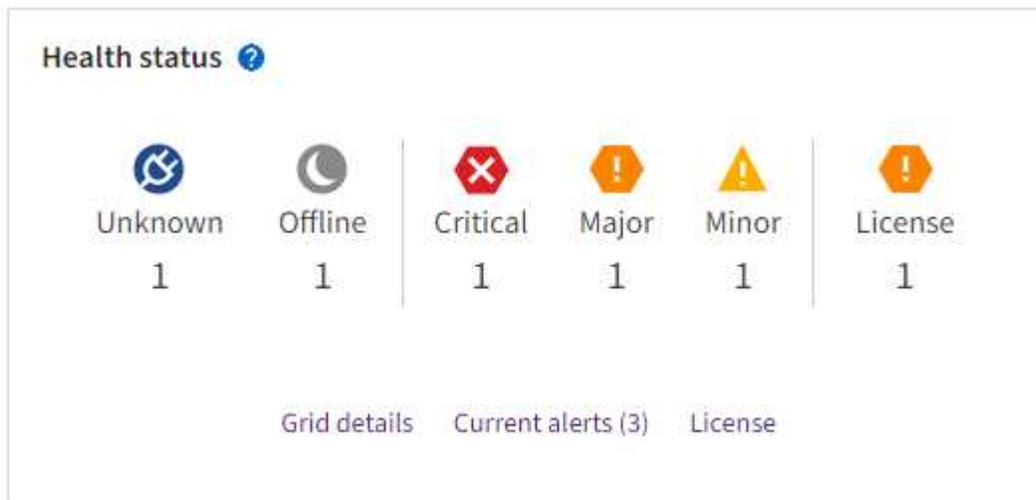
Systemzustand überwachen

Überwachen Sie täglich den Gesamtzustand Ihres StorageGRID Systems.

Über diese Aufgabe

Das StorageGRID System kann weiter betrieben werden, wenn Teile des Grids nicht verfügbar sind. Potenzielle Probleme, die durch Warnungen oder Alarme (Altsystem) angezeigt werden, sind nicht unbedingt Probleme mit dem Systembetrieb. Untersuchen Sie die auf der Statuskarte „Systemzustand“ des Grid Manager-Dashboards zusammengefassten Probleme.

Wenn Sie über Warnmeldungen benachrichtigt werden möchten, sobald diese ausgelöst werden, können Sie dies tun ["Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"](#) Oder ["Konfigurieren Sie SNMP-Traps"](#).



Wenn Probleme bestehen, werden Links angezeigt, mit denen Sie weitere Details anzeigen können:

Verlinken	Wird angezeigt, wenn...
Grid-Details	Alle Knoten sind getrennt (Verbindungsstatus Unbekannt oder Administrativ inaktiv).
Aktuelle Warnmeldungen (kritisch, Haupt, Nebenfach)	Warnmeldungen sind Derzeit aktiv .
Kürzlich behobene Warnmeldungen	In der letzten Woche ausgelöste Warnmeldungen Jetzt behoben .
Lizenz	Es liegt ein Problem mit der Softwarelizenz für dieses StorageGRID-System vor. Das können Sie "Aktualisieren Sie die Lizenzinformationen nach Bedarf" .

Überwachen Sie die Status der Node-Verbindung

Wenn ein oder mehrere Nodes vom Grid getrennt werden, können kritische StorageGRID-Vorgänge beeinträchtigt werden. Überwachen Sie den Verbindungsstatus des Knotens, und beheben Sie alle Probleme umgehend.

Symbol	Beschreibung	Handeln erforderlich
	<p>Nicht verbunden - Unbekannt</p> <p>Aus einem unbekanntem Grund ist die Verbindung zu einem Node unterbrochen, oder Dienste auf dem Node wurden unerwartet heruntergefahren. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren.</p> <p>Die Warnung * kann nicht mit Node* kommunizieren. Andere Warnmeldungen können ebenfalls aktiv sein.</p>	<p>Erfordert sofortige Aufmerksamkeit. Wählen Sie jede Warnmeldung aus Und befolgen Sie die empfohlenen Maßnahmen.</p> <p>Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten.</p> <p>Hinweis: Ein Knoten kann während des verwalteten Herunterfahrens als Unbekannt erscheinen. In diesen Fällen können Sie den Status Unbekannt ignorieren.</p>
	<p>Nicht verbunden - Administrativ unten</p> <p>Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden.</p> <p>Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist möglicherweise auch aktiv.</p> <p>Aufgrund des zugrunde liegenden Problems sind diese Nodes oft ohne Eingriff wieder online.</p>	<p>Ermitteln Sie, ob Warnmeldungen Auswirkungen auf diesen Node haben.</p> <p>Wenn eine oder mehrere Warnungen aktiv sind, Wählen Sie jede Warnmeldung aus Und befolgen Sie die empfohlenen Maßnahmen.</p>
	<ul style="list-style-type: none"> • Verbunden* <p>Der Knoten ist mit dem Raster verbunden.</p>	Keine Aktion erforderlich.

Anzeige aktueller und aufgelöster Warnmeldungen

Aktuelle Alarme: Wenn ein Alarm ausgelöst wird, wird ein Warnsymbol auf dem Dashboard angezeigt. Auf der Seite Knoten wird auch ein Warnungssymbol für den Knoten angezeigt. Wenn "[Benachrichtigungen für Warnmeldungen sind konfiguriert](#)", Eine E-Mail-Benachrichtigung wird ebenfalls gesendet, es sei denn, die Benachrichtigung wurde stummgeschaltet.

Aufgelöste Warnungen: Sie können einen Verlauf von Warnungen suchen und anzeigen, die behoben wurden.

Optional haben Sie sich das Video angesehen: "[Video: Übersicht über Warnmeldungen für StorageGRID 11.7](#)"



In der folgenden Tabelle werden die im Grid Manager angezeigten Informationen zu aktuellen und behobenen Warnmeldungen beschrieben.

Spaltenüberschrift	Beschreibung
Name oder Titel	Der Name der Warnmeldung und deren Beschreibung.
Schweregrad	<p>Der Schweregrad der Meldung. Wenn bei aktuellen Warnmeldungen mehrere Warnmeldungen gruppiert werden, zeigt die Titelzeile an, wie viele Instanzen dieser Warnmeldung bei jedem Schweregrad auftreten.</p> <p> Kritisch: Es existiert eine anormale Bedingung, die den normalen Betrieb eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen.</p> <p> Major: Es gibt einen anormalen Zustand, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für einen kritischen Alarm nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet.</p> <p> Minor: Das System funktioniert normal, aber es gibt einen ungewöhnlichen Zustand, der die Fähigkeit des Systems beeinflussen könnte, wenn es weitergeht. Sie sollten kleinere Warnmeldungen überwachen und beheben, die nicht von selbst geklärt werden, um sicherzustellen, dass sie nicht zu einem schwerwiegenden Problem führen.</p>
Auslösezeit	<p>Aktuelle Alarme: Das Datum und die Uhrzeit, zu der der Alarm in Ihrer Ortszeit und in UTC ausgelöst wurde. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile Zeiten für die letzte Instanz der Warnmeldung (<i>neueste</i>) und die älteste Instanz der Warnmeldung (<i>älteste</i>) an.</p> <p>Resolved Alerts: Wie lange ist es her, dass der Alarm ausgelöst wurde.</p>
Standort/Knoten	Der Name des Standorts und des Knotens, an dem die Warnung auftritt oder aufgetreten ist.

Spaltenüberschrift	Beschreibung
Status	Gibt an, ob die Warnmeldung aktiv, stummgeschaltet oder behoben ist. Wenn mehrere Warnungen gruppiert sind und Alle Alarme in der Dropdown-Liste ausgewählt ist, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung aktiv sind und wie viele Instanzen zum Schweigen gebracht wurden.
Behobene Zeit (nur behobene Warnmeldungen)	Wie lange zuvor wurde die Warnung behoben.
Aktuelle Werte oder <i>Datenwerte</i>	Der Wert der Metrik, der den Auslöser der Meldung verursacht hat. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Meldung mit * Objekt-Datenspeicher* enthalten beispielsweise den Prozentsatz des verwendeten Festplattenspeichers, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Festplattenspeichers. Hinweis: Wenn mehrere aktuelle Warnungen gruppiert werden, werden die aktuellen Werte nicht in der Titelzeile angezeigt.
Ausgelöste Werte (nur gelöste Warnmeldungen)	Der Wert der Metrik, der den Auslöser der Meldung verursacht hat. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Meldung mit * Objekt-Datenspeicher* enthalten beispielsweise den Prozentsatz des verwendeten Festplattenspeichers, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Festplattenspeichers.

Schritte

1. Wählen Sie den Link **Aktuelle Alarme** oder **gelöste Warnmeldungen** aus, um eine Liste der Warnungen in diesen Kategorien anzuzeigen. Sie können die Details für eine Warnmeldung auch anzeigen, indem Sie **Nodes > Node > Übersicht** auswählen und dann die Warnmeldung aus der Tabelle Alerts auswählen.

Standardmäßig werden aktuelle Warnmeldungen wie folgt angezeigt:

- Die zuletzt ausgelösten Warnmeldungen werden zuerst angezeigt.
- Mehrere Warnmeldungen desselben Typs werden als Gruppe angezeigt.
- Alarme, die stummgeschaltet wurden, werden nicht angezeigt.
- Wenn für eine bestimmte Warnmeldung auf einem bestimmten Node die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird nur die schwerste Warnmeldung angezeigt. Wenn also Alarmschwellenwerte für kleinere, größere und kritische Schweregrade erreicht werden, wird nur die kritische Warnung angezeigt.

Die Seite Aktuelle Warnmeldungen wird alle zwei Minuten aktualisiert.

2. Um die Gruppen von Warnmeldungen zu erweitern, wählen Sie das Down-Menü aus ▼. Um einzelne Warnmeldungen in einer Gruppe auszublenden, wählen Sie das up-Caret aus ▲, Oder wählen Sie den Namen der Gruppe aus.
3. Um einzelne Warnungen anstelle von Warengruppen anzuzeigen, deaktivieren Sie das Kontrollkästchen **Gruppenwarnungen**.

4. Um aktuelle Warnmeldungen oder Warnungsgruppen zu sortieren, wählen Sie die nach-oben-/nach-unten-Pfeile aus  In jeder Spaltenüberschrift.
 - Wenn **Group Alerts** ausgewählt ist, werden sowohl die Warnungsgruppen als auch die einzelnen Alarme innerhalb jeder Gruppe sortiert. Sie können beispielsweise die Warnungen in einer Gruppe nach **Zeit ausgelöst** sortieren, um die aktuellste Instanz eines bestimmten Alarms zu finden.
 - Wenn **Group Alerts** gelöscht wird, wird die gesamte Liste der Alerts sortiert. Beispielsweise können Sie alle Warnungen nach **Node/Site** sortieren, um alle Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.
5. Um aktuelle Warnmeldungen nach Status (**Alle Alarme**, **aktiv** oder **quittiert**) zu filtern, verwenden Sie das Dropdown-Menü oben in der Tabelle.

Siehe "[Benachrichtigung über Stille](#)".

6. So sortieren Sie behobene Warnmeldungen:
 - Wählen Sie im Dropdown-Menü **When Triggered** einen Zeitraum aus.
 - Wählen Sie eine oder mehrere Schweregrade aus dem Dropdown-Menü **Schweregrad** aus.
 - Wählen Sie im Dropdown-Menü **Warnregel** eine oder mehrere Standard- oder benutzerdefinierte Warnungsregeln aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einer bestimmten Alarmregel zusammenhängen.
 - Wählen Sie im Dropdown-Menü **Node** einen oder mehrere Knoten aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einem bestimmten Knoten verbunden sind.
7. Um Details für eine bestimmte Warnmeldung anzuzeigen, wählen Sie die Warnmeldung aus. Ein Dialogfeld enthält Details und empfohlene Aktionen für die ausgewählte Warnmeldung.
8. (Optional) Wählen Sie für einen bestimmten Alarm die Option Diese Warnung stummschalten, um die Alarmregel, die diese Warnung ausgelöst hat, stummzuschalten.

Sie müssen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff verfügen, um eine Warnungsregel stumm schalten zu können.



Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummzuschalten. Wenn eine Alarmregel stumm geschaltet ist, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang abgeschlossen wird.

9. So zeigen Sie die aktuellen Bedingungen für die Meldungsregel an:
 - a. Wählen Sie aus den Warnungsdetails **Bedingungen anzeigen**.

Es wird ein Popup-Fenster mit dem Prometheus-Ausdruck für jeden definierten Schweregrad angezeigt.
 - b. Um das Popup-Fenster zu schließen, klicken Sie außerhalb des Popup-Dialogfenster auf eine beliebige Stelle.
10. Wählen Sie optional **Regel bearbeiten**, um die Warnungsregel zu bearbeiten, die diese Warnung ausgelöst hat.

Sie müssen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff verfügen, um eine Warnungsregel bearbeiten zu können.



Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnungsregel zu bearbeiten. Wenn Sie die Triggerwerte ändern, können Sie möglicherweise ein zugrunde liegendes Problem erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

11. Um die Alarmdetails zu schließen, wählen Sie **Schließen**.

Monitoring der Storage-Kapazität

Überwachen Sie den insgesamt verfügbaren nutzbaren Speicherplatz, um sicherzustellen, dass dem StorageGRID System der Speicherplatz für Objekte oder Objekt-Metadaten nicht knapp wird.

StorageGRID speichert Objektdaten und Objektmetadaten separat und behält eine bestimmte Menge an Speicherplatz für eine verteilte Cassandra-Datenbank mit Objekt-Metadaten bei. Überwachen Sie den Gesamtspeicherplatz für Objekte und Objekt-Metadaten sowie Trends für den Speicherplatz, der für jeden verbraucht wird. So können Sie das Hinzufügen von Nodes vorausschauender planen und Serviceausfälle vermeiden.

Das können Sie ["Informationen zur Storage-Kapazität anzeigen"](#) Für das gesamte Grid, für jeden Standort und für jeden Storage-Node im StorageGRID-System.

Überwachung der Speicherkapazität für das gesamte Grid

Überwachen Sie die Gesamt-Storage-Kapazität Ihres Grids, um sicherzustellen, dass ausreichend freier Speicherplatz für Objektdaten und Objektmetadaten verbleibt. Wenn Sie verstehen, wie sich die Storage-Kapazität im Laufe der Zeit verändert, können Sie Storage-Nodes oder Storage-Volumes planen, bevor die nutzbare Storage-Kapazität des Grid verbraucht wird.

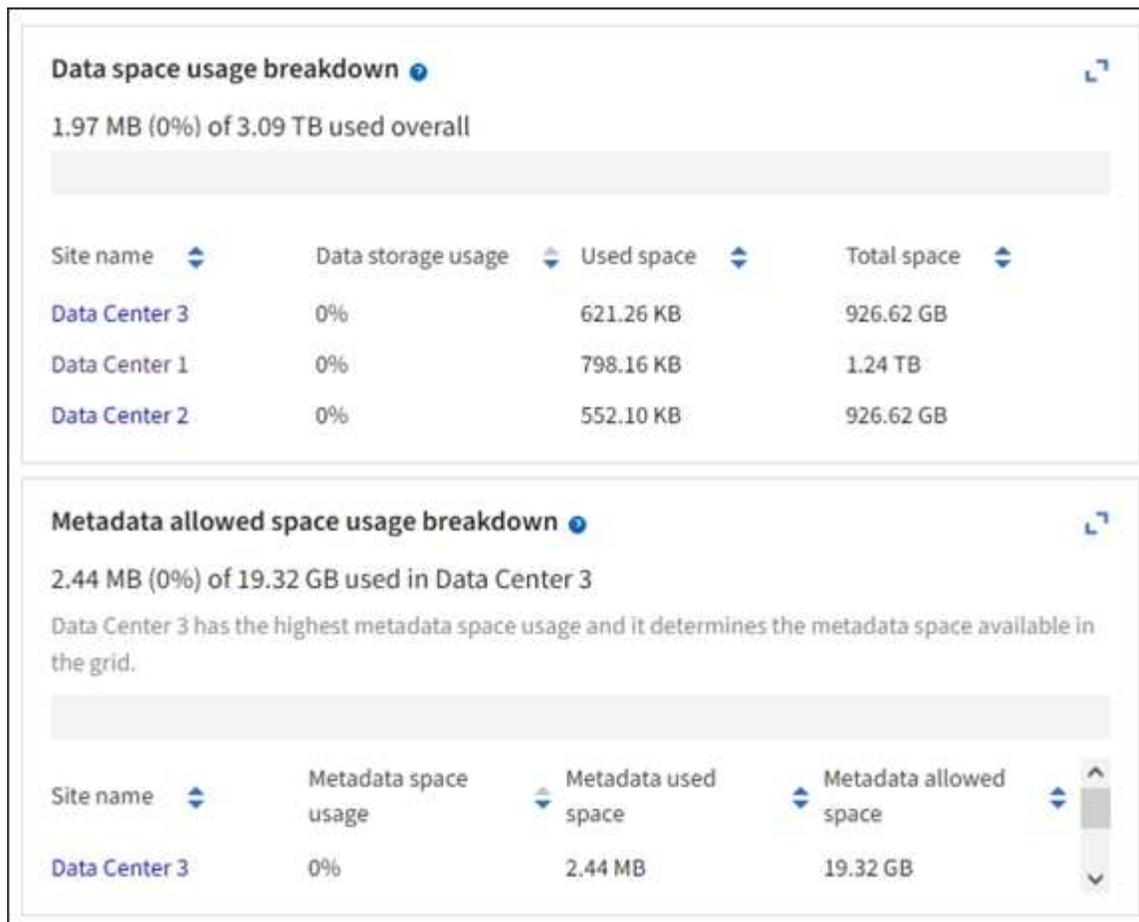
Mithilfe des Grid Manager Dashboards können Sie schnell bewerten, wie viel Storage für das gesamte Grid und für jedes Datacenter verfügbar ist. Die Seite Knoten enthält detailliertere Werte für Objektdaten und Objektmetadaten.

Schritte

1. Beurteilen Sie, wie viel Storage für das gesamte Grid und das jeweilige Datacenter verfügbar ist.
 - a. Wählen Sie **Dashboard > Übersicht**.
 - b. Beachten Sie die Werte für die Aufschlüsselung der Speicherplatznutzung und die Aufschlüsselung der Metadaten für die zulässige Speicherplatznutzung. Jede Karte listet einen Prozentsatz der Speichernutzung, die Kapazität des belegten Speicherplatzes und den gesamten verfügbaren oder von der Site erlaubten Speicherplatz auf.



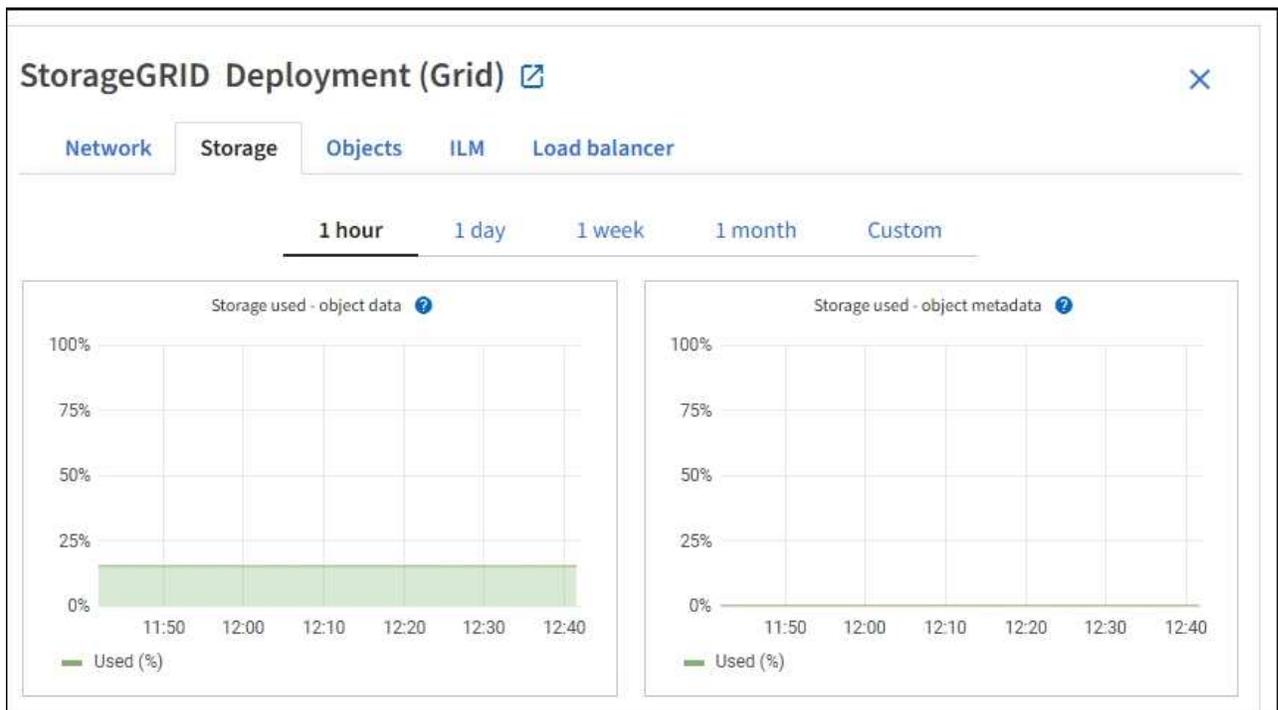
Die Zusammenfassung enthält keine Archivierungsmedien.



- a. Notieren Sie sich das Diagramm auf der Karte „Speicher im Zeitverlauf“. Anhand der Dropdown-Liste „Zeitraum“ können Sie ermitteln, wie schnell Storage verbraucht wird.



2. Auf der Seite Nodes finden Sie weitere Details dazu, wie viel Storage genutzt wurde und wie viel Storage für Objektdaten und Objektmetadaten im Grid verfügbar bleibt.
- Wählen Sie **KNOTEN**.
 - Wählen Sie **Grid > Storage** aus.



- c. Bewegen Sie den Cursor über die **Storage Used - Object Data** und die **Storage Used - Object metadata** Diagramme, um zu sehen, wie viel Objektspeicher und Objektmetadaten-Speicher für das gesamte Grid verfügbar sind und wie viel im Laufe der Zeit genutzt wurde.



Die Gesamtwerte für einen Standort oder das Raster enthalten keine Knoten, die mindestens fünf Minuten lang keine Kennzahlen gemeldet haben, z. B. Offline-Nodes.

3. Planung, eine Erweiterung zum Hinzufügen von Storage-Nodes oder Storage-Volumes durchzuführen, bevor die nutzbare Storage-Kapazität des Grid genutzt wird

Berücksichtigen Sie bei der Planung des Zeitplans für eine Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Storage dauern wird.



Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, wird es möglicherweise besser erweitert, wenn vorhandene Storage-Nodes ungefähr 70 % ausgelastet sind, um die Anzahl der hinzugefügten Nodes zu verringern.

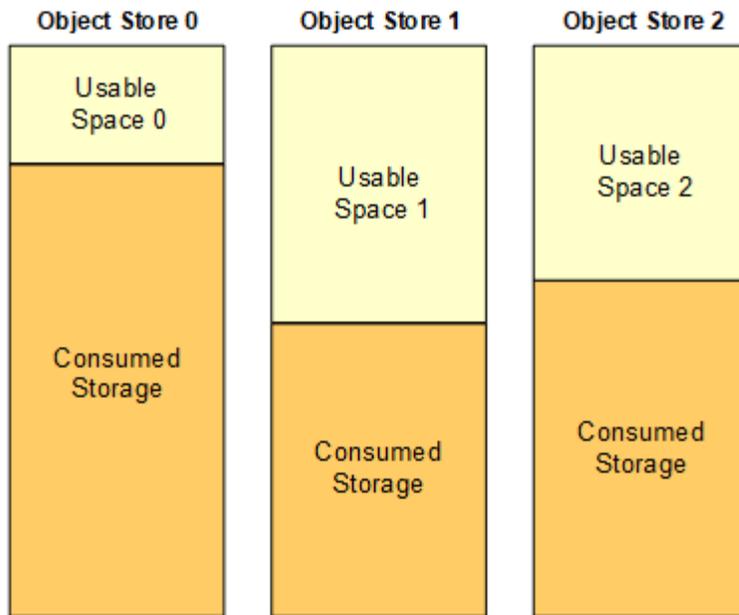
Weitere Informationen zur Planung einer Speichererweiterung finden Sie im "[Anweisungen zur Erweiterung von StorageGRID](#)".

Überwachen Sie die Storage-Kapazität für jeden Storage-Node

Überwachen Sie den insgesamt nutzbaren Speicherplatz für jeden Storage-Node, um sicherzustellen, dass der Node über ausreichend Speicherplatz für neue Objektdaten verfügt.

Über diese Aufgabe

Der nutzbare Speicherplatz ist der Speicherplatz, der zum Speichern von Objekten zur Verfügung steht. Der insgesamt nutzbare Speicherplatz für einen Storage-Node wird berechnet, indem der verfügbare Speicherplatz in allen Objektspeichern innerhalb des Node hinzugefügt wird.



Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2

Schritte

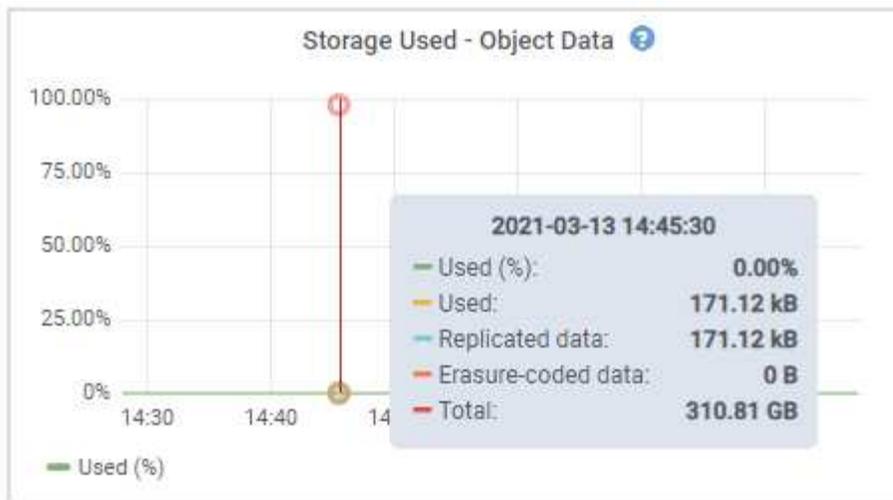
1. Wählen Sie **NODES > Storage Node > Storage** aus.

Die Diagramme und Tabellen für den Node werden angezeigt.

2. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objektdaten.

Die folgenden Werte werden angezeigt:

- **Used (%)**: 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, Standort oder Grid.
- **Erasur-codierte Daten**: Eine Schätzung der Menge der mit der Löschung codierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Gesamt**: Die Gesamtmenge an nutzbarem Speicherplatz auf diesem Knoten, Standort oder Grid. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` Metrisch.



3. Überprüfen Sie die verfügbaren Werte in den Tabellen Volumes und Objektspeichern unter den Diagrammen.



Klicken Sie auf die Diagrammsymbole, um Diagramme dieser Werte anzuzeigen. 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

- Überwachen Sie die Werte im Zeitbereich, um die Rate abzuschätzen, mit der der nutzbare Speicherplatz belegt wird.
- Um normale Systemvorgänge aufrechtzuerhalten, fügen Sie Storage-Nodes hinzu, fügen Storage Volumes oder Archivdaten hinzu, bevor der nutzbare Speicherplatz verbraucht wird.

Berücksichtigen Sie bei der Planung des Zeitplans für eine Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Storage dauern wird.



Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, wird es möglicherweise besser erweitert, wenn vorhandene Storage-Nodes ungefähr 70 % ausgelastet sind, um die Anzahl der hinzugefügten Nodes zu verringern.

Weitere Informationen zur Planung einer Speichererweiterung finden Sie im ["Anweisungen zur Erweiterung"](#)

von StorageGRID".

Der "Niedriger Objekt-Storage" Die Meldung wird ausgelöst, wenn nicht genügend Speicherplatz zum Speichern von Objektdaten auf einem Storage-Node verbleibt.

Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node

Überwachen Sie die Metadatenutzung für jeden Storage-Node, um sicherzustellen, dass ausreichend Speicherplatz für wichtige Datenbankvorgänge verfügbar ist. Sie müssen an jedem Standort neue Storage-Nodes hinzufügen, bevor die Objektmetadaten 100 % des zulässigen Metadaten-Speicherplatzes übersteigen.

Über diese Aufgabe

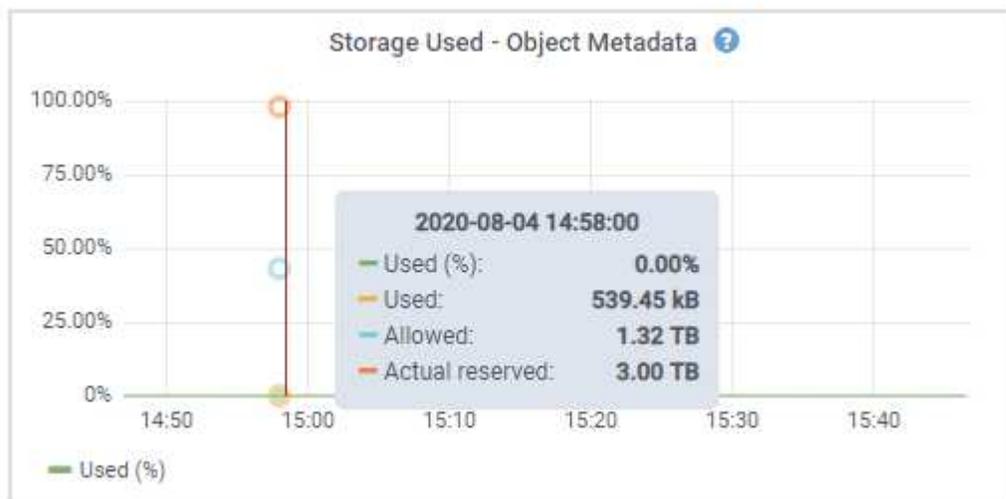
StorageGRID behält drei Kopien von Objektmetadaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem Storage Volume 0 jedes Storage-Nodes verwendet.

In einigen Fällen wird die Kapazität der Objektmetadaten des Grid möglicherweise schneller belegt als die Kapazität des Objekt-Storage. Wenn Sie zum Beispiel normalerweise eine große Anzahl von kleinen Objekten aufnehmen, müssen Sie möglicherweise Storage-Nodes hinzufügen, um die Metadaten-Kapazität zu erhöhen, obwohl weiterhin ausreichend Objekt-Storage-Kapazität vorhanden ist.

Zu den Faktoren, die die Metadatenutzung steigern können, gehören die Größe und Menge der Metadaten und -Tags der Benutzer, die Gesamtzahl der Teile in einem mehrteiligen Upload und die Häufigkeit von Änderungen an den ILM-Speicherorten.

Schritte

1. Wählen Sie **NODES > Storage Node > Storage** aus.
2. Bewegen Sie den Mauszeiger über das Diagramm Speicher verwendet – Objekt-Metadaten, um die Werte für eine bestimmte Zeit anzuzeigen.



Nutzung (%)

Der Prozentsatz des zulässigen Metadaten-Speicherplatzes, der auf diesem Storage-Node verwendet wurde.

Prometheus Kennzahlen: `storagegrid_storage_utilization_metadata_bytes` Und `storagegrid_storage_utilization_metadata_allowed_bytes`

Verwendet

Die Bytes des zulässigen Metadaten-Speicherplatzes, der auf diesem Speicherknoten verwendet wurde.

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_bytes`

Zulässig

Der zulässige Speicherplatz für Objektmetadaten auf diesem Storage-Node. Informationen darüber, wie dieser Wert für jeden Storage-Node bestimmt wird, finden Sie im ["Vollständige Beschreibung des zulässigen MetadatenSpeichers"](#).

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_allowed_bytes`

Ist reserviert

Der tatsächliche Speicherplatz, der für Metadaten auf diesem Speicherknoten reserviert ist. Beinhaltet den zulässigen Speicherplatz und den erforderlichen Speicherplatz für wichtige Metadaten-Vorgänge. Informationen dazu, wie dieser Wert für jeden Storage-Node berechnet wird, finden Sie im ["Vollständige Beschreibung des tatsächlich reservierten Speicherplatzes für Metadaten"](#).

Prometheus Metrik wird in einer zukünftigen Version hinzugefügt.



Die Gesamtwerte für einen Standort oder das Raster enthalten keine Knoten, die mindestens fünf Minuten lang keine Kennzahlen gemeldet haben, z. B. Offline-Nodes.

3. Wenn der * verwendete (%)*-Wert 70% oder höher ist, erweitern Sie Ihr StorageGRID-System, indem Sie jedem Standort Storage-Knoten hinzufügen.



Der Alarm * Low Metadaten Storage* wird ausgelöst, wenn der Wert **used (%)** bestimmte Schwellenwerte erreicht. Unerwünschte Ergebnisse können auftreten, wenn Objekt-Metadaten mehr als 100 % des zulässigen Speicherplatzes beanspruchen.

Wenn Sie die neuen Nodes hinzufügen, gleicht das System die Objektmetadaten automatisch auf alle Storage-Nodes am Standort aus. Siehe ["Anweisungen zum erweitern eines StorageGRID-Systems"](#).

Prognosen zur Speicherplatznutzung überwachen

Überwachen Sie Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten, um abzuschätzen, wann Sie dies benötigen ["Erweitern Sie Ihr Raster"](#).

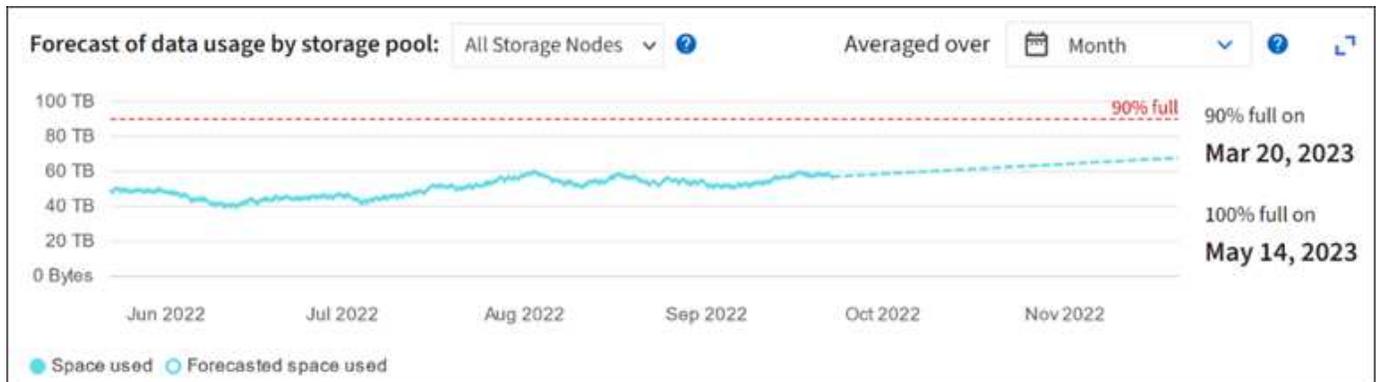
Wenn Sie feststellen, dass sich die Verbrauchsrate im Laufe der Zeit ändert, wählen Sie einen kürzeren Bereich aus dem Pull-down-Menü **gemittelt über** aus, um nur die neuesten Aufnahmemuster wiederzugeben. Wenn Sie saisonale Muster bemerken, wählen Sie einen längeren Bereich aus.

Falls Sie eine neue StorageGRID-Installation besitzen, lassen Sie vor der Evaluierung der Prognosen zur Speicherplatznutzung zu, dass sich Daten und Metadaten anhäufen können.

Schritte

1. Wählen Sie auf dem Dashboard **Speicher**.
2. Sie können die Dashboard-Karten, Prognosen zur Datennutzung nach Storage-Pool und Prognosen zur Metadatenutzung nach Standort anzeigen.
3. Verwenden Sie diese Werte, um zu schätzen, wann Sie neue Storage-Nodes für den Daten- und

Metadatenpeicher hinzufügen müssen.



Überwachung des Information Lifecycle Management

Das Information Lifecycle Management-System (ILM) ermöglicht Datenmanagement für alle im Grid gespeicherten Objekte. Sie müssen die ILM-Vorgänge überwachen, um nachzuvollziehen, ob das Grid die aktuelle Auslastung handhaben kann oder ob weitere Ressourcen erforderlich sind.

Über diese Aufgabe

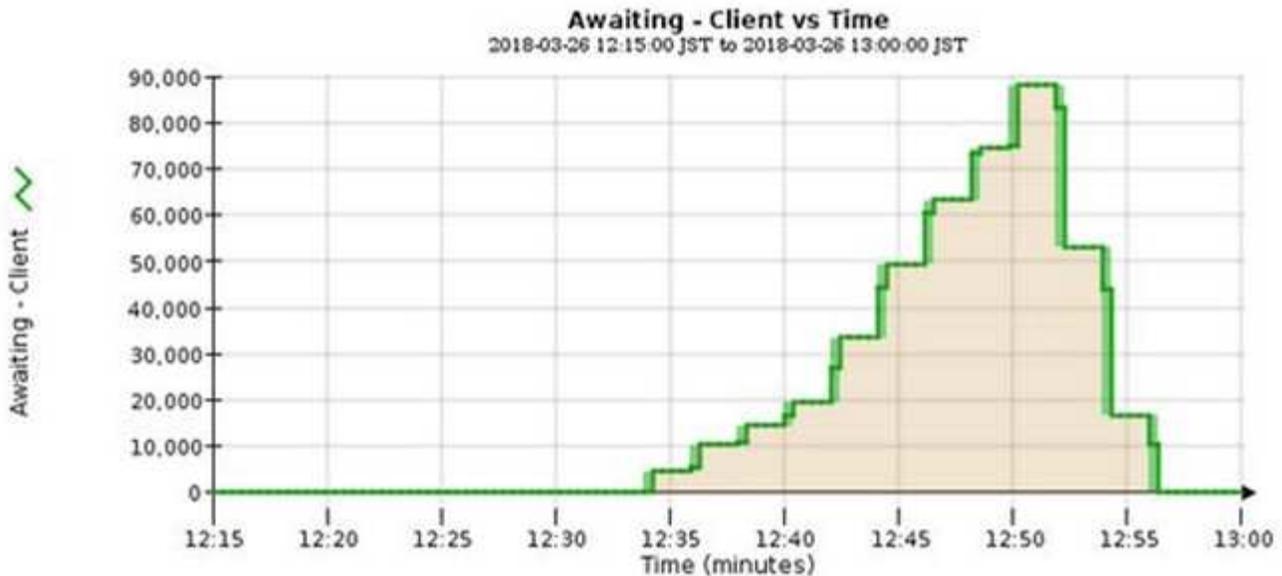
Das StorageGRID System managt Objekte mithilfe der aktiven ILM-Richtlinie. Die ILM-Richtlinie und die zugehörigen ILM-Regeln bestimmen die Anzahl der Kopien, die Art der erstellten Kopien, das Erstellen von Kopien und die Dauer der Aufbewahrung jeder Kopie.

Die Objektaufnahme und andere objektbezogene Aktivitäten können die Geschwindigkeit übersteigen, mit der StorageGRID ILM-Prozesse evaluieren kann, sodass das System Objekte in eine Warteschlange einstellt, deren ILM-Platzierungsanweisungen nicht nahezu in Echtzeit erfüllt werden können. Sie können überwachen, ob StorageGRID mit den Client-Aktionen Schritt hält, indem Sie das Attribut „Warten – Client“ schreiben.

So setzen Sie dieses Attribut auf:

1. Melden Sie sich beim Grid Manager an.
2. Suchen Sie im Dashboard auf der Registerkarte Information Lifecycle Management (ILM) den Eintrag **waiting - Client**.
3. Klicken Sie auf das Diagrammsymbol .

Das Beispieldiagramm zeigt eine Situation, in der die Anzahl der Objekte, die auf eine ILM-Bewertung warten, vorübergehend nicht aufrechterhalten ist, dann aber gesunken ist. Ein solcher Trend zeigt, dass ILM vorübergehend nicht in Echtzeit erfüllt wurde.



Temporäre Spitzen in der Tabelle von wartet - Client sind zu erwarten. Wenn der in der Grafik angezeigte Wert jedoch weiter steigt und nie sinkt, erfordert das Grid mehr Ressourcen für einen effizienten Betrieb: Entweder mehr Storage-Nodes oder, wenn die ILM-Richtlinie Objekte an Remote-Standorten platziert, erhöht sich die Netzwerkbandbreite.

Mithilfe der Seite **NODES** können Sie sich weiter mit ILM-Warteschlangen beschäftigen.

Schritte

1. Wählen Sie **KNOTEN**.
2. Wählen Sie **Grid Name > ILM** aus.
3. Bewegen Sie den Mauszeiger über das ILM-Warteschlangendiagramm, um den Wert der folgenden Attribute zu einem bestimmten Zeitpunkt anzuzeigen:
 - **Objekte in der Warteschlange (aus Client-Operationen)**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aufgrund von Client-Operationen warten (z. B. Aufnahme).
 - **Objekte in der Warteschlange (aus allen Operationen)**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung warten.
 - **Scan-Rate (Objects/sec)**: Die Geschwindigkeit, mit der Objekte im Raster gescannt und für ILM in die Warteschlange gestellt werden.
 - **Evaluationsrate (Objects/sec)**: Die aktuelle Rate, mit der Objekte anhand der ILM-Richtlinie im Grid ausgewertet werden.
4. Sehen Sie sich im Abschnitt ILM-Warteschlange die folgenden Attribute an.



Der Abschnitt ILM-Warteschlange ist nur für das Grid enthalten. Diese Informationen werden auf der Registerkarte ILM für einen Standort oder Storage Node nicht angezeigt.

- **Scan Period - Estimated**: Die geschätzte Zeit, um einen vollständigen ILM-Scan aller Objekte abzuschließen.



Ein vollständiger Scan gewährleistet nicht, dass ILM auf alle Objekte angewendet wurde.

- **Reparairs versuchte:** Die Gesamtzahl der Objektreparaturvorgänge für replizierte Daten, die versucht wurden. Diese Zählung erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein Objekt mit hohem Risiko zu reparieren. Risikobehaftete ILM-Reparaturen werden priorisiert, wenn das Grid besetzt wird.



Die Reparatur desselben Objekts erhöht sich möglicherweise erneut, wenn die Replikation nach der Reparatur fehlgeschlagen ist.

Diese Attribute können nützlich sein, wenn Sie den Fortschritt der Wiederherstellung von Storage Node Volumes überwachen. Wenn die Anzahl der versuchten Reparaturen gestoppt wurde 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 einzelner Grid-Nodes sind für einen effizienten Betrieb von entscheidender Bedeutung.

Überwachen Sie Netzwerkverbindungen und Performance

Netzwerkonnektivität und Bandbreite sind besonders wichtig, wenn Ihre Richtlinien für Information Lifecycle Management (ILM) replizierte Objekte zwischen Standorten kopieren oder Erasure Coding-codierte Objekte mit einem Schema speichern, das Site-Loss-Schutz bietet. Wenn das Netzwerk zwischen Standorten nicht verfügbar ist, die Netzwerklatenz zu hoch ist oder die Netzwerkbandbreite nicht ausreicht, können einige ILM-Regeln Objekte möglicherweise nicht an den erwarteten Stellen platzieren. Dies kann zu Aufnahmeausfällen (wenn die strikte Aufnahmeoption für ILM-Regeln ausgewählt wird) oder zu schlechter Aufnahme-Performance und ILM-Rückprotokollen führen.

Überwachen Sie die Konnektivität und die Netzwerk-Performance mit dem Grid Manager, damit Sie bei Problemen umgehend auf Probleme reagieren können.

Darüber hinaus sollten Sie in Betracht ziehen ["Erstellen von Klassifizierungsrichtlinien für den Netzwerkverkehr"](#) So können Sie den Datenverkehr zu bestimmten Mandanten, Buckets, Subnetzen oder Endpunkten des Load Balancer überwachen. Sie können Richtlinien zur Begrenzung des Datenverkehrs nach Bedarf festlegen.

Schritte

1. Wählen Sie **KNOTEN**.

Die Seite Knoten wird angezeigt. Jeder Knoten im Raster wird im Tabellenformat aufgelistet.

DASHBOARD

ALERTS ✓ ^

Current

Resolved

Silences

Rules

Email setup

NODES

TENANTS

ILM ∨

CONFIGURATION

MAINTENANCE

SUPPORT

Nodes

View the list and status of sites and grid nodes.

Search... 🔍 Total node count: 14

Name ? ∨	Type ∨	Object data used ? ∨	Object metadata used ? ∨	CPU usage ? ∨
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

2. Wählen Sie den Grid-Namen, einen bestimmten Datacenter-Standort oder einen Grid-Node aus, und wählen Sie dann die Registerkarte **Netzwerk** aus.

Das Diagramm „Netzwerk-Traffic“ bietet eine Zusammenfassung des gesamten Netzwerkverkehr für das gesamte Grid, den Datacenter-Standort oder für den Node.



- a. Wenn Sie einen Rasterknoten ausgewählt haben, scrollen Sie nach unten, um den Abschnitt **Netzwerkschnittstellen** auf der Seite anzuzeigen.

Network interfaces

Name ? ∨	Hardware address ? ∨	Speed ?	Duplex ? ∨	Auto-negotiation ? ∨	Link status ? ∨
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

- b. Blättern Sie bei Rasterknoten nach unten, um den Abschnitt **Netzwerkkommunikation** auf der Seite anzuzeigen.

Die Tabellen „Empfangen und Senden“ zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Übertragungstabellen.

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 Metriken für Ihre Traffic-Klassifizierungsrichtlinien zur Überwachung des Netzwerkverkehrs.

a. Wählen Sie **CONFIGURATION > Network > traffic classification**.

Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create ✎ Edit ✕ Remove 📊 Metrics		
Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

a. Um Diagramme anzuzeigen, die die mit einer Richtlinie verknüpften Netzwerkmetriken anzeigen, wählen Sie das Optionsfeld links neben der Richtlinie aus, und klicken Sie dann auf **Metriken**.

b. Überprüfen Sie die Diagramme, um den mit der Richtlinie verknüpften Netzwerkverkehr zu verstehen.

Wenn eine Richtlinie zur Klassifizierung von Verkehrsströmen darauf ausgelegt ist, den Netzwerkverkehr zu begrenzen, analysieren Sie, wie oft der Datenverkehr begrenzt ist, und entscheiden Sie, ob die Richtlinie Ihre Anforderungen weiterhin erfüllt. Von Zeit zu Zeit "[Passen Sie jede Richtlinie zur Verkehrsklassifizierung nach Bedarf an](#)".

Verwandte Informationen

["Zeigen Sie die Registerkarte Netzwerk an"](#)

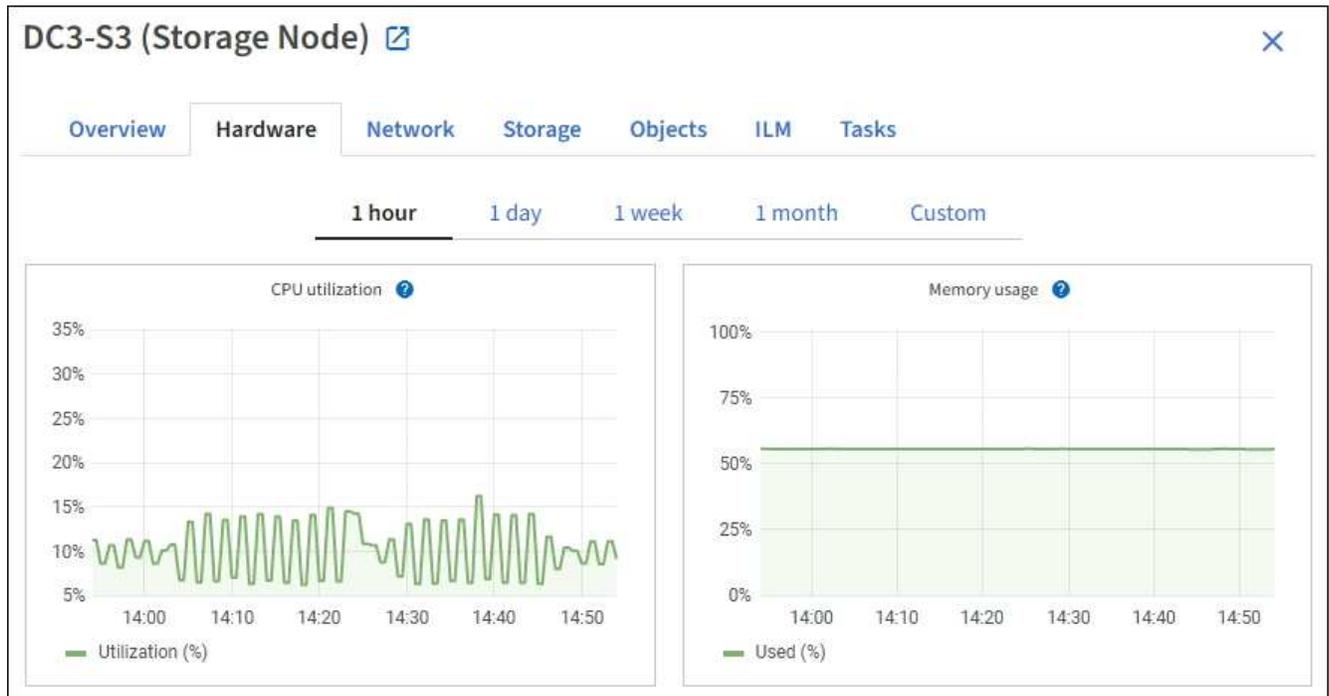
["Überwachen Sie die Status der Node-Verbindung"](#)

Monitoring von Ressourcen auf Node-Ebene

Überwachen Sie einzelne Grid-Nodes, um deren Ressourcenverbrauch zu prüfen. Sind Nodes konsistent überlastet, sind möglicherweise mehr Nodes erforderlich, um einen effizienten Betrieb zu gewährleisten.

Schritte

1. Wählen Sie auf der Seite **NODES** den Knoten aus.
2. Wählen Sie die Registerkarte **Hardware** aus, um Grafiken der CPU-Auslastung und der Speicherauslastung anzuzeigen.



3. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.
4. Wenn der Node auf einer Storage Appliance oder einer Services Appliance gehostet wird, scrollen Sie nach unten, um die Komponententabellen anzuzeigen. Der Status aller Komponenten sollte „Nominal“ sein. Untersuchen Sie Komponenten, die einen anderen Status haben.

Verwandte Informationen

["Zeigen Sie Informationen zu Appliance Storage Nodes an"](#)

["Zeigen Sie Informationen zu Appliance Admin Nodes und Gateway Nodes an"](#)

Überwachen Sie die Mandantenaktivität

Alle S3- und Swift-Client-Aktivitäten sind mit StorageGRID-Mandantenkonten verknüpft. Mit dem Grid Manager können Sie die Storage-Auslastung oder den Netzwerk-Traffic für alle Mandanten oder einen bestimmten Mandanten überwachen. Mithilfe des Revisionsprotokoll und Grafana-Dashboards können Sie detailliertere Informationen darüber sammeln, wie Mandanten StorageGRID verwenden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung Root-Zugriff oder Mandantenkonten.

Alle Mandanten anzeigen

Auf der Seite Tenants werden grundlegende Informationen für alle aktuellen Mandantenkonten angezeigt.

Schritte

1. Wählen Sie **MIETER**.
2. Überprüfen Sie die auf den Mandanten-Seiten angezeigten Informationen.

Für jeden Mandanten werden der verwendete logische Speicherplatz, die Kontingentnutzung, Kontingente und Objektanzahl aufgelistet. Wenn kein Kontingent für einen Mandanten festgelegt ist, enthalten die Felder Quotenauslastung und Quota einen Strich (—).



Die Werte für den genutzten Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;"></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;"></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;"></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;"></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

3. Melden Sie sich optional bei einem Mandantenkonto an, indem Sie den Anmeldelink auswählen [→](#) In der Spalte **Anmelden/URL kopieren**.
4. Kopieren Sie optional die URL für die Anmeldeseite eines Mandanten, indem Sie den Link URL kopieren auswählen [📄](#) In der Spalte **Anmelden/URL kopieren**.
5. Wählen Sie optional **Export to CSV**, um einen anzuzeigen und zu exportieren .csv Datei mit den Nutzungswerten für alle Mandanten.

Sie werden aufgefordert, das zu öffnen oder zu speichern .csv Datei:

Der Inhalt des .csv Datei sieht wie das folgende Beispiel aus:

Sie können das öffnen .csv Datei in einer Tabellenkalkulationsanwendung speichern oder in

Automatisierung verwenden.

6. Wenn keine Objekte aufgelistet sind, wählen Sie optional **actions** > **Delete** aus, um einen oder mehrere Tenants zu entfernen. Siehe "[Mandantenkonto löschen](#)".

Sie können ein Mandantenkonto nicht entfernen, wenn das Konto Buckets oder Container enthält.

Zeigen Sie eine bestimmte Serviceeinheit an

Sie können Details zu einem bestimmten Mandanten anzeigen.

Schritte

1. Wählen Sie auf der Seite Tenants den Namen der Serviceeinheit aus.

Die Seite mit den Mandantendetails wird angezeigt.

Tenant 02

Tenant ID: 4103 1879 2208 5551 2180 

Protocol: S3

Object count: 500

Quota utilization: 85%

Logical space used: 85.00 GB

Quota: 100.00 GB

[Sign in](#) [Edit](#) [Actions](#) ▾

[Space breakdown](#) [Allowed features](#)

Bucket space consumption

85.00 GB of 100.00 GB used

15.00 GB remaining (15%).



0 25% 50% 75% 100%

 bucket-01  bucket-02  bucket-03

Bucket details

[Export to CSV](#) 

Displaying 3 results

Name 	Region 	Space used 	Object count 
bucket-01		40.00 GB	250
bucket-02		30.00 GB	200
bucket-03		15.00 GB	50

2. Überprüfen Sie oben auf der Seite die Übersicht über die Serviceeinheiten.

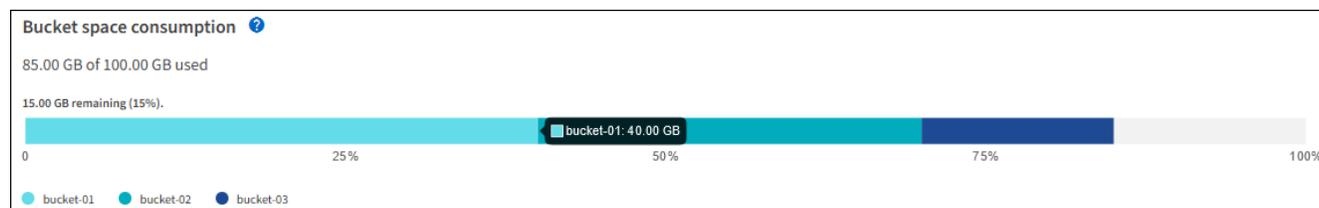
Dieser Abschnitt der Detailseite bietet zusammenfassende Informationen für den Mandanten, einschließlich der Objektanzahl des Mandanten, der Kontingentauslastung, des verwendeten logischen Speicherplatzes und der Kontingenteinstellung.

3. Sehen Sie sich auf der Registerkarte **Raumaufschlüsselung** das Diagramm **Speicherplatzverbrauch** an.

In diesem Diagramm wird der gesamte Speicherplatzverbrauch aller S3-Buckets (oder Swift-Container) des Mandanten angezeigt.

Wenn ein Kontingent für diesen Mandanten festgelegt wurde, wird die Menge der verwendeten und verbleibenden Kontingente im Text angezeigt (z. B. 85.00 GB of 100 GB used). Wenn kein Kontingent festgelegt wurde, hat der Mieter eine unbegrenzte Quote, und der Text enthält nur die Menge des belegten Speicherplatzes (z. B. 85.00 GB used). Das Balkendiagramm zeigt den Prozentsatz der Quoten in jedem Bucket oder Container. Wenn der Mieter das Speicherkontingent um mehr als 1 % und mindestens 1 GB überschritten hat, zeigt das Diagramm das Gesamtkontingent und den Überschuss an.

Sie können den Cursor über das Balkendiagramm platzieren, um den von jedem Bucket oder Container verwendeten Speicher anzuzeigen. Sie können den Cursor über das Segment freier Speicherplatz platzieren, um die verbleibende Menge an Speicherplatz anzuzeigen.



Die Kontingentnutzung basiert auf internen Schätzungen und kann in einigen Fällen sogar überschritten werden. StorageGRID überprüft beispielsweise das Kontingent, wenn ein Mandant beginnt, Objekte hochzuladen und neue Einlässe zurückweist, wenn der Mieter die Quote überschritten hat. StorageGRID berücksichtigt jedoch bei der Bestimmung, ob das Kontingent überschritten wurde, nicht die Größe des aktuellen Uploads. Wenn Objekte gelöscht werden, kann es vorübergehend verhindert werden, dass ein Mandant neue Objekte hochgeladen wird, bis die Kontingentnutzung neu berechnet wird. Berechnungen zur Kontingentnutzung können 10 Minuten oder länger dauern.



Die Kontingentnutzung eines Mandanten gibt die Gesamtanzahl der Objektdaten an, die der Mandant auf StorageGRID (logische Größe) hochgeladen hat. Die Kontingentnutzung stellt nicht den Speicherplatz dar, der zur Speicherung von Kopien dieser Objekte und ihrer Metadaten verwendet wird (physische Größe).



Sie können die Alarmregel **Tenant Quota Usage High** aktivieren, um festzustellen, ob Tenants ihre Quotas verbrauchen. Wenn diese Meldung aktiviert ist, wird diese Meldung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Anweisungen hierzu finden Sie unter ["Bearbeiten von Meldungsregeln"](#).

4. Überprüfen Sie auf der Registerkarte **Space Breakdown** die **Bucket Details**.

In dieser Tabelle werden die S3-Buckets (oder Swift-Container) für den Mandanten aufgeführt. Der verwendete Speicherplatz ist die Gesamtgröße der Objektdaten im Bucket oder Container. Dieser Wert stellt nicht den Storage-Platzbedarf für ILM-Kopien und Objekt-Metadaten dar.

5. Wählen Sie optional **in CSV exportieren** aus, um eine .csv-Datei anzuzeigen und zu exportieren, die die Nutzungswerte für jeden Bucket oder Container enthält.

Den Inhalt eines einzelnen S3-Mandanten .csv Datei sieht wie das folgende 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 öffnen .csv Datei in einer Tabellenkalkulationsanwendung speichern oder in Automatisierung verwenden.

- Wählen Sie optional die Registerkarte **allowed Features** aus, um eine Liste der Berechtigungen und Funktionen anzuzeigen, die für den Mandanten aktiviert sind. Siehe "[Mandantenkonto bearbeiten](#)". Wenn Sie eine dieser Einstellungen ändern müssen.
- Wenn der Mandant die Berechtigung **Grid Federation connection** verwenden hat, wählen Sie optional die Registerkarte **Grid Federation**, um mehr über die Verbindung zu erfahren.

Siehe "[Was ist Grid Federation?](#)" Und "[Verwalten Sie die zulässigen Mandanten für den Grid-Verbund](#)".

Netzwerkverkehr anzeigen

Wenn Richtlinien zur Traffic-Klassifizierung für einen Mandanten vorhanden sind, überprüfen Sie den Netzwerkverkehr für diesen Mandanten.

Schritte

- Wählen Sie **CONFIGURATION > Network > traffic classification**.

Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.

- Anhand der Liste der Richtlinien können Sie diejenigen ermitteln, die für einen bestimmten Mandanten gelten.
- Um Metriken anzuzeigen, die mit einer Richtlinie verknüpft sind, aktivieren Sie das Optionsfeld links neben der Richtlinie, und wählen Sie **Metriken** aus.
- Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

Siehe "[Verwalten von Richtlinien zur Verkehrsklassifizierung](#)" Finden Sie weitere Informationen.

Verwenden Sie das Überwachungsprotokoll

Optional können Sie das Revisionsprotokoll für ein granulareres Monitoring der Aktivitäten eines Mandanten verwenden.

Sie können beispielsweise folgende Informationstypen überwachen:

- Bestimmte Client-Vorgänge, z. B. PUT, GET oder DELETE
- Objektgrößen
- Die ILM-Regel wurde auf Objekte angewendet
- Die Quell-IP von Client-Anforderungen

Audit-Protokolle werden in Textdateien geschrieben, die Sie mit einem Tool Ihrer Wahl analysieren können. Dadurch können Sie Kundenaktivitäten besser verstehen oder ausgereifte Chargeback- und Abrechnungsmodelle implementieren.

Siehe ["Prüfung von Audit-Protokollen"](#) Finden Sie weitere Informationen.

Verwenden Sie Prometheus-Kennzahlen

Optional können Sie mit den Prometheus-Kennzahlen Berichte über die Mandantenaktivität erstellen.

- Wählen Sie im Grid Manager die Option **SUPPORT > Tools > Metriken**. Kunden können vorhandene Dashboards wie S3 Overview zur Überprüfung von Client-Aktivitäten nutzen.



Die auf der Seite Metriken verfügbaren Tools sind in erster Linie für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig.

- Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**. Sie können die Kennzahlen im Abschnitt „Kennzahlen“ der Grid Management API verwenden, um benutzerdefinierte Alarmregeln und Dashboards für Mandantenaktivitäten zu erstellen.

Siehe ["Prüfen von Support-Kennzahlen"](#) Finden Sie weitere Informationen.

Monitoring von Lastverteilungsvorgängen

Wenn Sie zum Verwalten von Client-Verbindungen zu StorageGRID einen Load Balancer verwenden, sollten Sie die Lastausgleichvorgänge überwachen, nachdem Sie das System zunächst und nachdem Sie Konfigurationsänderungen vorgenommen oder eine Erweiterung durchgeführt haben.

Über diese Aufgabe

Sie können den Load Balancer-Dienst auf Admin-Nodes oder Gateway-Nodes oder einen externen Load Balancer von Drittanbietern verwenden, um Clientanforderungen über mehrere Storage-Nodes zu verteilen.

Nach der Konfiguration des Lastausgleichs sollten Sie bestätigen, dass Einspeisung und Abruf von Objekten gleichmäßig über Storage Nodes verteilt werden. Gleichmäßig verteilte Anfragen stellen sicher, dass StorageGRID weiterhin auf die Workload-Anforderungen reagiert und die Client-Performance erhalten kann.

Wenn Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit) von Gateway Nodes oder Admin-Nodes im aktiv-Backup-Modus konfiguriert haben, verteilt nur ein Node in der Gruppe aktiv die Client-Anforderungen.

Weitere Informationen finden Sie unter ["Konfiguration von S3- und Swift-Client-Verbindungen"](#).

Schritte

1. Wenn sich S3- oder Swift-Clients über den Load Balancer Service verbinden, überprüfen Sie, ob Admin-Nodes oder Gateway-Nodes den Datenverkehr aktiv verteilen, wie Sie erwarten:
 - a. Wählen Sie **KNOTEN**.
 - b. Wählen Sie einen Gateway-Node oder einen Admin-Node aus.
 - c. Prüfen Sie auf der Registerkarte **Übersicht**, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle Primary hat.

Nodes mit der Rolle „Primär“ und Nodes, die sich nicht in einer HA-Gruppe befinden, sollten Anforderungen aktiv an die Clients verteilen.

- d. Wählen Sie für jeden Knoten, der Clientanforderungen aktiv verteilen soll, die aus ["Registerkarte Load Balancer"](#).

- e. Überprüfen Sie die Tabelle für den Datenverkehr der Lastverteilungsanforderung für die letzte Woche, um sicherzustellen, dass der Knoten die Anforderungen aktiv verteilt hat.

Nodes in einer aktiv-Backup-HA-Gruppe können die Backup-Rolle von Zeit zu Zeit übernehmen. Während dieser Zeit verteilen die Nodes keine Client-Anforderungen.

- f. Prüfen Sie das Diagramm der eingehenden Lastbalancer-Anfragerate für die letzte Woche, um den Objektdurchsatz des Nodes zu überprüfen.
- g. Wiederholen Sie diese Schritte für jeden Admin-Node oder Gateway-Node im StorageGRID-System.
- h. Optional können Sie mithilfe von Traffic-Klassifizierungsrichtlinien eine detailliertere Analyse des Datenverkehrs anzeigen, der vom Load Balancer Service bedient wird.

2. Stellen Sie sicher, dass diese Anfragen gleichmäßig auf Speicherknoten verteilt werden.

- a. Wählen Sie **Storage Node > LDR > HTTP** aus.
- b. Überprüfen Sie die Anzahl der **derzeit festgelegten eingehenden Sitzungen**.
- c. Wiederholen Sie diesen Vorgang für jeden Speicherknoten im Raster.

Die Anzahl der Sitzungen sollte ungefähr auf allen Storage-Nodes gleich sein.

Überwachen von Netzverbundverbindungen

Sie können grundlegende Informationen zu allen überwachen "[Netzverbundverbindungen](#)", Detaillierte Informationen über eine bestimmte Verbindung, oder Prometheus Metriken über Grid-übergreifende Replikationsvorgänge. Sie können eine Verbindung von beiden Rastergittern aus überwachen.

Bevor Sie beginnen

- Sie sind auf beiden Rastergittern mit einem beim Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Root-Zugriffsberechtigung für das Raster, bei dem Sie angemeldet sind.

Alle Verbindungen anzeigen

Die Seite Grid Federation enthält grundlegende Informationen zu allen Grid-Verbundverbindungen und zu allen Mandantenkonten, die für die Nutzung von Grid-Verbundverbindungen zugelassen sind.

Schritte

1. Wählen Sie **CONFIGURATION > System > Grid Federation**.

Die Seite Grid Federation wird angezeigt.

2. Um grundlegende Informationen für alle Verbindungen in diesem Raster anzuzeigen, wählen Sie die Registerkarte **Connections**.

Über diese Registerkarte können Sie:

- "[Erstellen Sie eine neue Verbindung](#)".
- Wählen Sie eine vorhandene Verbindung zu aus "[Bearbeiten oder testen](#)".

Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

Connections
Permitted tenants

Add connection
Upload verification file
Actions ▾

Search...

🔍
Displaying 1 connection

Connection name ▾	Remote hostname ? ▾	Connection status ? ▾
🔵 Grid 1 - Grid 2	10.96.130.76	🟢 Connected

3. Um grundlegende Informationen für alle Mandantenkonten in diesem Raster anzuzeigen, die über die Berechtigung **Grid Federation connection** verfügen, wählen Sie die Registerkarte **zulässige Mieter**.

Über diese Registerkarte können Sie:

- ["Zeigen Sie die Detailseite für jeden zulässigen Mandanten an"](#).
- Zeigen Sie die Detailseite für jede Verbindung an. Siehe [Zeigen Sie eine bestimmte Verbindung an](#).
- Wählen Sie eine zulässige Serviceeinheit und aus ["Entfernen Sie die Berechtigung"](#).
- Überprüfen Sie die Grid-übergreifende Replikation, und löschen Sie ggf. den letzten Fehler. Siehe ["Fehler beim Grid-Verbund beheben"](#).

Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

Connections
Permitted tenants

Remove permission
Clear error

Search...

🔍
Displaying one result

Tenant name ▾	Connection name ▾	Connection status ? ▾	Remote grid hostname ? ▾	Last error ? ▾
🔵 Tenant A	Grid 1 - Grid 2	🟢 Connected	10.96.130.76	Check for errors

eine bestimmte Verbindung anzeigen

Sie können Details für eine bestimmte Grid Federation-Verbindung anzeigen.

Schritte

1. Wählen Sie auf der Seite Grid Federation eine der beiden Registerkarten aus, und wählen Sie dann den Verbindungsnamen aus der Tabelle aus.

Auf der Detailseite für die Verbindung können Sie:

- Hier finden Sie grundlegende Statusinformationen zur Verbindung, einschließlich der lokalen und Remote-Hostnamen, des Ports und des Verbindungsstatus.

- Wählen Sie eine Verbindung zu aus "[Bearbeiten, testen oder entfernen](#)".
2. Wenn Sie eine bestimmte Verbindung anzeigen, wählen Sie die Registerkarte **zulässige Mandanten**, um Details über die zulässigen Tenants für die Verbindung anzuzeigen.

Über diese Registerkarte können Sie:

- "[Zeigen Sie die Detailseite für jeden zulässigen Mandanten an](#)".
- "[Entfernen Sie die Berechtigung eines Mandanten](#)" Um die Verbindung zu verwenden.
- Überprüfen Sie auf Grid-übergreifende Replikationsfehler, und löschen Sie den letzten Fehler. Siehe "[Fehler beim Grid-Verbund beheben](#)".

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64
Port: 23000
Remote hostname (other grid): 10.96.130.76
Connection status: ✔ Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

Permitted tenants [Certificates](#)

[Remove permission](#) [Clear error](#) Displaying one result

Tenant name	Last error
● Tenant A	Check for errors

3. Wenn Sie eine bestimmte Verbindung anzeigen, wählen Sie die Registerkarte **Zertifikate**, um die vom System generierten Server- und Client-Zertifikate für diese Verbindung anzuzeigen.

Über diese Registerkarte können Sie:

- "[Verbindungszertifikate drehen](#)".
- Wählen Sie **Server** oder **Client**, um das zugehörige Zertifikat anzuzeigen oder herunterzuladen oder das Zertifikat PEM zu kopieren.

Grid A-Grid B

Local hostname (this grid): 10.96.106.230
Port: 23000
Remote hostname (other grid): 10.96.104.230
Connection status:  Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Rotate certificates

Server

Client

Download certificate

Copy certificate PEM

Metadata

Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230
Serial number: 30:81:B8:DD:AE:B2:86:0A
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT
Issued on: 2022-10-04T02:21:18.000Z
Expires on: 2024-10-03T19:05:13.000Z
SHA-1 fingerprint: 92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF
SHA-256 fingerprint: 54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60
Alternative names: IP Address:10.96.106.230

Certificate PEM

```
-----BEGIN CERTIFICATE-----  
MIIGdTCCBF2gAwIBAgIIMIG43a6yhgowDQYJKoZIhvcNAQENBQAwZELMAkGA1UE  
BhMCVVMxExEzARBgNVBAGMCkNhbg1mb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEU  
MBEwDQYJKoZIhvcNAQENBQAwZELMAkGA1UEBhMCVVMxExEzARBgNVBAGMCkNhbg1mb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEU
```

Grid-übergreifende Replizierungsmetriken prüfen

Über das Cross-Grid Replication Dashboard in Grafana können Sie Prometheus-Metriken zu Grid-übergreifenden Replikationsvorgängen auf Ihrem Grid anzeigen.

Schritte

1. Wählen Sie im Grid Manager **SUPPORT > Tools > Metrics**.



Die auf der Seite Metriken verfügbaren Tools sind für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe Liste von "[Häufig verwendete Prometheus-Kennzahlen](#)".

2. Wählen Sie im Abschnitt Grafana der Seite **Cross Grid Replication** aus.

Ausführliche Anweisungen finden Sie unter "[Prüfen von Support-Kennzahlen](#)".

- Informationen zum erneuten Replizieren von Objekten, die nicht repliziert werden konnten, finden Sie unter ["Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut"](#).

Anwendung von Hotfixes oder ggf. Upgrade-Software

Wenn ein Hotfix oder eine neue Version der StorageGRID-Software verfügbar ist, sollten Sie prüfen, ob das Update für Ihr System geeignet ist, und installieren Sie es, falls erforderlich.

Über diese Aufgabe

StorageGRID Hotfixes enthalten Software-Änderungen, die außerhalb einer Feature- oder Patch-Freigabe verfügbar gemacht werden. Die gleichen Änderungen sind in einer zukünftigen Version enthalten.

Schritte

- Gehen Sie zu [https://mysupport.netapp.com/site/products/all/details/storagegrid/downloads-tab\[\"NetApp Downloads: StorageGRID\"\]](https://mysupport.netapp.com/site/products/all/details/storagegrid/downloads-tab[\).
- Wählen Sie den Abwärtspfeil für das Feld **Typ/Version auswählen** aus, um eine Liste der zum Herunterladen verfügbaren Aktualisierungen anzuzeigen:
 - StorageGRID Software-Versionen:** 11.x.y
 - StorageGRID Hotfixes:** 11.x. y.y.z
- Überprüfen Sie die Änderungen, die im Update enthalten sind:
 - Wählen Sie die Version aus dem Menü und wählen Sie **Go**.
 - Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
 - Lesen und akzeptieren Sie die Endnutzer-Lizenzvereinbarung.

Die Download-Seite für die ausgewählte Version wird angezeigt.

- Erfahren Sie mehr über die Änderungen in der Softwareversion oder Hotfix.
 - Informationen zu einer neuen Softwareversion finden Sie unter ["Was ist neu"](#) Für die ausgewählte Version.
 - Für einen Hotfix laden Sie die README-Datei herunter, um eine Zusammenfassung der Änderungen im Hotfix zu erhalten.
- Wenn Sie entscheiden, dass ein Softwareupdate erforderlich ist, suchen Sie die Anweisungen, bevor Sie fortfahren.
 - Für eine neue Softwareversion befolgen Sie die Anweisungen für ["Software wird aktualisiert"](#).
 - Informationen zu einem Hotfix finden Sie im ["StorageGRID Hotfix Verfahren"](#).

Überwachen Sie die Archivierungskapazität

Sie können die Kapazität eines externen Archiv-Storage-Systems nicht direkt über das StorageGRID System überwachen. Sie können jedoch überwachen, ob der Archiv-Node dennoch Objektdaten an das Archivierungsziel senden kann. Dies kann darauf hindeuten, dass eine Erweiterung der Archivierungsmedien erforderlich ist.

Über diese Aufgabe

Sie können die Store-Komponente überwachen, um zu überprüfen, ob der Archiv-Node weiterhin Objektdaten an das Ziel-Archiv-Storage-System senden kann. Der ARVF-Alarm (Store Failures) zeigt möglicherweise auch

an, dass das Zielspeichersystem die Kapazität erreicht hat und keine Objektdaten mehr annehmen kann.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Übersicht > Main**.
3. Überprüfen Sie die Attribute „Speicherstatus“ und „Speicherstatus“, um zu bestätigen, dass die Komponente „Speicher“ ohne Fehler online ist.

Component	State	Status	Icons
ARC State:	Online		[Server Icon] [Green Checkmark]
ARC Status:	No Errors		[Server Icon] [Green Checkmark]
Tivoli Storage Manager State:	Online		[Server Icon] [Green Checkmark]
Tivoli Storage Manager Status:	No Errors		[Server Icon] [Green Checkmark]
Store State:	Online		[Server Icon] [Green Checkmark]
Store Status:	No Errors		[Server Icon] [Green Checkmark]
Retrieve State:	Online		[Server Icon] [Green Checkmark]
Retrieve Status:	No Errors		[Server Icon] [Green Checkmark]
Inbound Replication Status:	No Errors		[Server Icon] [Green Checkmark]
Outbound Replication Status:	No Errors		[Server Icon] [Green Checkmark]

Eine Offline-Store-Komponente oder eine Komponente mit Fehlern weist möglicherweise darauf hin, dass das Ziel-Archivspeichersystem Objektdaten nicht mehr akzeptieren kann, da die Kapazität erreicht ist.

Alarmer und Alarme

Alarmer und Alarme verwalten: Übersicht

Das StorageGRID Alert System wurde entwickelt, um Sie über betriebliche Probleme zu informieren, die Ihre Aufmerksamkeit erfordern. Das alte Alarmsystem ist veraltet.

Meldungssystem

Das Alarmsystem wurde als Ihr vorrangiges Tool entwickelt, mit dem Sie alle eventuell auftretenden Probleme in Ihrem StorageGRID System überwachen können. Das Alarmsystem bietet eine benutzerfreundliche Oberfläche zum Erkennen, Bewerten und Beheben von Problemen.

Warnmeldungen werden auf bestimmten Schweregraden ausgelöst, wenn Alarmregelbedingungen als wahr bewertet werden. Wenn eine Meldung ausgelöst wird, treten die folgenden Aktionen auf:

- Im Grid Manager wird ein Symbol für den Schweregrad der Warnmeldung im Dashboard angezeigt, und die Anzahl der aktuellen Warnmeldungen wird erhöht.
- Die Warnmeldung wird auf der Seite **NODES** Zusammenfassung und auf der Registerkarte **NODES > Node > Übersicht** angezeigt.
- Es wird eine E-Mail-Benachrichtigung gesendet, vorausgesetzt, Sie haben einen SMTP-Server konfiguriert und E-Mail-Adressen für die Empfänger bereitgestellt.

- Es wird eine SNMP-Benachrichtigung (Simple Network Management Protocol) gesendet, vorausgesetzt, Sie haben den StorageGRID SNMP-Agent konfiguriert.

Altes Alarmsystem

Wie bei Warnungen werden auch Alarme mit bestimmten Schweregraden ausgelöst, wenn Attribute definierte Schwellenwerte erreichen. Im Gegensatz zu Warnmeldungen werden jedoch viele Alarme für Ereignisse ausgelöst, die Sie sicher ignorieren können, was zu einer übermäßigen Anzahl an E-Mail- oder SNMP-Benachrichtigungen führen kann.



Das Alarmsystem ist veraltet und wird in einer zukünftigen Version entfernt. Wenn Sie weiterhin ältere Alarme verwenden, sollten Sie so schnell wie möglich auf das Alarmsystem umstellen.

Wenn ein Alarm ausgelöst wird, treten folgende Aktionen auf:

- Der Alarm wird auf der Seite **SUPPORT > Alarme (alt) > Aktuelle Alarme** angezeigt.
- Es wird eine E-Mail-Benachrichtigung gesendet, vorausgesetzt, Sie haben einen SMTP-Server konfiguriert und eine oder mehrere Mailinglisten konfiguriert.
- Es kann eine SNMP-Benachrichtigung gesendet werden, vorausgesetzt, Sie haben den StorageGRID SNMP-Agent konfiguriert. (SNMP-Benachrichtigungen werden nicht für alle Alarme oder Alarmgrenzen gesendet.)

Vergleichen von Warnungen und Alarmen

Es gibt mehrere Ähnlichkeiten zwischen dem Alarmsystem und dem alten Alarmsystem, aber das Alarmsystem bietet erhebliche Vorteile und ist einfacher zu bedienen.

In der folgenden Tabelle erfahren Sie, wie Sie ähnliche Vorgänge ausführen.

	Meldungen	Alarme (Altsystem)
Wie sehe ich, welche Alarme oder Alarme aktiv sind?	<ul style="list-style-type: none"> • Wählen Sie den Link Aktuelle Alarme auf dem Dashboard aus. • Wählen Sie die Warnmeldung auf der Seite NODES > Übersicht aus. • Wählen Sie ALERTS > Current. <p>"Anzeigen aktueller Warnmeldungen"</p>	<p>Wählen Sie SUPPORT > Alarme (alt) > Aktueller Alarm aus.</p> <p>"Verwalten von Alarmen (Altsystem)"</p>
Was bewirkt, dass eine Warnung oder ein Alarm ausgelöst wird?	<p>Alarme werden ausgelöst, wenn ein Prometheus-Ausdruck in einer Alarmregel für die spezifische Triggerbedingung und -Dauer als wahr bewertet wird.</p> <p>"Zeigen Sie Alarmregeln an"</p>	<p>Alarme werden ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht.</p> <p>"Verwalten von Alarmen (Altsystem)"</p>

	Meldungen	Alarmer (Altsystem)
Wie kann ich das zugrunde liegende Problem lösen, wenn eine Meldung oder ein Alarm ausgelöst wird?	<p>Die empfohlenen Aktionen für eine Warnmeldung sind in E-Mail-Benachrichtigungen enthalten und stehen auf den Alerts-Seiten im Grid Manager zur Verfügung.</p> <p>Falls erforderlich, werden weitere Informationen in der StorageGRID-Dokumentation bereitgestellt.</p> <p>"Alerts Referenz"</p>	<p>Sie können sich über einen Alarm informieren, indem Sie den Attributnamen auswählen oder in der StorageGRID-Dokumentation nach einem Alarmcode suchen.</p> <p>"Alarmreferenz (Altsystem)"</p>
Wo kann ich eine Liste der Alarmer oder Alarmer sehen, die gelöst wurden?	<p>Wählen Sie ALARME > aufgelöst.</p> <p>"Anzeige aktueller und aufgelöster Warnmeldungen"</p>	<p>Wählen Sie SUPPORT > Alarmer (alt) > Historische Alarmer.</p> <p>"Verwalten von Alarmen (Altsystem)"</p>
Wo kann ich die Einstellungen verwalten?	<p>Wählen Sie ALERTS > Rules.</p> <p>"Verwalten von Meldungen"</p>	<p>Wählen Sie SUPPORT. Verwenden Sie dann die Optionen im Abschnitt Alarmer (alt) des Menüs.</p> <p>"Verwalten von Alarmen (Altsystem)"</p>
Welche Benutzergruppenberechtigungen brauche ich?	<ul style="list-style-type: none"> • Jeder, der sich beim Grid Manager anmelden kann, kann aktuelle und behobene Warnmeldungen anzeigen. • Sie müssen über die Berechtigung zum Verwalten von Warnmeldungen verfügen, um Stille, Warnmeldungen und Warnungsregeln zu verwalten. <p>"StorageGRID verwalten"</p>	<ul style="list-style-type: none"> • Jeder, der sich beim Grid Manager anmelden kann, kann ältere Alarmer anzeigen. • Sie müssen über die Berechtigung zum Quittieren von Alarmen verfügen, um Alarmer bestätigen zu können. • Sie müssen sowohl über die Konfiguration der Seite „Grid-Topologie“ als auch über andere Berechtigungen für die Rasterkonfiguration verfügen, um globale Alarmer und E-Mail-Benachrichtigungen verwalten zu können. <p>"StorageGRID verwalten"</p>

	Meldungen	Alarme (Altsystem)
Wie managt ich E-Mail-Benachrichtigungen?	<p>Wählen Sie ALERTS > Email Setup.</p> <p>Hinweis: Da Alarme und Alarme unabhängige Systeme sind, wird das E-Mail-Setup für Alarm- und AutoSupport-Benachrichtigungen nicht für Benachrichtigungen verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden.</p> <p>"Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"</p>	<p>Wählen Sie SUPPORT > Alarme (alt) > Legacy E-Mail-Einrichtung.</p> <p>"Verwalten von Alarmen (Altsystem)"</p>
Wie verwalte ich SNMP Benachrichtigungen?	<p>Wählen Sie KONFIGURATION > Überwachung > SNMP-Agent.</p> <p>"Verwenden Sie SNMP-Überwachung"</p>	<i>Nicht unterstützt</i>
Wie kontrolliere ich, wer Benachrichtigungen erhält?	<ol style="list-style-type: none"> 1. Wählen Sie ALERTS > Email Setup. 2. Geben Sie im Abschnitt Empfänger eine E-Mail-Adresse für jede E-Mail-Liste oder Person ein, die eine E-Mail erhalten soll, wenn eine Benachrichtigung erfolgt. <p>"Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"</p>	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Alarme (alt) > Legacy E-Mail-Einrichtung. 2. Mailingliste wird erstellt. 3. Wählen Sie Benachrichtigungen. 4. Wählen Sie die Mailingliste aus. <p>"Verwalten von Alarmen (Altsystem)"</p>
Welche Admin Nodes senden Benachrichtigungen?	<p>Ein einzelner Admin-Knoten (der bevorzugte Absender).</p> <p>"Was ist ein Admin-Node?"</p>	<p>Ein einzelner Admin-Knoten (der bevorzugte Absender).</p> <p>"Was ist ein Admin-Node?"</p>

	Meldungen	Alarme (Altsystem)
Wie kann ich einige Benachrichtigungen unterdrücken?	<ol style="list-style-type: none"> 1. Wählen Sie ALARME > Stille. 2. Wählen Sie die Alarmregel aus, die stummschalten soll. 3. Geben Sie eine Dauer für die Stille an. 4. Wählen Sie den Schweregrad der Warnmeldung aus, den Sie stummschalten möchten. 5. Wählen Sie diese Option aus, um die Stille auf das gesamte Raster, einen einzelnen Standort oder einen einzelnen Knoten anzuwenden. <p>Hinweis: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren.</p> <p>"Benachrichtigung über Stille"</p>	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Alarme (alt) > Legacy E-Mail-Einrichtung. 2. Wählen Sie Benachrichtigungen. 3. Wählen Sie eine Mailingliste aus, und wählen Sie unterdrücken. <p>"Verwalten von Alarmen (Altsystem)"</p>
Wie kann ich alle Benachrichtigungen unterdrücken?	<p>Wählen Sie ALARME > Stille und dann Alle Regeln.</p> <p>Hinweis: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren.</p> <p>"Benachrichtigung über Stille"</p>	<i>Nicht unterstützt</i>
Wie kann ich die Bedingungen und Trigger anpassen?	<ol style="list-style-type: none"> 1. Wählen Sie ALERTS > Rules. 2. Wählen Sie eine Standardregel zum Bearbeiten aus, oder wählen Sie benutzerdefinierte Regel erstellen. <p>"Bearbeiten von Meldungsregeln"</p> <p>"Erstellen benutzerdefinierter Warnungsregeln"</p>	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Alarme (alt) > Globale Alarme. 2. Erstellen Sie einen globalen benutzerdefinierten Alarm, um einen Standardalarm zu überschreiben oder ein Attribut zu überwachen, das keinen Standardalarm hat. <p>"Verwalten von Alarmen (Altsystem)"</p>

	Meldungen	Alarme (Altsystem)
Wie deaktiviere ich eine einzelne Warnung oder einen einzelnen Alarm?	<ol style="list-style-type: none"> 1. Wählen Sie ALERTS > Rules. 2. Wählen Sie die Regel aus, und wählen Sie Regel bearbeiten. 3. Deaktivieren Sie das Kontrollkästchen aktiviert. <p>"Deaktivieren von Meldungsregeln"</p>	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Alarme (alt) > Globale Alarme. 2. Wählen Sie die Regel aus, und wählen Sie das Symbol Bearbeiten aus. 3. Deaktivieren Sie das Kontrollkästchen aktiviert. <p>"Verwalten von Alarmen (Altsystem)"</p>

Verwalten von Meldungen

Benachrichtigungen verwalten: Übersicht

Das Warnsystem bietet eine benutzerfreundliche Oberfläche zum Erkennen, Bewerten und Beheben von Problemen, die während des StorageGRID-Betriebs auftreten können.

Sie können benutzerdefinierte Warnmeldungen erstellen, Warnmeldungen bearbeiten oder deaktivieren und Warnmeldungen verwalten.

Weitere Informationen:

- Sehen Sie sich das Video an: ["Video: Übersicht über Warnmeldungen für StorageGRID 11.7"](#)



- Sehen Sie sich das Video an: ["Video: Verwendung von Kennzahlen zum Erstellen von benutzerdefinierten Warnmeldungen in StorageGRID 11.7"](#)



- Siehe ["Alerts Referenz"](#).

Zeigen Sie Alarmregeln an

Alarmregeln definieren die Bedingungen, die ausgelöst werden "[Spezifische Warnmeldungen](#)". StorageGRID enthält eine Reihe von Standardwarnregeln, die Sie unverändert verwenden oder ändern können, oder Sie können individuelle Alarmregeln erstellen.

Sie können die Liste aller Standard- und benutzerdefinierten Warnungsregeln anzeigen, um zu erfahren, welche Bedingungen die einzelnen Warnmeldungen auslösen und feststellen, ob Meldungen deaktiviert sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff.
- Optional haben Sie sich das Video angesehen: "[Video: Übersicht über Warnmeldungen für StorageGRID 11.7](#)"



Schritte

1. Wählen Sie **ALERTS > Rules**.

Die Seite Alarmregeln wird angezeigt.

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

+ Create custom rule Edit rule Remove custom rule			
Name	Conditions	Type	Status
<input type="radio"/> Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") <i>Major</i> > 0	Default	Enabled
<input type="radio"/> Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") <i>Major</i> > 0	Default	Enabled

Displaying 62 alert rules.

2. Die Informationen in der Tabelle mit den Alarmregeln prüfen:

Spaltenüberschrift	Beschreibung
Name	Der eindeutige Name und die Beschreibung der Warnungsregel. Benutzerdefinierte Alarmregeln werden zuerst aufgeführt, gefolgt von Standardwarnregeln. Der Name der Alarmregel ist Betreff für E-Mail-Benachrichtigungen.

Spaltenüberschrift	Beschreibung
Bestimmten Bedingungen	<p>Die Prometheus Ausdrücke, die bestimmen, wann diese Warnung ausgelöst wird. Eine Meldung kann auf einem oder mehreren der folgenden Schweregrade ausgelöst werden, jedoch ist für jeden Schweregrad ein Zustand nicht erforderlich.</p> <ul style="list-style-type: none"> • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. • Major : Es besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. • Klein : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die nicht von selbst geklärt werden, um sicherzustellen, dass sie nicht zu einem schwerwiegenden Problem führen.
Typ	<p>Der Typ der Warnregel:</p> <ul style="list-style-type: none"> • Standard: Eine mit dem System bereitgestellte Warnregel. Sie können eine Standardwarnregel deaktivieren oder die Bedingungen und Dauer für eine Standardwarnregel bearbeiten. Eine Standard-Warnungsregel kann nicht entfernt werden. • Standard*: Eine Standardwarnregel, die eine bearbeitete Bedingung oder Dauer enthält. Bei Bedarf können Sie eine geänderte Bedingung ganz einfach wieder auf die ursprüngliche Standardeinstellung zurücksetzen. • Benutzerdefiniert: Eine Alarmregel, die Sie erstellt haben. Sie können benutzerdefinierte Alarmregeln deaktivieren, bearbeiten und entfernen.
Status	<p>Gibt an, ob diese Warnungsregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnungsregeln werden nicht ausgewertet, sodass keine Warnmeldungen ausgelöst werden.</p>

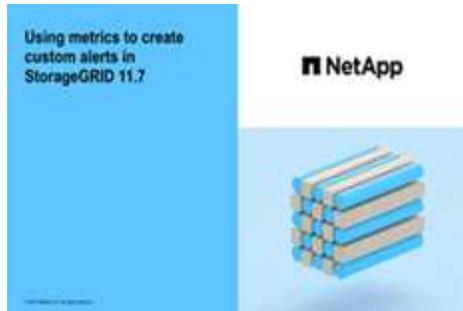
Erstellen benutzerdefinierter Warnungsregeln

Sie können benutzerdefinierte Alarmregeln erstellen, um eigene Bedingungen für das Auslösen von Warnmeldungen zu definieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)"

- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff
- Sie kennen das "[Häufig verwendete Prometheus-Kennzahlen](#)"
- Sie verstehen den "[Syntax der Prometheus-Abfragen](#)"
- Optional haben Sie sich das Video angesehen: "[Video: Verwendung von Kennzahlen zum Erstellen von benutzerdefinierten Warnmeldungen in StorageGRID 11.7](#)"



Über diese Aufgabe

StorageGRID validiert keine benutzerdefinierten Warnmeldungen. Wenn Sie sich für die Erstellung benutzerdefinierter Warnungsregeln entscheiden, befolgen Sie die folgenden allgemeinen Richtlinien:

- Informieren Sie sich über die Bedingungen für die Standardwarnregeln und verwenden Sie sie als Beispiele für Ihre benutzerdefinierten Warnungsregeln.
- Wenn Sie mehrere Bedingungen für eine Warnungsregel definieren, verwenden Sie denselben Ausdruck für alle Bedingungen. Ändern Sie dann den Schwellenwert für jede Bedingung.
- Prüfen Sie jede Bedingung sorgfältig auf Tippfehler und Logikfehler.
- Verwenden Sie nur die in der Grid Management API aufgeführten Metriken.
- Beachten Sie beim Testen eines Ausdrucks mit der Grid Management API, dass eine „successful“-Antwort möglicherweise ein leerer Antworttext ist (keine Warnung ausgelöst). Um zu überprüfen, ob die Meldung tatsächlich ausgelöst wird, können Sie vorübergehend einen Schwellenwert auf einen Wert festlegen, der Ihrer Meinung nach derzeit „true“ ist.

Zum Beispiel zum Testen des Ausdrucks `node_memory_MemTotal_bytes < 24000000000`, Erste Ausführung `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 gewünschten Werte und führen Sie die Ausführung erneut aus. Keine Ergebnisse zeigen an, dass für diesen Ausdruck keine aktuellen Warnmeldungen vorhanden sind.

- Gehen Sie nicht davon aus, dass eine benutzerdefinierte Warnung funktioniert, es sei denn, Sie haben bestätigt, dass die Warnmeldung erwartungsgemäß ausgelöst wird.

Schritte

1. Wählen Sie **ALERTS > Rules**.

Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie **eigene Regel erstellen**.

Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.

Create Custom Rule

Enabled

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

Cancel

Save

3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **enabled**, um zu bestimmen, ob diese Warnungsregel aktuell aktiviert ist.

Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.

4. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Alarmregel wird auf der Seite „Meldungen“ angezeigt und ist außerdem Betreff für E-Mail-Benachrichtigungen. Die Namen für Warnungsregeln können zwischen 1 und 64 Zeichen umfassen.

Feld	Beschreibung
Beschreibung	Eine Beschreibung des Problems. Die Beschreibung ist die auf der Seite „Meldungen“ und in E-Mail-Benachrichtigungen angezeigte Warnmeldung. Die Beschreibungen für Warnungsregeln können zwischen 1 und 128 Zeichen umfassen.
Empfohlene Maßnahmen	Optional sind die zu ergriffenen Maßnahmen verfügbar, wenn diese Meldung ausgelöst wird. Geben Sie empfohlene Aktionen als Klartext ein (keine Formatierungscodes). Die empfohlenen Aktionen für Warnungsregeln können zwischen 0 und 1,024 Zeichen liegen.

5. Geben Sie im Abschnitt Bedingungen einen Prometheus-Ausdruck für eine oder mehrere der Schweregrade für Warnmeldungen ein.

Ein Grundausdruck ist in der Regel die Form:

```
[metric] [operator] [value]
```

Ausdrücke können eine beliebige Länge haben, aber in einer einzigen Zeile in der Benutzeroberfläche angezeigt werden. 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** den Zeitraum ein, den eine Bedingung kontinuierlich wirksam bleiben muss, bevor die Warnung ausgelöst wird, und wählen Sie eine Zeiteinheit aus.

Um sofort eine Warnung auszulösen, wenn eine Bedingung wahr wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass temporäre Bedingungen Warnungen auslösen.

Der Standardwert ist 5 Minuten.

7. Wählen Sie **Speichern**.

Das Dialogfeld wird geschlossen, und die neue benutzerdefinierte Alarmregel wird in der Tabelle Alarmregeln angezeigt.

Bearbeiten von Meldungsregeln

Sie können eine Meldungsregel bearbeiten, um die Triggerbedingungen zu ändern. Für eine benutzerdefinierte Warnungsregel können Sie auch den Regelnamen, die Beschreibung und die empfohlenen Aktionen aktualisieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff.

Über diese Aufgabe

Wenn Sie eine standardmäßige Warnungsregel bearbeiten, können Sie die Bedingungen für kleinere, größere und kritische Warnmeldungen sowie die Dauer ändern. Wenn Sie eine benutzerdefinierte Alarmregel bearbeiten, können Sie auch den Namen, die Beschreibung und die empfohlenen Aktionen der Regel bearbeiten.



Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnungsregel zu bearbeiten. Wenn Sie die Triggerwerte ändern, können Sie möglicherweise ein zugrunde liegendes Problem erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

Schritte

1. Wählen Sie **ALERTS > Rules**.

Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie das Optionsfeld für die Alarmregel, die Sie bearbeiten möchten.
3. Wählen Sie **Regel bearbeiten**.

Das Dialogfeld Regel bearbeiten wird angezeigt. Dieses Beispiel zeigt eine Standard-Alarmregel: Die Felder eindeutiger Name, Beschreibung und Empfohlene Aktionen sind deaktiviert und können nicht bearbeitet werden.

Edit Rule - Low installed node memory

Enabled

Unique Name

Description

Recommended Actions (optional)

Conditions ?

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **enabled**, um zu bestimmen, ob diese Warnungsregel aktuell aktiviert ist.

Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.



Wenn Sie die Meldungsregel für eine aktuelle Meldung deaktivieren, müssen Sie einige Minuten warten, bis die Meldung nicht mehr als aktive Meldung angezeigt wird.



Im Allgemeinen wird es nicht empfohlen, eine Standardwarnregel zu deaktivieren. Wenn eine Meldungsregel deaktiviert ist, kann ein zugrunde liegendes Problem möglicherweise erst erkannt werden, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

5. Aktualisieren Sie für benutzerdefinierte Warnungsregeln die folgenden Informationen, falls erforderlich.



Sie können diese Informationen für Standard-Warnungsregeln nicht bearbeiten.

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Alarmregel wird auf der Seite „Meldungen“ angezeigt und ist außerdem Betreff für E-Mail-Benachrichtigungen. Die Namen für Warnungsregeln können zwischen 1 und 64 Zeichen umfassen.
Beschreibung	Eine Beschreibung des Problems. Die Beschreibung ist die auf der Seite „Meldungen“ und in E-Mail-Benachrichtigungen angezeigte Warnmeldung. Die Beschreibungen für Warnungsregeln können zwischen 1 und 128 Zeichen umfassen.
Empfohlene Maßnahmen	Optional sind die zu ergriffenen Maßnahmen verfügbar, wenn diese Meldung ausgelöst wird. Geben Sie empfohlene Aktionen als Klartext ein (keine Formatierungs-codes). Die empfohlenen Aktionen für Warnungsregeln können zwischen 0 und 1,024 Zeichen liegen.

6. Geben Sie im Abschnitt Bedingungen den Prometheus-Ausdruck für eine oder mehrere Schweregrade für Warnmeldungen ein oder aktualisieren Sie diesen.



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.

Conditions

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes < 2400000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes <= 1400000000"/>





Wenn Sie die Bedingungen für eine aktuelle Meldung aktualisieren, werden Ihre Änderungen möglicherweise erst implementiert, wenn der vorherige Zustand behoben ist. Wenn das nächste Mal eine der Bedingungen für die Regel erfüllt ist, zeigt die Warnmeldung die aktualisierten Werte an.

Ein Grundausrück ist in der Regel die Form:

```
[metric] [operator] [value]
```

Ausdrücke können eine beliebige Länge haben, aber in einer einzigen Zeile in der Benutzeroberfläche angezeigt werden. 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** den Zeitraum ein, den eine Bedingung kontinuierlich wirksam bleiben muss, bevor die Warnmeldung ausgelöst wird, und wählen Sie die Zeiteinheit aus.

Um sofort eine Warnung auszulösen, wenn eine Bedingung wahr wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass temporäre Bedingungen Warnungen auslösen.

Der Standardwert ist 5 Minuten.

8. Wählen Sie **Speichern**.

Wenn Sie eine Standardwarnregel bearbeitet haben, wird in der Spalte Typ **Standard*** angezeigt. Wenn Sie eine Standard- oder benutzerdefinierte Alarmregel deaktiviert haben, wird in der Spalte **Status deaktiviertes** angezeigt.

Deaktivieren von Meldungsregeln

Sie können den aktivierten/deaktivierten Status für eine Standard- oder eine benutzerdefinierte Warnungsregel ändern.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff.

Über diese Aufgabe

Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.



Im Allgemeinen wird es nicht empfohlen, eine Standardwarnregel zu deaktivieren. Wenn eine Meldungsregel deaktiviert ist, kann ein zugrunde liegendes Problem möglicherweise erst erkannt werden, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

Schritte

1. Wählen Sie **ALERTS > Rules**.

Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie das Optionsfeld für die Warnungsregel, die deaktiviert oder aktiviert werden soll.
3. Wählen Sie **Regel bearbeiten**.

Das Dialogfeld Regel bearbeiten wird angezeigt.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **enabled**, um zu bestimmen, ob diese Warnungsregel aktuell aktiviert ist.

Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.



Wenn Sie die Meldungsregel für eine aktuelle Meldung deaktivieren, müssen Sie einige Minuten warten, bis die Meldung nicht mehr als aktive Meldung angezeigt wird.

5. Wählen Sie **Speichern**.

Deaktiviert wird in der Spalte **Status** angezeigt.

Entfernen Sie benutzerdefinierte Warnungsregeln

Sie können eine benutzerdefinierte Alarmregel entfernen, wenn Sie sie nicht mehr verwenden möchten.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff.

Schritte

1. Wählen Sie **ALERTS > Rules**.

Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie das Optionsfeld für die benutzerdefinierte Alarmregel, die Sie entfernen möchten.

Eine Standard-Warnungsregel kann nicht entfernt werden.

3. Wählen Sie **Benutzerdefinierte Regel entfernen**.

Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie * OK* aus, um die Warnregel zu entfernen.

Alle aktiven Instanzen der Warnmeldung werden innerhalb von 10 Minuten behoben.

Verwalten von Warnmeldungen

Einrichten von SNMP-Benachrichtigungen für Warnmeldungen

Wenn StorageGRID SNMP-Benachrichtigungen senden soll, wenn Warnmeldungen auftreten, müssen Sie den StorageGRID SNMP-Agent aktivieren und ein oder mehrere Trap-Ziele konfigurieren.

Sie können die Option **CONFIGURATION > Monitoring > SNMP Agent** im Grid Manager oder die SNMP-Endpunkte für die Grid Management API verwenden, um den StorageGRID SNMP-Agent zu aktivieren und zu konfigurieren. Der SNMP-Agent unterstützt alle drei Versionen des SNMP-Protokolls.

Informationen zum Konfigurieren des SNMP-Agenten finden Sie unter ["Verwenden Sie SNMP-Überwachung"](#).

Nachdem Sie den StorageGRID SNMP-Agent konfiguriert haben, können zwei Arten von ereignisgesteuerten Benachrichtigungen gesendet werden:

- Traps sind Benachrichtigungen, die vom SNMP-Agenten gesendet werden und keine Bestätigung durch das Managementsystem erfordern. Traps dienen dazu, das Managementsystem über etwas innerhalb von StorageGRID zu informieren, wie z. B. eine Warnung, die ausgelöst wird. Traps werden in allen drei Versionen von SNMP unterstützt.
- Informationen sind ähnlich wie Traps, aber sie erfordern eine Bestätigung durch das Management-System. Wenn der SNMP-Agent innerhalb einer bestimmten Zeit keine Bestätigung erhält, wird die Benachrichtigung erneut gesendet, bis eine Bestätigung empfangen wurde oder der maximale Wiederholungswert erreicht wurde. Die Informationsunterstützung wird in SNMPv2c und SNMPv3 unterstützt.

Trap- und Informieren-Benachrichtigungen werden gesendet, wenn eine Standard- oder benutzerdefinierte Warnung auf einem Schweregrad ausgelöst wird. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, müssen Sie eine Stille für die Warnung konfigurieren. Siehe ["Benachrichtigung über Stille"](#).

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Nachrichten, SNMP-Traps und -Benachrichtigungen sowie ältere Alarmmeldungen. Wenn der primäre Admin-Node nicht mehr verfügbar ist, werden vorübergehend Benachrichtigungen von anderen Admin-Nodes gesendet. Siehe ["Was ist ein Admin-Node?"](#).

Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein

Wenn E-Mail-Benachrichtigungen gesendet werden sollen, wenn Warnmeldungen auftreten, müssen Sie Informationen über Ihren SMTP-Server angeben. Sie müssen auch E-Mail-Adressen für Empfänger von Benachrichtigungen eingeben.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff.

Über diese Aufgabe

Da es sich bei den Alarmen um unabhängige Systeme handelt, wird das E-Mail-Setup, das für Alarmbenachrichtigungen verwendet wird, nicht für Alarmbenachrichtigungen und AutoSupport-Meldungen verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden.

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Nachrichten, SNMP-Traps und -Benachrichtigungen sowie ältere Alarmmeldungen. Wenn der primäre Admin-Node nicht mehr verfügbar ist, werden vorübergehend Benachrichtigungen von anderen Admin-Nodes gesendet. Siehe ["Was ist ein Admin-Node?"](#).

Schritte

1. Wählen Sie **ALERTS > Email Setup**.

Die Seite E-Mail-Einrichtung wird angezeigt.

Email Setup

You can configure the email server for alert notifications, define filters to limit the number of notifications, and enter email addresses for alert recipients.

Use these settings to define the email server used for alert notifications. These settings are not used for alarm notifications and AutoSupport. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Enable Email Notifications

Save

2. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, um anzugeben, dass Benachrichtigungs-E-Mails gesendet werden sollen, wenn Benachrichtigungen 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	Eingabe
Mailserver	Der vollständig qualifizierte Domänenname (FQDN) oder die IP-Adresse des SMTP-Servers.
Port	Der Port, der für den Zugriff auf den SMTP-Server verwendet wird. Muss zwischen 1 und 65535 liegen.
Benutzername (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen ein, mit dem Sie sich authentifizieren möchten.
Kennwort (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie das Kennwort für die Authentifizierung ein.

Email (SMTP) Server

Mail Server	<input type="text" value="10.224.1.250"/>
Port	<input type="text" value="25"/>
Username (optional)	<input type="text" value="smtpuser"/>
Password (optional)	<input type="password" value="*****"/>

4. Geben Sie im Abschnitt E-Mail-Adressen die E-Mail-Adressen für den Absender und für jeden Empfänger ein.

- a. Geben Sie für die **Absender E-Mail-Adresse** eine gültige E-Mail-Adresse an, die als Absenderadresse für Benachrichtigungen verwendet werden soll.

Beispiel: `storagegrid-alerts@example.com`

- b. Geben Sie im Abschnitt Empfänger eine E-Mail-Adresse für jede E-Mail-Liste oder Person ein, die beim Auftreten einer Warnmeldung eine E-Mail erhalten soll.

Wählen Sie das Plus-Symbol **+** Um Empfänger hinzuzufügen.

Email Addresses

Sender Email Address 	<input type="text" value="storagegrid-alerts@example.com"/>	
Recipient 1 	<input type="text" value="recipient1@example.com"/>	
Recipient 2 	<input type="text" value="recipient2@example.com"/>	 

5. Wenn Transport Layer Security (TLS) für die Kommunikation mit dem SMTP-Server 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 Identifizierung des SMTP-Servers verwendet wird.

Sie können den Inhalt in dieses Feld kopieren und einfügen, oder wählen Sie **Durchsuchen** und wählen Sie die Datei aus.

Sie müssen eine einzelne Datei bereitstellen, die die Zertifikate jeder Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

- b. Aktivieren Sie das Kontrollkästchen **Client-Zertifikat senden**, wenn Ihr SMTP-E-Mail-Server E-Mail-Absender benötigt, um Clientzertifikate für die Authentifizierung bereitzustellen.
- c. Geben Sie im Feld **Client Certificate** das PEM-codierte Clientzertifikat an, das an den SMTP-Server gesendet werden kann.

Sie können den Inhalt in dieses Feld kopieren und einfügen, oder wählen Sie **Durchsuchen** und wählen Sie die Datei aus.

- d. Geben Sie im Feld **Private Key** den privaten Schlüssel für das Clientzertifikat in unverschlüsselter PEM-Codierung ein.

Sie können den Inhalt in dieses Feld kopieren und einfügen, oder wählen Sie **Durchsuchen** und wählen Sie die Datei aus.



Wenn Sie das E-Mail-Setup bearbeiten müssen, klicken Sie auf das Stift-Symbol, um dieses Feld zu aktualisieren.

Transport Layer Security (TLS)

Require TLS 

CA Certificate 

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Browse

Send Client Certificate 

Client Certificate 

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Browse

Private Key 

```
-----BEGIN PRIVATE KEY-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----BEGIN PRIVATE KEY-----
```

Browse

6. Wählen Sie im Abschnitt Filter aus, welche Alarmschweregrade zu E-Mail-Benachrichtigungen führen soll, es sei denn, die Regel für eine bestimmte Warnung wurde stummgeschaltet.

Schweregrad	Beschreibung
Klein, groß, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die kleine, größere oder kritische Bedingung für eine Alarmregel erfüllt wird.
Kritisch	Wenn die Hauptbedingung für eine Warnmeldung erfüllt ist, wird eine E-Mail-Benachrichtigung gesendet. Benachrichtigungen werden nicht für kleinere Warnmeldungen gesendet.

Schweregrad	Beschreibung
Nur kritisch	Eine E-Mail-Benachrichtigung wird nur gesendet, wenn die kritische Bedingung für eine Alarmregel erfüllt ist. Benachrichtigungen werden nicht für kleinere oder größere Warnmeldungen gesendet.

Filters

Severity  Minor, major, critical Major, critical Critical only

Send Test Email

Save

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 angibt, dass eine Test-E-Mail gesendet wurde.

b. Aktivieren Sie die Kontrollkästchen aller E-Mail-Empfänger, und bestätigen Sie, dass eine Test-E-Mail empfangen wurde.



Wenn die E-Mail nicht innerhalb weniger Minuten empfangen wird oder wenn die Meldung **E-Mail-Benachrichtigung Fehler** ausgelöst wird, überprüfen Sie Ihre Einstellungen und versuchen Sie es erneut.

c. Melden Sie sich bei anderen Admin-Knoten an und senden Sie eine Test-E-Mail, um die Verbindung von allen Standorten zu überprüfen.



Wenn Sie die Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Verbindung zu überprüfen. Dies steht im Gegensatz zum Testen von AutoSupport-Meldungen und älteren Alarmmeldungen, bei denen alle Admin-Knoten die Test-E-Mail senden.

8. Wählen Sie **Speichern**.

Beim Senden einer Test-E-Mail werden Ihre Einstellungen nicht gespeichert. Sie müssen **Speichern** wählen.

Die E-Mail-Einstellungen werden gespeichert.

Informationen, die in E-Mail-Benachrichtigungen für Warnmeldungen enthalten sind

Nachdem Sie den SMTP-E-Mail-Server konfiguriert haben, werden beim Auslösen einer Warnung E-Mail-Benachrichtigungen an die angegebenen Empfänger gesendet, es sei denn, die Alarmregel wird durch Stille unterdrückt. Siehe "[Benachrichtigung über Stille](#)".

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 4
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

DC1-S2-227

Node DC1-S2-227
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

Sent from: DC1-ADM1-225 5

Legende	Beschreibung
1	Der Name der Warnmeldung, gefolgt von der Anzahl der aktiven Instanzen dieser Warnmeldung.
2	Die Beschreibung der Warnmeldung.
3	Alle empfohlenen Aktionen für die Warnmeldung
4	Details zu jeder aktiven Instanz der Warnmeldung, einschließlich des betroffenen Node und Standorts, des Meldungsschweregrads, der UTC-Zeit, zu der die Meldungsregel ausgelöst wurde, und des Namens des betroffenen Jobs und Service.
5	Der Hostname des Admin-Knotens, der die Benachrichtigung gesendet hat.

Gruppierung von Warnungen

Um zu verhindern, dass bei der Auslösung von Warnmeldungen eine übermäßige Anzahl von E-Mail-Benachrichtigungen gesendet wird, versucht StorageGRID, mehrere Warnmeldungen in derselben Benachrichtigung zu gruppieren.

In der folgenden Tabelle finden Sie Beispiele, wie StorageGRID mehrere Warnmeldungen in E-Mail-Benachrichtigungen gruppiert.

Verhalten	Beispiel
<p>Jede Warnbenachrichtigung gilt nur für Warnungen, die denselben Namen haben. Wenn zwei Benachrichtigungen mit verschiedenen Namen gleichzeitig ausgelöst werden, werden zwei E-Mail-Benachrichtigungen gesendet.</p>	<ul style="list-style-type: none"> • Bei zwei Nodes wird gleichzeitig ein Alarm A ausgelöst. Es wird nur eine Benachrichtigung gesendet. • Bei Knoten 1 wird die Warnmeldung A ausgelöst, und gleichzeitig wird auf Knoten 2 die Warnmeldung B ausgelöst. Für jede Warnung werden zwei Benachrichtigungen gesendet.
<p>Wenn für eine bestimmte Warnmeldung auf einem bestimmten Node die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird eine Benachrichtigung nur für die schwerste Warnmeldung gesendet.</p>	<ul style="list-style-type: none"> • Die Warnmeldung A wird ausgelöst und die kleineren, größeren und kritischen Alarmschwellenwerte werden erreicht. Eine Benachrichtigung wird für die kritische Warnmeldung gesendet.
<p>Bei der ersten Alarmauslösung wartet StorageGRID zwei Minuten, bevor eine Benachrichtigung gesendet wird. Wenn während dieser Zeit andere Warnmeldungen mit demselben Namen ausgelöst werden, gruppiert StorageGRID alle Meldungen in der ersten Benachrichtigung.</p>	<ol style="list-style-type: none"> 1. An Knoten 1 um 08:00 wird eine Warnmeldung A ausgelöst. Es wird keine Benachrichtigung gesendet. 2. An Knoten 2 um 08:01 wird eine Warnmeldung A ausgelöst. Es wird keine Benachrichtigung gesendet. 3. Um 08:02 Uhr wird eine Benachrichtigung gesendet, um beide Instanzen der Warnmeldung zu melden.
<p>Falls eine weitere Benachrichtigung 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), selbst wenn sie zuvor gemeldet wurden.</p>	<ol style="list-style-type: none"> 1. An Knoten 1 um 08:00 wird eine Warnmeldung A ausgelöst. Eine Benachrichtigung wird um 08:02 Uhr gesendet. 2. An Knoten 2 um 08:05 wird eine Warnmeldung A ausgelöst. Eine zweite Benachrichtigung wird um 08:15 Uhr (10 Minuten später) versendet. Beide Nodes werden gemeldet.
<p>Wenn mehrere aktuelle Warnmeldungen mit demselben Namen vorliegen und eine dieser Meldungen gelöst wird, wird eine neue Benachrichtigung nicht gesendet, wenn die Meldung auf dem Node, für den die Meldung behoben wurde, erneut auftritt.</p>	<ol style="list-style-type: none"> 1. Für Knoten 1 wird eine Warnmeldung A ausgelöst. Eine Benachrichtigung wird gesendet. 2. Für Knoten 2 wird eine Warnmeldung A ausgelöst. Eine zweite Benachrichtigung wird gesendet. 3. Die Warnung A wird für Knoten 2 behoben, bleibt jedoch für Knoten 1 aktiv. 4. Für Node 2 wird erneut eine Warnmeldung A ausgelöst. Es wird keine neue Benachrichtigung gesendet, da die Meldung für Node 1 noch aktiv ist.

Verhalten	Beispiel
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen der Warnmeldung gelöst oder die Alarmregel stummgeschaltet wurde.	<ol style="list-style-type: none"> 1. Am 8. März wird Alarm A für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Warnung A ist nicht gelöst oder stummgeschaltet. Weitere Benachrichtigungen erhalten Sie am 15. März, 22. März 29 usw.

Beheben Sie Warnmeldungen bei E-Mail-Benachrichtigungen

Wenn die Meldung **E-Mail-Benachrichtigung Fehler** ausgelöst wird oder Sie die Test-Benachrichtigung nicht erhalten können, führen Sie die folgenden Schritte aus, um das Problem zu beheben.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff.

Schritte

1. Überprüfen Sie Ihre Einstellungen.
 - a. Wählen Sie **ALERTS > Email Setup**.
 - b. Überprüfen Sie, ob die Einstellungen des SMTP-Servers (E-Mail) korrekt sind.
 - c. Stellen Sie sicher, dass Sie gültige E-Mail-Adressen für die Empfänger angegeben haben.
2. Überprüfen Sie Ihren Spam-Filter, und stellen Sie sicher, dass die E-Mail nicht an einen Junk-Ordner gesendet wurde.
3. Bitten Sie Ihren E-Mail-Administrator, zu bestätigen, 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 anhand der in den Protokollen enthaltenen Informationen ermitteln, was schief gelaufen ist. Beispielsweise kann die Datei prometheus.log einen Fehler anzeigen, wenn Sie eine Verbindung zu dem von Ihnen angegebenen Server herstellen.

Siehe "[Erfassen von Protokolldateien und Systemdaten](#)".

Benachrichtigung über Stille

Optional können Sie Stille konfigurieren, um Benachrichtigungen vorübergehend zu unterdrücken.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie verfügen über die Berechtigung zum Verwalten von Warnmeldungen oder Root-Zugriff.

Über diese Aufgabe

Sie können Alarmregeln für das gesamte Grid, eine einzelne Site oder einen einzelnen Knoten und für einen oder mehrere Schweregrade stummschalten. Bei jeder Silence werden alle Benachrichtigungen für eine einzelne Warnungsregel oder für alle Warnungsregeln unterdrückt.

Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren.



Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummzuschalten. Wenn Sie eine Warnmeldung stummschalten, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.



Da Alarme und Alarme unabhängige Systeme sind, können Sie diese Funktion nicht zum Unterdrücken von Alarmmeldungen verwenden.

Schritte

1. Wählen Sie **ALARME > Stille**.

Die Seite „Stille“ wird angezeigt.

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create Edit Remove				
Alert Rule	Description	Severity	Time Remaining	Nodes
<i>No results found.</i>				

2. Wählen Sie **Erstellen**.

Das Dialogfeld Stille erstellen wird angezeigt.

Create Silence

Alert Rule

Description (optional)

Duration

Severity Minor only Minor, major Minor, major, critical

Nodes

- StorageGRID Deployment
 - Data Center 1
 - DC1-ADM1
 - DC1-G1
 - DC1-S1
 - DC1-S2
 - DC1-S3

3. Wählen Sie die folgenden Informationen aus, oder geben Sie sie ein:

Feld	Beschreibung
Meldungsregel	<p>Der Name der Alarmregel, die Sie stumm schalten möchten. Sie können eine beliebige Standard- oder benutzerdefinierte Warnungsregel auswählen, auch wenn die Alarmregel deaktiviert ist.</p> <p>Hinweis: Wählen Sie Alle Regeln aus, wenn Sie alle Alarmregeln mit den in diesem Dialogfeld angegebenen Kriterien stummschalten möchten.</p>
Beschreibung	<p>Optional eine Beschreibung der Stille. Beschreiben Sie zum Beispiel den Zweck dieser Stille.</p>
Dauer	<p>Wie lange Sie möchten, dass diese Stille in Minuten, Stunden oder Tagen wirksam bleibt. Eine Stille kann von 5 Minuten bis 1,825 Tage (5 Jahre) in Kraft sein.</p> <p>Hinweis: eine Alarmregel sollte nicht für längere Zeit stummgemacht werden. Wenn eine Alarmregel stumm geschaltet ist, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang abgeschlossen wird. Möglicherweise müssen Sie jedoch eine erweiterte Stille verwenden, wenn eine Warnung durch eine bestimmte, vorsätzliche Konfiguration ausgelöst wird, wie z. B. bei den Services Appliance Link Down-Alarmen und den Storage Appliance Link down-Alarmen.</p>

Feld	Beschreibung
Schweregrad	Welche Alarmschweregrade oder -Schweregrade stummgeschaltet werden sollten. Wenn die Warnung bei einem der ausgewählten Schweregrade ausgelöst wird, werden keine Benachrichtigungen gesendet.
Knoten	<p>Auf welchen Knoten oder Knoten Sie diese Stille anwenden möchten. Sie können eine Meldungsregel oder alle Regeln im gesamten Grid, einer einzelnen Site oder einem einzelnen Node unterdrücken. Wenn Sie das gesamte Raster auswählen, gilt die Stille für alle Standorte und alle Knoten. Wenn Sie einen Standort auswählen, gilt die Stille nur für die Knoten an diesem Standort.</p> <p>Hinweis: Sie können nicht mehr als einen Knoten oder mehr als einen Standort für jede Stille auswählen. Sie müssen zusätzliche Stille erstellen, wenn Sie dieselbe Warnungsregel auf mehr als einem Node oder mehreren Standorten gleichzeitig unterdrücken möchten.</p>

4. Wählen Sie **Speichern**.

5. Wenn Sie eine Stille ändern oder beenden möchten, bevor sie abläuft, können Sie sie bearbeiten oder entfernen.

Option	Beschreibung
Stille bearbeiten	<ol style="list-style-type: none"> Wählen Sie ALARME > Stille. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie bearbeiten möchten. Wählen Sie Bearbeiten. Ändern Sie die Beschreibung, die verbleibende Zeit, die ausgewählten Schweregrade oder den betroffenen Knoten. Wählen Sie Speichern.
Entfernen Sie eine Stille	<ol style="list-style-type: none"> Wählen Sie ALARME > Stille. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie entfernen möchten. Wählen Sie Entfernen. Wählen Sie OK, um zu bestätigen, dass Sie diese Stille entfernen möchten. <p>Hinweis: Benachrichtigungen werden jetzt gesendet, wenn diese Warnung ausgelöst wird (es sei denn, sie werden durch eine andere Stille unterdrückt). Wenn diese Warnmeldung derzeit ausgelöst wird, kann es einige Minuten dauern, bis E-Mail- oder SNMP-Benachrichtigungen gesendet werden und die Seite „Meldungen“ aktualisiert wird.</p>

Verwandte Informationen

- ["Konfigurieren Sie den SNMP-Agent"](#)

Alerts Referenz

In dieser Referenz werden die Standardwarnungen aufgeführt, die im Grid Manager angezeigt werden. Empfohlene Maßnahmen finden Sie in der Warnmeldung, die Sie erhalten.

Bei Bedarf können Sie benutzerdefinierte Alarmregeln erstellen, die Ihrem Systemmanagement entsprechen.

Einige der Standardwarnungen werden verwendet ["Kennzahlen von Prometheus"](#).

Appliance-Warnungen

Alarmname	Beschreibung
Akku des Geräts abgelaufen	Der Akku im Speicher-Controller des Geräts ist abgelaufen.
Akku des Geräts fehlgeschlagen	Der Akku im Speicher-Controller des Geräts ist ausgefallen.
Der Akku des Geräts weist nicht genügend Kapazität auf	Der Akku im Speicher-Controller des Geräts weist nicht genügend Kapazität auf.
Akku des Geräts befindet sich nahe dem Ablauf	Der Akku im Speicher-Controller des Geräts läuft langsam ab.
Akku des Geräts entfernt	Der Akku im Speicher-Controller des Geräts fehlt.
Der Akku des Geräts ist zu heiß	Die Batterie im Speicher-Controller des Geräts ist überhitzt.
Fehler bei der BMC-Kommunikation des Geräts	Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren.
Fehler beim Sichern des Appliance-Cache	Ein persistentes Cache-Sicherungsgerät ist fehlgeschlagen.
Gerät-Cache-Backup-Gerät unzureichende Kapazität	Die Kapazität des Cache-Sicherungsgeräts ist nicht ausreichend.
Appliance Cache Backup-Gerät schreibgeschützt	Ein Cache-Backup-Gerät ist schreibgeschützt.
Die Größe des Appliance-Cache-Speichers stimmt nicht überein	Die beiden Controller im Gerät haben unterschiedliche Cache-Größen.
Die Temperatur des Computing-Controller-Chassis des Geräts ist zu hoch	Die Temperatur des Computing-Controllers in einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten.

Alarmname	Beschreibung
Die CPU-Temperatur des Appliance-Compute-Controllers ist zu hoch	Die Temperatur der CPU im Computing-Controller einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten.
Aufmerksamkeit für Compute-Controller ist erforderlich	Im Compute-Controller einer StorageGRID-Appliance wurde ein Hardwarefehler erkannt.
Ein Problem besteht in der Stromversorgung Des Computercontrollers A des Geräts	Bei Netzteil A im Compute-Controller ist ein Problem aufgetreten.
Das Netzteil B des Compute-Controllers ist ein Problem	Die Stromversorgung B im Compute-Controller hat ein Problem.
Der Service zur Überwachung der Computing-Hardware des Appliances ist ausgesetzt	Der Dienst, der den Status der Speicherhardware überwacht, ist blockiert.
Fehler des Appliance-das-Laufwerks erkannt	Bei einem Direct-Attached Storage (das)-Laufwerk in der Appliance wurde ein Problem festgestellt.
Wiederherstellung des Appliance-das-Laufwerks	Ein Direct-Attached Storage (das)-Laufwerk wird neu erstellt. Dies wird erwartet, wenn es vor kurzem ersetzt oder entfernt/wieder eingesetzt wurde.
Fehler des Gerätelüfters erkannt	Es wurde ein Problem mit einer Lüftereinheit im Gerät festgestellt.
Fibre-Channel-Fehler des Geräts erkannt	Zwischen dem Appliance-Storage-Controller und dem Rechner-Controller wurde ein Fibre-Channel-Verbindungsproblem festgestellt
Fehler des Fibre-Channel-HBA-Ports des Geräts	Ein Fibre-Channel-HBA-Port ist ausgefallen oder ist ausgefallen.
Appliance Flash Cache Laufwerke sind nicht optimal	Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal.
Geräteverbindung/Batteriebehälter entfernt	Der Verbindungs-/Batteriebehälter fehlt.
Geräte-LACP-Port fehlt	Ein Port auf einer StorageGRID-Appliance beteiligt sich nicht an der LACP-Verbindung.
Appliance-NIC-Fehler erkannt	Es wurde ein Problem mit einer Netzwerkkarte (NIC) im Gerät festgestellt.

Alarmname	Beschreibung
Das gesamte Netzteil des Geräts ist heruntergestuft	Die Leistung eines StorageGRID-Geräts ist von der empfohlenen Betriebsspannung abweichen.
Kritische Warnung bei Appliance-SSD	Eine Appliance-SSD meldet eine kritische Warnung.
Ausfall des Appliance Storage Controller A	Der Speicher-Controller A in einer StorageGRID-Appliance ist ausgefallen.
Fehler beim Speicher-Controller B des Geräts	Bei Speicher-Controller B in einer StorageGRID-Appliance ist ein Fehler aufgetreten.
Laufwerksausfall des Appliance-Storage-Controllers	Mindestens ein Laufwerk in einer StorageGRID-Appliance ist ausgefallen oder nicht optimal.
Hardwareproblem des Appliance Storage Controllers	SANtricity meldet, dass für eine Komponente einer StorageGRID Appliance ein Hinweis erforderlich ist.
Ausfall der Stromversorgung des Speicher-Controllers	Die Stromversorgung A in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abweichen.
Fehler bei Netzteil B des Speicher-Controllers	Stromversorgung B bei einem StorageGRID-Gerät hat von der empfohlenen Betriebsspannung abweichen.
Monitordienst der Appliance-Storage-Hardware ist ausgesetzt	Der Dienst, der den Status der Speicherhardware überwacht, ist blockiert.
Appliance Storage-Shelfs ist beeinträchtigt	Der Status einer der Komponenten im Storage Shelf für eine Storage Appliance ist beeinträchtigt.
Gerätetemperatur überschritten	Die nominale oder maximale Temperatur für den Lagercontroller des Geräts wurde überschritten.
Temperatursensor des Geräts entfernt	Ein Temperatursensor wurde entfernt.
Die Festplatten-I/O ist sehr langsam	Sehr langsamer Festplatten-I/O kann die Grid-Performance beeinträchtigen.
Lüfterfehler des Speichergeräts erkannt	Es wurde ein Problem mit einer Lüftereinheit im Speicher-Controller für eine Appliance festgestellt.
Die Storage-Konnektivität der Storage-Appliance ist herabgesetzt	Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller.

Alarmname	Beschreibung
Speichergerät nicht zugänglich	Auf ein Speichergerät kann nicht zugegriffen werden.

Audit- und Syslog-Warnmeldungen

Alarmname	Beschreibung
Audit-Protokolle werden der Warteschlange im Speicher hinzugefügt	Der Knoten kann keine Protokolle an den lokalen Syslog-Server senden, und die Speicherwarteschlange füllt sich.
Fehler bei der Weiterleitung des externen Syslog-Servers	Der Knoten kann keine Protokolle an den externen Syslog-Server weiterleiten.
Große Audit-Warteschlange	Die Datenträgerwarteschlange für Überwachungsmeldungen ist voll. Wenn diese Bedingung nicht erfüllt 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-Warnmeldungen

Alarmname	Beschreibung
FabricPool Bucket hat die nicht unterstützte Bucket-KonsistenzEinstellung	Ein FabricPool Bucket verwendet die verfügbare Konsistenzstufe, die nicht unterstützt wird.

Cassandra – Warnmeldungen

Alarmname	Beschreibung
Cassandra Auto-Kompaktor-Fehler	Beim Cassandra Auto-Kompaktor ist ein Fehler aufgetreten.
Cassandra Auto-Kompaktor-Kennzahlen veraltet	Die Kennzahlen, die den Cassandra Auto-Kompaktor beschreiben, sind veraltet.
Cassandra Kommunikationsfehler	Die Nodes, auf denen der Cassandra-Service ausgeführt wird, haben Probleme bei der Kommunikation untereinander.
Cassandra-Kompensation überlastet	Der Cassandra-Verdichtungsprozess ist überlastet.
Cassandra-Fehler bei der Übergröße des Schreibvorgangs	Bei einem internen StorageGRID-Prozess wurde eine zu große Schreibenforderung an Cassandra gesendet.

Alarmname	Beschreibung
Veraltete Reparaturkennzahlen für Cassandra	Die Kennzahlen, die Cassandra-Reparaturaufträge beschreiben, sind veraltet.
Cassandra Reparaturfortschritt langsam	Der Fortschritt der Cassandra-Datenbankreparaturen ist langsam.
Cassandra Reparaturservice nicht verfügbar	Der Cassandra-Reparaturservice ist nicht verfügbar.
Cassandra Tabelle beschädigt	Cassandra hat Tabellenbeschädigungen erkannt. Cassandra wird automatisch neu gestartet, wenn Tabellenbeschädigungen erkannt werden.
Verbesserte Leseverfügbarkeit deaktiviert	Wenn die verbesserte Leseverfügbarkeit deaktiviert ist, können GET- und HEAD-Anforderungen fehlschlagen, wenn Storage-Nodes nicht verfügbar sind.

Warnmeldungen für Cloud-Storage-Pool

Alarmname	Beschreibung
Verbindungsfehler beim Cloud-Storage-Pool	Bei der Zustandsprüfung für Cloud-Storage-Pools wurde ein oder mehrere neue Fehler erkannt.

Warnmeldungen bei Grid-übergreifender Replizierung

Alarmname	Beschreibung
Dauerhafter Ausfall der Grid-übergreifenden Replizierung	Es ist ein gitterübergreifender Replikationsfehler aufgetreten, der vom Benutzer behoben werden muss.
Grid-übergreifende Replizierungsressourcen nicht verfügbar	Grid-übergreifende Replikationsanforderungen stehen aus, da eine Ressource nicht verfügbar ist.

DHCP-Warnungen

Alarmname	Beschreibung
DHCP-Leasing abgelaufen	Der DHCP-Leasingvertrag auf einer Netzwerkschnittstelle ist abgelaufen.
DHCP-Leasing läuft bald ab	Der DHCP-Lease auf einer Netzwerkschnittstelle läuft demnächst aus.
DHCP-Server nicht verfügbar	Der DHCP-Server ist nicht verfügbar.

Debug- und Trace-Warnungen

Alarmname	Beschreibung
Leistungsbeeinträchtigung debuggen	Wenn der Debug-Modus aktiviert ist, kann sich die Systemleistung negativ auswirken.
Trace-Konfiguration aktiviert	Wenn die Trace-Konfiguration aktiviert ist, kann die Systemleistung beeinträchtigt werden.

E-Mail- und AutoSupport-Benachrichtigungen

Alarmname	Beschreibung
Fehler beim Senden der AutoSupport-Nachricht	Die letzte AutoSupport-Meldung konnte nicht gesendet werden.
E-Mail-Benachrichtigung fehlgeschlagen	Die E-Mail-Benachrichtigung für eine Warnmeldung konnte nicht gesendet werden.

Alarmer für Erasure Coding (EC)

Alarmname	Beschreibung
EC-Ausgleichfehler	Das EC-Ausgleichsverfahren ist fehlgeschlagen oder wurde gestoppt.
EC-Reparaturfehler	Ein Reparaturauftrag für EC-Daten ist fehlgeschlagen oder wurde angehalten.
EC-Reparatur blockiert	Ein Reparaturauftrag für EC-Daten ist blockiert.

Ablauf von Zertifikatwarnungen

Alarmname	Beschreibung
Ablauf des Client-Zertifikats	Mindestens ein Clientzertifikat läuft bald ab.
Ablauf des globalen Serverzertifikats für S3 und Swift	Das globale Serverzertifikat für S3 und Swift läuft demnächst ab.
Ablauf des Endpunktzertifikats des Load Balancer	Ein oder mehrere Load Balancer-Endpunktzertifikate laufen kurz vor dem Ablauf.
Ablauf des Serverzertifikats für die Verwaltungsschnittstelle	Das für die Managementoberfläche verwendete Serverzertifikat läuft bald ab.
Ablauf des externen Syslog CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des externen Syslog-Serverzertifikats verwendet wird, läuft in Kürze ab.

Alarmname	Beschreibung
Ablauf des externen Syslog-Client-Zertifikats	Das Client-Zertifikat für einen externen Syslog-Server läuft kurz vor dem Ablauf.
Ablauf des externen Syslog-Serverzertifikats	Das vom externen Syslog-Server präsentierte Serverzertifikat läuft bald ab.

Warnmeldungen zum Grid-Netzwerk

Alarmname	Beschreibung
MTU-Diskrepanz bei dem Grid-Netzwerk	Die MTU-Einstellung für die Grid Network-Schnittstelle (eth0) unterscheidet sich deutlich von Knoten im Grid.

Warnmeldungen zu Grid-Verbund

Alarmname	Beschreibung
Ablauf des Netzverbundzertifikats	Ein oder mehrere Grid Federation-Zertifikate laufen demnächst ab.
Fehler bei der Verbindung mit dem Grid-Verbund	Die Netzverbundverbindung zwischen dem lokalen und dem entfernten Netz funktioniert nicht.

Warnmeldungen bei hoher Auslastung oder hoher Latenz

Alarmname	Beschreibung
Hohe Java-Heap-Nutzung	Es wird ein hoher Prozentsatz von Java Heap Space verwendet.
Hohe Latenz bei Metadatenanfragen	Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang.

Warnmeldungen zur Identitätsföderation

Alarmname	Beschreibung
Synchronisierungsfehler bei der Identitätsföderation	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren.
Fehler bei der Synchronisierung der Identitätsföderation für einen Mandanten	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren, die von einem Mandanten konfiguriert wurde.

Warnmeldungen für Information Lifecycle Management (ILM)

Alarmname	Beschreibung
ILM-Platzierung nicht erreichbar	Eine Platzierungsanweisung in einer ILM-Regel kann für bestimmte Objekte nicht erreicht werden.
Der ILM-Scan ist zu lang	Der Zeitaufwand für das Scannen, Bewerten und Anwenden von ILM auf Objekte ist zu lang.
ILM-Scan-Rate niedrig	Die ILM-Scan-Rate ist auf weniger als 100 Objekte/Sekunde eingestellt.

KMS-Warnungen (Key Management Server)

Alarmname	Beschreibung
ABLAUF DES KMS-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des KMS-Zertifikats (Key Management Server) verwendet wird, läuft bald ab.
ABLAUF DES KMS-Clientzertifikats	Das Clientzertifikat für einen Schlüsselverwaltungsserver läuft demnächst ab
KMS-Konfiguration konnte nicht geladen werden	Es ist die Konfiguration für den Verschlüsselungsmanagement-Server vorhanden, konnte aber nicht geladen werden.
KMS-Verbindungsfehler	Ein Appliance-Node konnte keine Verbindung zum Schlüsselmanagementserver für seinen Standort herstellen.
DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt.
DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen	Alle Appliance-Volumes wurden erfolgreich entschlüsselt, ein oder mehrere Volumes konnten jedoch nicht auf den neuesten Schlüssel gedreht werden.
KM ist nicht konfiguriert	Für diesen Standort ist kein Schlüsselverwaltungsserver vorhanden.
KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln	Ein oder mehrere Volumes auf einer Appliance mit aktivierter Node-Verschlüsselung konnten nicht mit dem aktuellen KMS-Schlüssel entschlüsselt werden.
Ablauf DES KMS-Serverzertifikats	Das vom KMS (Key Management Server) verwendete Serverzertifikat läuft in Kürze ab.

Lokale Zeitversatz-Warnungen

Alarmname	Beschreibung
Großer Zeitversatz der lokalen Uhr	Der Offset zwischen lokaler Uhr und NTP-Zeit (Network Time Protocol) ist zu groß.

Warnungen zu wenig Speicher oder zu wenig Speicherplatz

Alarmname	Beschreibung
Geringe Kapazität der Auditprotokoll-Festplatte	Der für Audit-Protokolle verfügbare Platz ist gering. Wenn diese Bedingung nicht erfüllt wird, können S3- oder Swift-Vorgänge fehlschlagen.
Niedriger verfügbarer Node-Speicher	Die RAM-Menge, die auf einem Knoten verfügbar ist, ist gering.
Wenig freier Speicherplatz für den Speicherpool	Der verfügbare Speicherplatz zum Speichern von Objektdaten im Storage Node ist gering.
Wenig installierter Node-Speicher	Der installierte Arbeitsspeicher auf einem Node ist gering.
Niedriger Metadaten-Storage	Der zur Speicherung von Objektmetadaten verfügbare Speicherplatz ist gering.
Niedrige Kenngrößen für die Festplattenkapazität	Der für die Kennzahlendatenbank verfügbare Speicherplatz ist gering.
Niedriger Objekt-Storage	Der zum Speichern von Objektdaten verfügbare Platz ist gering.
Low Read-Only-Wasserzeichen überschreiben	Der Speichervolumen Soft Read-Only-Wasserzeichen-Überschreiben ist kleiner als der für einen Speicherknoten optimierte Mindestwert.
Niedrige Root-Festplattenkapazität	Der auf der Stammfestplatte verfügbare Speicherplatz ist gering.
Niedrige Datenkapazität des Systems	Der für StorageGRID-Systemdaten verfügbare Speicherplatz auf dem /var/local Mount-Punkt ist gering.
Geringer Tmp-Telefonspeicherplatz	Der im Verzeichnis /tmp verfügbare Speicherplatz ist gering.

Warnmeldungen für das Node- oder Node-Netzwerk

Alarmname	Beschreibung
Fehler bei der Firewall-Konfiguration	Firewall-Konfiguration konnte nicht angewendet werden.

Alarmname	Beschreibung
Fehler bei der Node-Netzwerkverbindung	Beim Übertragen der Daten zwischen den Nodes ist ein Fehler aufgetreten.
Node-Netzwerkannahme-Frame-Fehler	Bei einem hohen Prozentsatz der Netzwerkframes, die von einem Node empfangen wurden, gab es Fehler.
Der Node ist nicht mit dem NTP-Server synchronisiert	Der Node ist nicht mit dem NTP-Server (Network Time Protocol) synchronisiert.
Der Node ist nicht mit dem NTP-Server gesperrt	Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt.
Nicht-Appliance-Knotennetzwerk ausgefallen	Mindestens ein Netzwerkgerät ist ausgefallen oder nicht verbunden.
Verbindung zur Service-Appliance im Admin-Netzwerk getrennt	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Services-Appliance-Verbindung am Admin-Netzwerkanschluss 1 getrennt	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden.
Verbindung zur Service-Appliance im Client-Netzwerk getrennt	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 1 getrennt	Netzwerkport 1 auf der Appliance ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 2 getrennt	Netzwerkport 2 auf der Appliance ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 3 getrennt	Netzwerkport 3 auf der Appliance ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 4 getrennt	Netzwerkport 4 auf der Appliance ist ausgefallen oder getrennt.
Verbindung der Storage-Appliance im Admin-Netzwerk getrennt	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Verknüpfung der Speicher-Appliance auf Admin-Netzwerk-Port 1 ausgefallen	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden.
Verbindung der SpeicherAppliance im Client-Netzwerk getrennt	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.

Alarmname	Beschreibung
Verbindung der Speicher-Appliance auf Netzwerkport 1 getrennt	Netzwerkport 1 auf der Appliance ist ausgefallen oder getrennt.
Verbindung der Speicher-Appliance auf Netzwerkport 2 getrennt	Netzwerkport 2 auf der Appliance ist ausgefallen oder getrennt.
Verbindung der Speicher-Appliance auf Netzwerkport 3 getrennt	Netzwerkport 3 auf der Appliance ist ausgefallen oder getrennt.
Verbindung der Speicher-Appliance auf Netzwerkport 4 getrennt	Netzwerkport 4 auf der Appliance ist ausgefallen oder getrennt.
Storage-Node befindet sich nicht im gewünschten Speicherzustand	Der LDR-Service auf einem Storage Node kann aufgrund eines internen Fehlers oder Volume-bezogenen Problems nicht in den gewünschten Status wechseln
Kommunikation mit Knoten nicht möglich	Mindestens ein Dienst reagiert nicht, oder der Node kann nicht erreicht werden.
Unerwarteter Node-Neustart	Ein Node wurde in den letzten 24 Stunden unerwartet neu gebootet.

Objektwarnmeldungen

Alarmname	Beschreibung
Überprüfung der Objektexistenz fehlgeschlagen	Der Job für die Objektexistenzprüfung ist fehlgeschlagen.
Prüfung der ObjektExistenz ist blockiert	Der Job zur Prüfung der ObjektExistenz ist blockiert.
Objekte verloren	Mindestens ein Objekt ist aus dem Raster verloren gegangen.
S3 PUT Objekt size zu groß	Ein Client versucht, eine PUT-Objekt-Operation durchzuführen, die die S3-Größenlimits überschreitet.
Nicht identifizierte beschädigte Objekte erkannt	Im replizierten Objekt-Storage wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte.

Benachrichtigungen zu Plattform-Services

Alarmname	Beschreibung
Plattform-Services nicht verfügbar	Zu wenige Speicherknoten mit dem RSM-Service laufen oder sind an einem Standort verfügbar.

Warnmeldungen zu Storage-Volumes

Alarmname	Beschreibung
Das Storage-Volume muss beachtet werden	Ein Storage Volume ist offline und muss beachtet werden.
Das Speicher-Volume muss wiederhergestellt werden	Ein Speicher-Volume wurde wiederhergestellt und muss wiederhergestellt werden.
Das Storage-Volume ist offline	Ein Storage-Volume ist länger als 5 Minuten offline, möglicherweise aufgrund des Neubootens des Node während der Formatierung des Volumes.
Die Volume-Wiederherstellung konnte die Reparatur replizierter Daten nicht starten	Die Reparatur replizierter Daten für ein repariertes Volume konnte nicht automatisch gestartet werden.

Warnmeldungen zu StorageGRID-Services

Alarmname	Beschreibung
Nginx-Dienst mit Backup-Konfiguration	Die Konfiguration des nginx-Dienstes ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.
Nginx-gw-Dienst mit Backup-Konfiguration	Die Konfiguration des nginx-gw-Dienstes ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.
SSH-Service unter Verwendung der Backup-Konfiguration	Die Konfiguration des SSH-Dienstes ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.

Mandantenwarnmeldungen

Alarmname	Beschreibung
Hohe Kontingentnutzung für Mandanten	Ein hoher Prozentsatz des Quota-Speicherplatzes wird verwendet. Diese Regel ist standardmäßig deaktiviert, da sie möglicherweise zu viele Benachrichtigungen verursacht.

Häufig verwendete Prometheus-Kennzahlen

In dieser Liste der häufig verwendeten Prometheus-Kennzahlen können Sie die Bedingungen in den Standardwarnungsregeln besser verstehen oder die Bedingungen für benutzerdefinierte Warnungsregeln erstellen.

Das können Sie auch [Holen Sie sich eine vollständige Liste aller Kennzahlen](#).

Details zur Syntax von Prometheus-Abfragen finden Sie unter "[Prometheus Wird Abgefragt](#)".

Was sind Prometheus-Kennzahlen?

Prometheus Kennzahlen sind Zeitreihenmessungen. Der Prometheus-Service auf Admin-Nodes erfasst diese Kennzahlen von den Services auf allen Knoten. Metriken werden auf jedem Admin-Node gespeichert, bis der für Prometheus-Daten reservierte Speicherplatz voll ist. Wenn der `/var/local/mysql_ibdata/` Volume erreicht die Kapazität, zuerst werden die ältesten Metriken gelöscht.

Wo werden Prometheus-Kennzahlen verwendet?

Die von Prometheus gesammelten Kennzahlen werden an mehreren Stellen im Grid Manager verwendet:

- **Knoten Seite:** Die Grafiken und Diagramme auf den Registerkarten, die auf der Seite Knoten verfügbar sind, zeigen mit dem Grafana Visualization Tool die von Prometheus erfassten Zeitreihenmetriken an. Grafana zeigt Zeitserien-Daten im Diagramm- und Diagrammformat an, Prometheus dient als Back-End-Datenquelle.



- **Alerts:** Warnmeldungen werden auf bestimmten Schweregraden ausgelöst, wenn Alarmregelbedingungen, die Prometheus-Metriken verwenden, als wahr bewerten.
- **Grid Management API:** Sie können Prometheus-Kennzahlen in benutzerdefinierten Alarmregeln oder mit externen Automatisierungstools verwenden, um Ihr StorageGRID-System zu überwachen. Eine vollständige Liste der Prometheus-Kennzahlen finden Sie über die Grid Management API. (Klicken Sie oben im Grid Manager auf das Hilfesymbol und wählen Sie **API-Dokumentation > metrics**.) Obwohl mehr als tausend Kennzahlen verfügbar sind, ist nur eine relativ geringe Zahl zur Überwachung der wichtigsten StorageGRID-Vorgänge erforderlich.



Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

- Die Seite **SUPPORT > Tools > Diagnostics** und die Seite **SUPPORT > Tools > Metrics**: Diese Seiten, die in erster Linie für den technischen Support bestimmt sind, bieten verschiedene Tools und Diagramme, die die Werte von Prometheus Metrics verwenden.



Einige Funktionen und Menüelemente auf der Seite Metriken sind absichtlich nicht funktionsfähig und können sich ändern.

Liste der häufigsten Kennzahlen

Die folgende Liste enthält die am häufigsten verwendeten Prometheus Kennzahlen.



Metriken, die *private* in ihren Namen enthalten, sind nur für den internen Gebrauch und können ohne vorherige Ankündigung zwischen StorageGRID Versionen geändert werden.

Alertmanager_notifications_failed_total

Die Gesamtzahl der fehlgeschlagenen Warnmeldungen.

Node_Fileystem_verfügbare_Byte

Die Menge des Dateisystemspeichers, der nicht-Root-Benutzern in Byte zur Verfügung steht.

Node_Memory_MemAvailable_Bytes

Feld Speicherinformationen MemAvailable_Bytes.

Node_Network_Carrier

Trägerwert von `/sys/class/net/iface`.

Node_Network_receive_errs_total

Netzwerkgerätestatistik `receive_errs`.

Node_Network_transmit_errs_total

Netzwerkgerätestatistik `transmit_errs`.

storagegrid_administrativ_down

Der Node ist aus einem erwarteten Grund nicht mit dem Grid verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert.

storagegrid_Appliance_Compute_Controller_Hardware_Status

Der Status der Computing-Controller-Hardware in einer Appliance.

storagegrid_Appliance_failed_Disks

Für den Speicher-Controller in einer Appliance die Anzahl der Laufwerke, die nicht optimal sind.

storagegrid_Appliance_Storage_Controller_Hardware_Status

Der Gesamtstatus der Hardware eines Storage Controllers in einer Appliance.

storagegrid_Content_Buckets_und_Containern

Die Gesamtzahl der S3-Buckets und Swift-Container, die von diesem Storage-Node bekannt sind

storagegrid_Content_Objects

Die Gesamtzahl der von diesem Storage-Node bekannten S3 und Swift Datenobjekte. Die Anzahl ist nur für Datenobjekte gültig, die von Client-Applikationen erstellt werden, die über S3 oder Swift mit dem System interface.

storagegrid_Content_Objects_Lost

Gesamtzahl der vom StorageGRID System erkannten Objekte, die von diesem Service als fehlend erkannt werden. Es sollten Maßnahmen ergriffen werden, um die Ursache des Schadens zu ermitteln und ob eine Erholung möglich ist.

["Fehlerbehebung bei verlorenen und fehlenden Objektdaten"](#)

storagegrid_http_Sessions_Incoming_versuchte

Die Gesamtzahl der HTTP-Sitzungen, die zu einem Speicherknoten versucht wurden.

storagegrid_http_Sessions_Incoming_derzeit_etabliertes

Die Anzahl der derzeit aktiven HTTP-Sitzungen (offen) auf dem Speicherknoten.

storagegrid_http_Sessions_INCOMING_FAILED

Die Gesamtzahl der HTTP-Sitzungen, die nicht erfolgreich abgeschlossen wurden, entweder aufgrund einer fehlerhaften HTTP-Anfrage oder aufgrund eines Fehlers bei der Verarbeitung eines Vorgangs.

storagegrid_http_Sessions_Incoming_successful

Die Gesamtzahl der erfolgreich abgeschlossenen HTTP-Sitzungen.

storagegrid_ilm_awaiting_background_Objects

Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus dem Scan warten

storagegrid_ilm_awaiting_Client_Evaluation_Objects_per_Second

Die aktuelle Rate, mit der Objekte im Vergleich zur ILM-Richtlinie auf diesem Node bewertet werden.

storagegrid_ilm_awaiting_Client_Objects

Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus den Client-Vorgängen (z. B. Aufnahme) warten

storagegrid_ilm_awaiting_total_Objects

Gesamtzahl der Objekte, die auf eine ILM-Bewertung warten

storagegrid_ilm_Scan_Objects_per_Second

Die Geschwindigkeit, mit der Objekte des Node gescannt und für ILM in der Warteschlange gestellt werden.

storagegrid_ilm_Scan_Period_Geschätzter_Minuten

Die geschätzte Zeit zum Abschließen eines vollständigen ILM-Scans auf diesem Node.

Hinweis: Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde, die sich im Besitz dieses Knotens befinden.

storagegrid_Load_Balancer_Endpoint_cert_expiry_time

Die Ablaufzeit des Endpunktzertifikats des Load Balancer in Sekunden seit der Epoche.

storagegrid_Metadatenabfragen_average_Latency_Millisekunden

Die durchschnittliche Zeit, die zum Ausführen einer Abfrage des MetadatenSpeichers über diesen Service benötigt wird.

storagegrid_Network_received_Byte

Die Gesamtmenge der seit der Installation empfangenen Daten.

storagegrid_Network_transmitted_Byte

Die Gesamtmenge der seit der Installation gesendeten Daten.

storagegrid_Node_cpu_Utifficiency_percenty

Der Prozentsatz der verfügbaren CPU-Zeit, die derzeit von diesem Service genutzt wird. Gibt an, wie beschäftigt der Dienst ist. Die verfügbare CPU-Zeit hängt von der Anzahl der CPUs für den Server ab.

storagegrid_ntp_Choosed_time_source_Offset_Millisekunden

Systematischer Zeitversatz, der von einer ausgewählten Zeitquelle bereitgestellt wird. Offset wird eingeführt, wenn die Verzögerung zum Erreichen einer Zeitquelle nicht der Zeit entspricht, die für das Erreichen des NTP-Clients benötigt wird.

storagegrid_ntp_gesperrt

Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt.

storagegrid_s3_Data_Transfers_Bytes_aufgenommen

Die Gesamtmenge an Daten, die seit dem letzten Zurücksetzen des Attributs von S3-Clients auf diesen Storage-Node aufgenommen wurden.

storagegrid_s3_Data_Transfers_Bytes_abgerufen

Die Gesamtanzahl der Daten, die von S3-Clients von diesem Speicherknoten seit dem letzten Zurücksetzen des Attributs abgerufen wurden.

storagegrid_s3_Operations_fehlgeschlagen

Die Gesamtzahl der fehlgeschlagenen S3-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen solche, die durch S3-Autorisierungsfehler verursacht wurden.

storagegrid_s3_Operations_erfolgreich

Die Gesamtzahl der erfolgreichen S3-Vorgänge (HTTP-Statuscode 2xx).

storagegrid_s3_Operations_nicht autorisiert

Die Gesamtzahl der fehlerhaften S3-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind.

storagegrid_Serverzertifikat_Management_Interface_cert_expiry_days

Die Anzahl der Tage vor Ablauf des Managementschnittstelle-Zertifikats.

storagegrid_Serverzertifikat_Storage_API_endpunktes_cert_expiry_days

Die Anzahl der Tage, bevor das Objekt-Speicher-API-Zertifikat abläuft.

storagegrid_Service_cpu_Sekunden

Der kumulierte Zeitaufwand, die die CPU seit der Installation bei diesem Service verwendet hat.

storagegrid_Service_Memory_Usage_Byte

Die Speichermenge (RAM), die derzeit von diesem Dienst verwendet wird. Dieser Wert ist identisch mit dem, der vom Linux-Top-Dienstprogramm als RES angezeigt wird.

storagegrid_Service_Network_received_Byte

Die Gesamtanzahl der Daten, die seit der Installation von diesem Service eingehen.

storagegrid_Service_Network_transmitted_Byte

Die Gesamtanzahl der von diesem Service gesendeten Daten.

storagegrid_Service_startet neu

Die Gesamtanzahl der Neustarts des Dienstes.

storagegrid_Service_Runtime_seconds

Die Gesamtzeit, die der Service seit der Installation ausgeführt hat.

storagegrid_Service_Uptime_Sekunden

Die Gesamtzeit, die der Dienst seit dem letzten Neustart ausgeführt hat.

storagegrid_Storage_State_current

Der aktuelle Status der Storage-Services. Attributwerte sind:

- 10 = Offline
- 15 = Wartung
- 20 = schreibgeschützt
- 30 = Online

storagegrid_Storage_Status

Der aktuelle Status der Storage-Services. Attributwerte sind:

- 0 = Keine Fehler
- 10 = In Transition
- 20 = Nicht Genügend Freier Speicherplatz
- 30 = Volume(s) nicht verfügbar
- 40 = Fehler

storagegrid_Storage_Utilization_Data_Bytes

Schätzung der Gesamtgröße der replizierten und Erasure-codierten Objektdaten auf dem Storage-Node

storagegrid_Storage_Utiffici“_Metadata_allowed_Bytes

Der gesamte Speicherplatz auf Volume 0 jedes Storage-Node, der für Objekt-Metadaten zulässig ist. Dieser Wert ist immer kleiner als der tatsächlich für Metadaten auf einem Node reservierte Speicherplatz, da für grundlegende Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades ein Teil des reservierten Speicherplatzes benötigt wird. Der zulässige Speicherplatz für Objektmetadaten steuert die allgemeine Objektkapazität.

storagegrid_Storage_Utifficiendatij_Metadata_Bytes

Die Menge der Objekt-Metadaten auf dem Storage-Volume 0 in Bytes.

storagegrid_Storage_Utifficienfficienals_total_space_Bytes

Der gesamte Speicherplatz, der allen Objektspeichern zugewiesen ist.

storagegrid_Storage_Utiabile_space_Bytes

Die verbleibende Menge an Objekt-Storage. Berechnet durch Hinzufügen der verfügbaren Menge an Speicherplatz für alle Objektspeichern auf dem Storage-Node.

storagegrid_Swift_Data_Transfers_Bytes_aufgenommen

Die Gesamtmenge der Daten, die Swift-Clients seit dem letzten Zurücksetzen des Attributs von diesem Storage-Node aufgenommen haben.

storagegrid_Swift_Data_Transfers_Bytes_abgerufen

Die Gesamtanzahl der Daten, die Swift-Clients von diesem Speicherknoten seit dem letzten Zurücksetzen des Attributs abgerufen haben.

storagegrid_Swift_Operations_fehlgeschlagen

Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen solche, die durch Swift-Autorisierungsfehler verursacht wurden.

storagegrid_Swift_Operations_erfolgreich

Die Gesamtzahl der erfolgreichen Swift-Vorgänge (HTTP-Statuscode 2xx).

storagegrid_Swift_Operations_nicht autorisiert

Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind (HTTP-Statuscodes 401, 403, 405).

storagegrid_Tenant_Usage_Data_Byte

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, die für die Objekte des Mandanten verfügbar ist. Wenn keine Quota-Metrik angegeben wird, steht eine unbegrenzte Menge an Speicherplatz zur Verfügung.

Eine Liste aller Kennzahlen abrufen

[[Alle Metriken abrufen]]um die vollständige Liste der Metriken zu erhalten, verwenden Sie die Grid Management API.

1. Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
2. Suchen Sie nach den **Metriken**-Vorgängen.
3. Ausführen des `GET /grid/metric-names` Betrieb.
4. Ergebnisse herunterladen

Verwalten von Alarmen (Altsystem)

Verwalten von Alarmen (Altsystem)

Das StorageGRID-Alarmssystem ist das ältere System, mit dem Störstellen identifiziert werden können, die manchmal während des normalen Betriebs auftreten.



Das alte Alarmssystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Alarmklassen (altes System)

Ein älterer Alarm kann zu einer von zwei sich gegenseitig ausschließenden Alarmklassen gehören.

- Standardalarme werden mit jedem StorageGRID-System geliefert und können nicht geändert werden. Sie können jedoch Standardalarme deaktivieren oder überschreiben, indem Sie globale benutzerdefinierte Alarme definieren.
- Globale benutzerdefinierte Alarme überwachen den Status aller Dienste eines bestimmten Typs im StorageGRID-System. Sie können einen globalen benutzerdefinierten Alarm erstellen, um einen Standardalarm zu überschreiben. Sie können auch einen neuen globalen benutzerdefinierten Alarm

erstellen. Dies kann nützlich sein, um alle angepassten Bedingungen Ihres StorageGRID-Systems zu überwachen.

Alarmauslöselogik (Älteres System)

Ein alter Alarm wird ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht, der für eine Kombination aus Alarmklasse (Standard oder Global Custom) und Alarmschweregrade auf „true“ bewertet.

Symbol	Farbe	Alarmschweregrad	Bedeutung
	Gelb	Hinweis	Der Node ist mit dem Grid verbunden. Es ist jedoch eine ungewöhnliche Bedingung vorhanden, die den normalen Betrieb nicht beeinträchtigt.
	Hellorange	Gering	Der Node ist mit dem Raster verbunden, aber es existiert eine anormale Bedingung, die den Betrieb in Zukunft beeinträchtigen könnte. Sie sollten untersuchen, um eine Eskalation zu verhindern.
	Dunkelorange	Major	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die sich derzeit auf den Betrieb auswirkt. Um eine Eskalation zu vermeiden, ist eine sofortige Aufmerksamkeit erforderlich.
	Rot	Kritisch	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die normale Vorgänge angehalten hat. Sie sollten das Problem sofort beheben.

Für jedes numerische Attribut kann der Alarmschweregrad und der entsprechende Schwellenwert eingestellt werden. Der NMS-Service auf jedem Admin-Node überwacht kontinuierlich die aktuellen Attributwerte im Vergleich zu konfigurierten Schwellenwerten. Wenn ein Alarm ausgelöst wird, wird eine Benachrichtigung an alle designierten Mitarbeiter gesendet.

Beachten Sie, dass ein Schweregrad „Normal“ keinen Alarm auslöst.

Attributwerte werden anhand der Liste der aktivierten Alarme bewertet, die für dieses Attribut definiert wurden. Die Liste der Alarme wird in der folgenden Reihenfolge überprüft, um die erste Alarmklasse mit einem definierten und aktivierten Alarm für das Attribut zu finden:

1. Globale benutzerdefinierte Alarme mit Alarmabtrennungen von kritisch bis zur Mitteilung.
2. Standardalarme mit Alarmtrennungen von kritisch bis Notice.

Nachdem in der höheren Alarmklasse ein aktivierter Alarm für ein Attribut gefunden wurde, wird der NMS-Dienst nur innerhalb dieser Klasse ausgewertet. Der NMS-Dienst wird nicht mit den anderen Klassen mit niedrigerer Priorität bewertet. Wenn also ein globaler benutzerdefinierter Alarm für ein Attribut aktiviert ist, wertet der NMS-Dienst den Attributwert nur gegen globale benutzerdefinierte Alarme aus. Standardalarme werden nicht ausgewertet. Somit kann ein aktivierter Standardalarm für ein Attribut die Kriterien erfüllen, die zum Auslösen eines Alarms erforderlich sind. Er wird jedoch nicht ausgelöst, da ein globaler benutzerdefinierter Alarm (der nicht den angegebenen Kriterien entspricht) für dasselbe Attribut aktiviert ist. Es

wird kein Alarm ausgelöst und keine Benachrichtigung gesendet.

Beispiel für Alarmauslösung

Anhand dieses Beispiels können Sie verstehen, wie globale benutzerdefinierte Alarmer und Standardalarmer ausgelöst werden.

Im folgenden Beispiel ist ein Attribut mit einem globalen benutzerdefinierten Alarm und einem Standardalarm definiert und aktiviert, wie in der folgenden Tabelle dargestellt.

	Globale benutzerdefinierte Alarmschwelle (aktiviert)	Standard-Alarmschwellenwert (aktiviert)
Hinweis	>= 1500	>= 1000
Gering	>= 15,000	>= 1000
Major	>=150,000	>= 250,000

Wird das Attribut bei einem Wert von 1000 ausgewertet, wird kein Alarm ausgelöst und keine Benachrichtigung gesendet.

Der globale benutzerdefinierte Alarm hat Vorrang vor dem Standardalarm. Ein Wert von 1000 erreicht für den globalen benutzerdefinierten Alarm keinen Schwellenwert eines Schweregrads. Daher wird der Alarmpegel als normal bewertet.

Wenn nach dem obigen Szenario der globale benutzerdefinierte Alarm deaktiviert ist, ändert sich nichts. Der Attributwert muss neu bewertet werden, bevor eine neue Alarmstufe ausgelöst wird.

Wenn der globale benutzerdefinierte Alarm deaktiviert ist und der Attributwert neu bewertet wird, wird der Attributwert anhand der Schwellenwerte für den Standardalarm ausgewertet. Die Alarmstufe löst einen Alarm für die Benachrichtigungsstufe aus, und eine E-Mail-Benachrichtigung wird an das entsprechende Personal gesendet.

Alarmer desselben Schweregrads

Wenn zwei globale benutzerdefinierte Alarmer für dasselbe Attribut den gleichen Schweregrad haben, werden die Alarmer mit der Priorität „top down“ bewertet.

Wenn UMEM beispielsweise auf 50 MB abfällt, wird der erste Alarm ausgelöst (= 50000000), nicht jedoch der untere Alarm (<=100000000).



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		

Wird die Reihenfolge umgekehrt, wenn UMEM auf 100MB fällt, wird der erste Alarm (<=100000000) ausgelöst, nicht jedoch der darunter stehende Alarm (= 50000000).



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes

Benachrichtigungen

Eine Benachrichtigung meldet das Auftreten eines Alarms oder die Änderung des Status eines Dienstes. Alarmbenachrichtigungen können per E-Mail oder über SNMP gesendet werden.

Um zu vermeiden, dass bei Erreichen eines Alarmschwellenwerts mehrere Alarme und Benachrichtigungen gesendet werden, wird der Schweregrad des Alarms anhand des aktuellen Alarmschwerfalls für das Attribut überprüft. Wenn es keine Änderung gibt, dann werden keine weiteren Maßnahmen ergriffen. Das bedeutet, dass der NMS-Dienst das System weiterhin überwacht, nur ein Alarm ausgelöst und Benachrichtigungen sendet, wenn er zum ersten Mal einen Alarmzustand für ein Attribut bemerkt. Wenn ein neuer Wertschwellenwert für das Attribut erreicht und erkannt wird, ändert sich der Schweregrad des Alarms und eine neue Benachrichtigung wird gesendet. Die Alarme werden gelöscht, wenn die Zustände wieder auf den normalen Stand zurückkehren.

Der in der Benachrichtigung über einen Alarmzustand angezeigte Triggerwert wird auf drei Dezimalstellen

gerundet. Daher löst ein Attributwert von 1.9999 einen Alarm aus, dessen Schwellenwert unter (<) 2.0 liegt, obwohl die Alarmbenachrichtigung den Triggerwert als 2.0 anzeigt.

Neuer Services

Wenn neue Services durch Hinzufügen neuer Grid-Nodes oder -Standorte hinzugefügt werden, erben sie Standardalarme und globale benutzerdefinierte Alarme.

Alarme und Tabellen

In Tabellen angezeigte Alarmattribute können auf Systemebene deaktiviert werden. Alarme können für einzelne Zeilen in einer Tabelle nicht deaktiviert werden.

Die folgende Tabelle zeigt beispielsweise zwei kritische Einträge (VMFI)-Alarme. (Wählen Sie **SUPPORT > Tools > Grid-Topologie**. Wählen Sie dann **Storage-Node > SSM > Ressourcen**.)

Sie können den VMFI-Alarm so deaktivieren, dass der VMFI-Alarm der kritischen Stufe nicht ausgelöst wird (beide derzeit kritischen Alarme werden in der Tabelle grün angezeigt); Sie können jedoch einen einzelnen Alarm in einer Tabellenzeile nicht deaktivieren, sodass ein VMFI-Alarm als kritischer Alarmwert angezeigt wird, während der andere grün bleibt.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Quittierung aktueller Alarme (Legacy-System)

Ältere Alarme werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Wenn Sie die Liste der alten Alarme verringern oder löschen möchten, können Sie die Alarme bestätigen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über die Berechtigung zum Quittieren von Alarmen verfügen.

Über diese Aufgabe

Da das alte Alarmsystem weiterhin unterstützt wird, wird die Liste der alten Alarme auf der Seite Aktuelle Alarme bei jedem neuen Alarm erhöht. Sie können die Alarme in der Regel ignorieren (da Alarme eine bessere Sicht auf das System bieten) oder die Alarme quittieren.



Wenn Sie auf das Alarmsystem umgestellt haben, können Sie optional jeden älteren Alarm deaktivieren, um zu verhindern, dass er ausgelöst wird und der Anzahl der älteren Alarme hinzugefügt wird.

Wenn Sie einen Alarm quittieren, wird er nicht mehr auf der Seite „Aktuelle Alarme“ im Grid Manager aufgeführt, es sei denn, der Alarm wird auf der nächsten Schweregrade ausgelöst oder behoben und tritt erneut auf.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Aktueller Alarm** aus.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

Show Acknowledged Alarms

(1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show Records Per Page

Previous Next

2. Wählen Sie in der Tabelle den Dienstnamen aus.

Die Registerkarte Alarme für den ausgewählten Dienst wird angezeigt (**SUPPORT > Tools > Grid Topology > Grid Node > Service > Alarme**).

Overview	Alarms	Reports	Configuration
Main	History		



Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
 Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes 

3. Aktivieren Sie das Kontrollkästchen **quittieren** für den Alarm, und klicken Sie auf **Änderungen übernehmen**.

Der Alarm wird nicht mehr auf dem Armaturenbrett oder der Seite Aktuelle Alarme angezeigt.



Wenn Sie einen Alarm bestätigen, wird die Quittierung nicht auf andere Admin-Knoten kopiert. Wenn Sie das Dashboard von einem anderen Admin-Knoten aus anzeigen, wird der aktive Alarm möglicherweise weiterhin angezeigt.

4. Zeigen Sie bei Bedarf bestätigte Alarme an.
 - a. Wählen Sie **SUPPORT > Alarme (alt) > Aktueller Alarm** aus.
 - b. Wählen Sie **Bestätigte Alarme Anzeigen**.

Alle quittierten Alarme werden angezeigt.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 17:38:58 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable	2020-05-27 17:38:14 MDT

Show Records Per Page Previous « 1 » Next

Standardalarme anzeigen (Altsystem)

Sie können die Liste aller älteren Standardalarme anzeigen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Globale Alarme**.
2. Wählen Sie für Filter by die Option **Attributcode** oder **Attributname** aus.
3. Geben Sie für gleich ein Sternchen ein: *
4. Klicken Sie auf den Pfeil  Oder drücken Sie **Enter**.

Alle Standardalarme werden aufgelistet.



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

Default Alarms

Filter by equals

221 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Major	Greater than 10,000,000	>=	10000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Minor	Greater than 1,000,000	>=	1000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Notice	Greater than 150,000	>=	150000	
<input checked="" type="checkbox"/>		XCVF (% Completion)	Notice	Foreground Verification Completed	=	100	
<input checked="" type="checkbox"/>	ADC	ADCA (ADC Status)	Minor	Error	>=	10	
<input checked="" type="checkbox"/>	ADC	ADCE (ADC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ADC	ALIS (Inbound Attribute Sessions)	Notice	Over 100	>=	100	
<input checked="" type="checkbox"/>	ADC	ALOS (Outbound Attribute Sessions)	Notice	Over 200	>=	200	

Prüfen historischer Alarme und Alarmfrequenz (altes System)

Bei der Fehlerbehebung eines Problems können Sie überprüfen, wie oft in der Vergangenheit ein älterer Alarm ausgelöst wurde.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Führen Sie diese Schritte aus, um eine Liste aller Alarme zu erhalten, die über einen bestimmten Zeitraum ausgelöst wurden.
 - a. Wählen Sie **SUPPORT > Alarme (alt) > Historische Alarme**.
 - b. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie auf einen der Zeiträume.

- Geben Sie einen benutzerdefinierten Bereich ein, und klicken Sie auf **Benutzerdefinierte Abfrage**.
2. Befolgen Sie diese Schritte, um herauszufinden, wie oft Alarme für ein bestimmtes Attribut ausgelöst wurden.
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid Node > Service oder Component > Alarme > Historie** aus.
 - c. Wählen Sie das Attribut aus der Liste aus.
 - d. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie auf einen der Zeiträume.
 - Geben Sie einen benutzerdefinierten Bereich ein, und klicken Sie auf **Benutzerdefinierte Abfrage**.

Die Alarme werden in umgekehrter chronologischer Reihenfolge aufgeführt.

- e. Um zum Formular für die Anforderung des Alarmverlaufs zurückzukehren, klicken Sie auf **Historie**.

Globale benutzerdefinierte Alarme erstellen (altes System)

Sie haben möglicherweise globale benutzerdefinierte Alarme für das alte System verwendet, um bestimmte Überwachungsanforderungen zu erfüllen. Globale benutzerdefinierte Alarme können Alarmstufen haben, die Standardalarme überschreiben oder Attribute überwachen, die keinen Standardalarm haben.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Globale benutzerdefinierte Alarme überschreiben Standardalarme. Sie sollten die Standardalarmwerte nur dann ändern, wenn dies unbedingt erforderlich ist. Durch Ändern der Standardalarme besteht die Gefahr, Probleme zu verbergen, die sonst einen Alarm auslösen könnten.



Seien Sie vorsichtig, wenn Sie die Alarmeinstellungen ändern. Wenn Sie beispielsweise den Schwellenwert für einen Alarm erhöhen, können Sie ein zugrunde liegendes Problem möglicherweise nicht erkennen. Besprechen Sie Ihre vorgeschlagenen Änderungen mit dem technischen Support, bevor Sie eine Alarmeinstellung ändern.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Globale Alarme**.
2. Neue Zeile zur Tabelle „Globale benutzerdefinierte Alarme“ hinzufügen:
 - Um einen neuen Alarm hinzuzufügen, klicken Sie auf **Bearbeiten**  (Wenn dies der erste Eintrag ist) oder **Einfügen** .



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000		

Default Alarms

Filter by Attribute Code equals AR*

9 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000	
<input checked="" type="checkbox"/>	ARC	ARRF (Request Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARRV (Verification Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARVF (Store Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	NMS	ARRC (Remaining Capacity)	Notice	Below 10	<=	10	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Major	Disconnected	<=	9	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Notice	Standby	<=	19	

Apply Changes

- Um einen Standardalarm zu ändern, suchen Sie nach dem Standardalarm.
 - i. Wählen Sie unter Filter by entweder **Attributcode** oder **Attributname** aus.
 - ii. Geben Sie einen Suchstring ein.

Geben Sie vier Zeichen an oder verwenden Sie Platzhalter (z. B. A????). Oder ab*). Sternchen (*) stellen mehrere Zeichen dar und Fragezeichen (?) Stellt ein einzelnes Zeichen dar.

- iii. Klicken Sie auf den Pfeil Oder drücken Sie **Enter**.
- iv. Klicken Sie in der Ergebnisliste auf **Kopieren** Neben dem Alarm, den Sie ändern möchten.

Der Standardalarm wird in die Tabelle „Globale benutzerdefinierte Alarme“ kopiert.

3. Nehmen Sie alle erforderlichen Änderungen an den Einstellungen für globale benutzerdefinierte Alarme vor:

Überschrift	Beschreibung
Aktiviert	Aktivieren oder deaktivieren Sie das Kontrollkästchen, um den Alarm zu aktivieren oder zu deaktivieren.

Überschrift	Beschreibung
Attribut	Wählen Sie den Namen und den Code des zu überwachenden Attributs aus der Liste aller Attribute aus, die für den ausgewählten Dienst oder die ausgewählte Komponente gelten. Um Informationen über das Attribut anzuzeigen, klicken Sie auf Info  Neben dem Namen des Attributs.
Schweregrad	Das Symbol und der Text, der die Alarmstufe angibt.
Nachricht	Der Grund für den Alarm (Verbindung unterbrochen, Lagerraum unter 10 % usw.).
Operator	Operatoren für das Testen des aktuellen Attributwerts gegen den Wert-Schwellenwert: <ul style="list-style-type: none"> • = gleich • > größer als • < kleiner als • >= größer als oder gleich • <= kleiner als oder gleich • ≠ ist nicht gleich
Wert	Der Schwellenwert des Alarms, der zum Testen mit dem tatsächlichen Wert des Attributs über den Operator verwendet wird. Die Eingabe kann eine einzelne Zahl, eine Reihe von Zahlen mit einem Doppelpunkt (1:3) oder eine kommasetrennte Liste von Zahlen und Bereichen sein.
Zusätzliche Empfänger	Eine zusätzliche Liste der E-Mail-Adressen, die bei Auslösung des Alarms benachrichtigt werden sollen. Dies ist zusätzlich zur Mailingliste, die auf der Seite Alarme > E-Mail-Einrichtung konfiguriert ist. Listen sind durch Komma abgegrenzt. Hinweis: Mailinglisten erfordern die Einrichtung des SMTP-Servers. Bestätigen Sie vor dem Hinzufügen von Mailinglisten, dass SMTP konfiguriert ist. Benachrichtigungen für benutzerdefinierte Alarme können Benachrichtigungen von globalen benutzerdefinierten oder Standardalarmen überschreiben.
Aktionen	Steuertasten zu:  Bearbeiten Sie eine Zeile +  Eine Zeile einfügen +  Löschen Sie eine Zeile +  Ziehen Sie eine Zeile nach oben oder unten +  Kopieren Sie eine Zeile

4. Klicken Sie Auf **Änderungen Übernehmen**.

Deaktivieren von Alarmen (Legacy-System)

Die Alarme im alten Alarmsystem sind standardmäßig aktiviert, Sie können jedoch Alarme deaktivieren, die nicht erforderlich sind. Sie können auch die älteren Alarme deaktivieren, nachdem Sie vollständig auf das neue Alarmsystem umgestellt haben.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Deaktivieren eines Standardalarms (Legacy-System)

Sie können einen der älteren Standardalarme für das gesamte System deaktivieren.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Durch Deaktivieren eines Alarms für ein Attribut, das derzeit über einen Alarm ausgelöst wird, wird der aktuelle Alarm nicht gelöscht. Der Alarm wird deaktiviert, wenn das Attribut das nächste Mal den Alarmschwellenwert überschreitet, oder Sie können den ausgelösten Alarm löschen.



Deaktivieren Sie keine der älteren Alarme, bis Sie vollständig auf das neue Alarmsystem umgestellt haben. Andernfalls wird ein zugrunde liegendes Problem möglicherweise erst erkannt, wenn ein kritischer Vorgang nicht abgeschlossen wurde.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Globale Alarme**.
2. Suchen Sie nach dem Standardalarm, der deaktiviert werden soll.
 - a. Wählen Sie im Abschnitt Standardalarme die Option **Filtern nach > Attributcode** oder **Attributname** aus.
 - b. Geben Sie einen Suchstring ein.

Geben Sie vier Zeichen an oder verwenden Sie Platzhalter (z. B. A????). Oder ab*). Sternchen (*) stellen mehrere Zeichen dar und Fragezeichen (?) Stellt ein einzelnes Zeichen dar.
 - c. Klicken Sie auf den Pfeil Oder drücken Sie **Enter**.



Wenn Sie **deaktivierte Standardeinstellungen** auswählen, wird eine Liste aller derzeit deaktivierten Standardalarme angezeigt.

3. Klicken Sie in der Tabelle mit den Suchergebnissen auf das Symbol Bearbeiten Für den Alarm, den Sie deaktivieren möchten.



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

Default Alarms

Filter by equals

3 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Critical	Under 10000000	<=	10000000	
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Major	Under 50000000	<=	50000000	
<input type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 100000000	<=	100000000	

Apply Changes

Das Kontrollkästchen **enabled** für den ausgewählten Alarm wird aktiviert.

4. Deaktivieren Sie das Kontrollkästchen **aktiviert**.
5. Klicken Sie Auf **Änderungen Übernehmen**.

Der Standardalarm ist deaktiviert.

Globale benutzerdefinierte Alarme deaktivieren (Legacy-System)

Sie können einen veralteten globalen benutzerdefinierten Alarm für das gesamte System deaktivieren.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Durch Deaktivieren eines Alarms für ein Attribut, das derzeit über einen Alarm ausgelöst wird, wird der aktuelle Alarm nicht gelöscht. Der Alarm wird deaktiviert, wenn das Attribut das nächste Mal den Alarmschwellenwert überschreitet, oder Sie können den ausgelösten Alarm löschen.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Globale Alarme**.
2. Klicken Sie in der Tabelle Globale benutzerdefinierte Alarme auf **Bearbeiten** Neben dem Alarm, den Sie deaktivieren möchten.
3. Deaktivieren Sie das Kontrollkästchen **aktiviert**.



Global Custom Alarms (1 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>	All	RDTE (Tivoli Storage Manager State)	Major	Offline	=	10		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes

4. Klicken Sie Auf **Änderungen Übernehmen**.

Der globale benutzerdefinierte Alarm ist deaktiviert.

Ausgelöste Alarme löschen (Legacy-System)

Wenn ein älterer Alarm ausgelöst wird, können Sie ihn löschen, anstatt ihn zu bestätigen.

Bevor Sie beginnen

- Sie müssen die haben `Passwords.txt` Datei:

Durch Deaktivieren eines Alarms für ein Attribut, das derzeit einen Alarm ausgelöst hat, wird der Alarm nicht gelöscht. Bei der nächsten Änderung des Attributs wird der Alarm deaktiviert. Sie können den Alarm bestätigen oder, wenn Sie den Alarm sofort löschen möchten, anstatt zu warten, bis sich der Attributwert ändert (was zu einer Änderung des Alarmstatus führt), können Sie den ausgelösten Alarm löschen. Dies ist hilfreich, wenn Sie einen Alarm sofort gegen ein Attribut löschen möchten, dessen Wert sich nicht oft ändert (z. B. Attribute für den Status).

1. Deaktivieren Sie den Alarm.
2. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Starten Sie den NMS-Service neu: `service nms restart`
4. Melden Sie sich beim Admin-Knoten ab: `exit`

Der Alarm wurde gelöscht.

Benachrichtigungen für Alarme konfigurieren (Altsystem)

StorageGRID System kann automatisch E-Mails und senden "[SNMP-Benachrichtigungen](#)" Wenn ein Alarm ausgelöst wird oder sich ein Servicenstatus ändert.

Standardmäßig werden keine Alarm-E-Mail-Benachrichtigungen gesendet. Für E-Mail-Benachrichtigungen müssen Sie den E-Mail-Server konfigurieren und die E-Mail-Empfänger angeben. Für SNMP-Benachrichtigungen müssen Sie den SNMP-Agent konfigurieren.

Arten von Alarmanmeldungen (Legacy-System)

Wenn ein älterer Alarm ausgelöst wird, sendet das StorageGRID System zwei Arten von Alarmmeldungen: Schweregrad und Service-Status.

Benachrichtigungen auf Schweregraden

Eine Alarm-E-Mail-Benachrichtigung wird gesendet, wenn ein älterer Alarm auf einer ausgewählten Schweregrade ausgelöst wird:

- Hinweis
- Gering
- Major
- Kritisch

Eine Mailingliste erhält alle Benachrichtigungen, die sich auf den Alarm für den ausgewählten Schweregrad beziehen. Eine Benachrichtigung wird auch gesendet, wenn der Alarm den Alarmpegel verlässt – entweder durch eine Lösung oder durch Eingabe eines anderen Schweregrads.

Service-Status-Benachrichtigungen

Eine Benachrichtigung über den Servicenstatus wird gesendet, wenn ein Dienst (z. B. der LDR-Dienst oder der NMS-Dienst) den ausgewählten Servicenstatus eingibt und den ausgewählten Servicenstatus verlässt. Dienststatus-Benachrichtigungen werden gesendet, wenn ein Dienst einen der folgenden Servicenstatus eingibt oder verlässt:

- Unbekannt
- Administrativ Nach Unten

Eine Mailingliste erhält alle Benachrichtigungen, die sich auf Änderungen im ausgewählten Status beziehen.

E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)

Wenn StorageGRID E-Mail-Benachrichtigungen senden soll, wenn ein älterer Alarm ausgelöst wird, müssen Sie die SMTP-Mail-Server-Einstellungen angeben. Das StorageGRID System sendet nur E-Mails, es kann keine E-Mails empfangen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Verwenden Sie diese Einstellungen, um den SMTP-Server zu definieren, der für ältere E-Mail-

Benachrichtigungen und AutoSupport-E-Mail-Nachrichten verwendet wird. Diese Einstellungen werden nicht für Warnmeldungen verwendet.



Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, haben Sie möglicherweise bereits einen SMTP-Mail-Server konfiguriert. Derselbe SMTP-Server wird für Benachrichtigungen über Alarm-E-Mails verwendet, sodass Sie diesen Vorgang überspringen können. Siehe "[Anweisungen für die Administration von StorageGRID](#)".

SMTP ist das einzige Protokoll, das zum Senden von E-Mails unterstützt wird.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Server** aus.

Die Seite E-Mail-Server wird angezeigt. Auf dieser Seite wird auch der E-Mail-Server für AutoSupport-Meldungen konfiguriert.

Use these settings to define the email server used for alarm notifications and for AutoSupport messages. These settings are not used for alert notifications. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).



Email Server

Updated: 2016-03-17 11:11:59 PDT

E-mail Server (SMTP) Information

Mail Server	<input type="text"/>
Port	<input type="text"/>
Authentication	<input type="button" value="Off"/>
Authentication Credentials	Username: <input type="text" value="root"/>
	Password: <input type="password" value="....."/>
From Address	<input type="text"/>
Test E-mail	To: <input type="text"/>
	<input type="checkbox"/> Send Test E-mail

Apply Changes

3. Fügen Sie die folgenden SMTP-Mail-Server-Einstellungen hinzu:

Element	Beschreibung
Mailserver	IP-Adresse des SMTP-Mail-Servers. Sie können anstelle einer IP-Adresse einen Hostnamen eingeben, wenn Sie zuvor DNS-Einstellungen auf dem Admin-Knoten konfiguriert haben.
Port	Portnummer für den Zugriff auf den SMTP-Mail-Server.

Element	Beschreibung
Authentifizierung	Ermöglicht die Authentifizierung des SMTP-Mail-Servers. Standardmäßig ist die Authentifizierung deaktiviert.
Authentifizierungsdaten	Benutzername und Passwort des SMTP-Mail-Servers. Wenn die Authentifizierung auf ein festgelegt ist, müssen ein Benutzername und ein Passwort für den Zugriff auf den SMTP-Mail-Server angegeben werden.

4. Geben Sie unter **von Address** eine gültige E-Mail-Adresse ein, die der SMTP-Server als sendende E-Mail-Adresse erkennt. Dies ist die offizielle E-Mail-Adresse, von der die E-Mail-Nachricht gesendet wird.
5. Senden Sie optional eine Test-E-Mail, um zu bestätigen, dass die SMTP-Mail-Servereinstellungen korrekt sind.
 - a. Fügen Sie im Feld **E-Mail-Test > bis** eine oder mehrere Adressen hinzu, auf die Sie zugreifen können.

Sie können eine einzelne E-Mail-Adresse oder eine kommagetrennte Liste von E-Mail-Adressen eingeben. Da der NMS-Dienst den Erfolg oder Fehler beim Senden einer Test-E-Mail nicht bestätigt, müssen Sie den Posteingang des Testempfängers überprüfen können.

- b. Wählen Sie **Test-E-Mail senden**.

6. Klicken Sie Auf **Änderungen Übernehmen**.

Die SMTP-Mail-Server-Einstellungen werden gespeichert. Wenn Sie Informationen für eine Test-E-Mail eingegeben haben, wird diese E-Mail gesendet. Test-E-Mails werden sofort an den Mailserver gesendet und nicht über die Benachrichtigungswarteschlange gesendet. In einem System mit mehreren Admin-Nodes sendet jeder Admin-Node eine E-Mail. Der Empfang der Test-E-Mail bestätigt, dass Ihre SMTP-Mail-Server-Einstellungen korrekt sind und dass der NMS-Dienst erfolgreich eine Verbindung zum Mail-Server herstellt. Ein Verbindungsproblem zwischen dem NMS-Dienst und dem Mail-Server löst den Alarm für ältere MINUTEN (NMS Notification Status) auf der Stufe mit dem Schweregrad „Minor“ aus.

E-Mail-Vorlagen für Alarme erstellen (altes System)

Mithilfe von E-Mail-Vorlagen können Sie die Kopfzeile, Fußzeile und den Betreff einer früheren Alarm-E-Mail-Benachrichtigung anpassen. Sie können E-Mail-Vorlagen verwenden, um eindeutige Benachrichtigungen zu senden, die denselben Text an verschiedene Mailinglisten enthalten.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Mit diesen Einstellungen können Sie die E-Mail-Vorlagen festlegen, die für ältere Benachrichtigungen verwendet werden. Diese Einstellungen werden nicht für Warnmeldungen verwendet.

Für unterschiedliche Mailinglisten sind möglicherweise andere Kontaktinformationen erforderlich. Vorlagen enthalten keinen Haupttext der E-Mail-Nachricht.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Legacy E-Mail-Einrichtung**.

- Wählen Sie im Menü E-Mail die Option **Vorlagen**.
- Klicken Sie Auf **Bearbeiten**  (Oder **Einfügen**  Falls dies nicht die erste Vorlage ist).



Email Templates

Updated: 2016-03-17 11:21:54 PDT

Template (0 - 0 of 0)

Template Name	Subject Prefix	Header	Footer	Actions
Template One	Notifications	All Email Lists	From SGWS	  

Show Records Per Page



- Fügen Sie in der neuen Zeile Folgendes hinzu:

Element	Beschreibung
Vorlagenname	Eindeutiger Name zur Identifizierung der Vorlage. Vorlagennamen können nicht dupliziert werden.
Präfix Für Betreff	Optional Präfix, das am Anfang der Betreffzeile einer E-Mail angezeigt wird. Mit Präfixen können E-Mail-Filter einfach konfiguriert und Benachrichtigungen organisiert werden.
Kopfzeile	Optional Kopfzeilentext, der am Anfang des E-Mail-Nachrichtentextes erscheint. Der Kopfzeilentext kann verwendet werden, um den Inhalt der E-Mail-Nachricht mit Informationen wie Firmenname und Adresse zu versehen.
Fußzeile	Optional Fußzeilentext, der am Ende des E-Mail-Nachrichtentexts angezeigt wird. Über Fußzeile können Sie die eMail-Nachricht mit Erinnerungsdaten wie einer Telefonnummer oder einem Link zu einer Website schließen.

- Klicken Sie Auf **Änderungen Übernehmen**.

Es wird eine neue Vorlage für Benachrichtigungen hinzugefügt.

Erstellen von Mailinglisten für Alarmbenachrichtigungen (Altsystem)

Mit Mailinglisten können Sie Empfänger benachrichtigen, wenn ein älterer Alarm ausgelöst wird oder wenn sich ein Servicenstatus ändert. Sie müssen mindestens eine Mailingliste erstellen, bevor Sie Alarm-E-Mail-Benachrichtigungen senden können. Um eine Benachrichtigung an einen einzelnen Empfänger zu senden,

erstellen Sie eine Mailingliste mit einer E-Mail-Adresse.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie eine E-Mail-Vorlage für die Mailingliste (benutzerdefinierte Kopfzeile, Fußzeile und Betreffzeile) angeben möchten, müssen Sie die Vorlage bereits erstellt haben.

Über diese Aufgabe

Mit diesen Einstellungen können Sie die Mailinglisten definieren, die für Benachrichtigungen über ältere E-Mails verwendet werden. Diese Einstellungen werden nicht für Warnmeldungen verwendet.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Listen** aus.
3. Klicken Sie Auf **Bearbeiten**  (Oder *Einfügen*  Falls dies nicht die erste Mailingliste ist).



Email Lists

Updated: 2016-03-17 11:56:24 PDT

Lists (0 - 0 of 0)

Group Name	Recipients	Template	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	  

Show Records Per Page

« »



4. Fügen Sie in der neuen Zeile Folgendes hinzu:

Element	Beschreibung
Gruppenname	Eindeutiger Name zur Identifizierung der Mailingliste. Mailinglistenamen können nicht dupliziert werden. Hinweis: Wenn Sie den Namen einer Mailingliste ändern, wird die Änderung nicht an die anderen Standorte weitergegeben, die den Namen der Mailingliste verwenden. Sie müssen alle konfigurierten Benachrichtigungen manuell aktualisieren, um den neuen Namen der Mailingliste zu verwenden.
Empfänger	Eine einzelne E-Mail-Adresse, eine zuvor konfigurierte Mailingliste oder eine kommagetrennte Liste von E-Mail-Adressen und Mailinglisten, an die Benachrichtigungen gesendet werden. Hinweis: Wenn eine E-Mail-Adresse zu mehreren Mailinglisten gehört, wird nur eine E-Mail-Benachrichtigung gesendet, wenn ein Benachrichtigungserlösungs-Ereignis auftritt.

Element	Beschreibung
Vorlage	Wählen Sie optional eine E-Mail-Vorlage aus, um eine eindeutige Kopfzeile, Fußzeile und Betreffzeile zu Benachrichtigungen hinzuzufügen, die an alle Empfänger dieser Mailingliste gesendet werden.

5. Klicken Sie Auf **Änderungen Übernehmen**.

Es wird eine neue Mailingliste erstellt.

E-Mail-Benachrichtigungen für Alarmer konfigurieren (Legacy-System)

Um E-Mail-Benachrichtigungen für das ältere Alarmsystem zu erhalten, müssen die Empfänger Mitglied einer Mailingliste sein und diese Liste zur Seite Benachrichtigungen hinzugefügt werden. Benachrichtigungen werden so konfiguriert, dass E-Mails nur dann an Empfänger gesendet werden, wenn ein Alarm mit einem bestimmten Schweregrad ausgelöst wird oder wenn sich ein Servicenstatus ändert. Empfänger erhalten somit nur die Benachrichtigungen, die sie erhalten müssen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen eine E-Mail-Liste konfiguriert haben.

Über diese Aufgabe

Mit diesen Einstellungen können Sie Benachrichtigungen für ältere Alarmer konfigurieren. Diese Einstellungen werden nicht für Warnmeldungen verwendet.

Wenn eine E-Mail-Adresse (oder eine Liste) zu mehreren Mailinglisten gehört, wird nur eine E-Mail-Benachrichtigung gesendet, wenn ein Ereignis auftritt, bei dem eine Benachrichtigung ausgelöst wird. So kann beispielsweise eine Gruppe von Administratoren in Ihrem Unternehmen so konfiguriert werden, dass sie Benachrichtigungen für alle Alarmer unabhängig vom Schweregrad erhalten. Eine andere Gruppe benötigt möglicherweise nur Benachrichtigungen für Alarmer mit einem Schweregrad von „kritisch“. Sie können zu beiden Listen gehören. Wenn ein kritischer Alarm ausgelöst wird, erhalten Sie nur eine Benachrichtigung.

Schritte

1. Wählen Sie **SUPPORT > Alarmer (alt) > Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Benachrichtigungen** aus.
3. Klicken Sie Auf *Bearbeiten*  (Oder *Einfügen*  Wenn dies nicht die erste Benachrichtigung ist).
4. Wählen Sie unter E-Mail-Liste die Mailingliste aus.
5. Wählen Sie eine oder mehrere Alarmschweregrade und Servicestufen aus.
6. Klicken Sie Auf **Änderungen Übernehmen**.

Benachrichtigungen werden an die Mailingliste gesendet, wenn Alarmer mit dem ausgewählten Schweregrad „Alarm“ oder „Service“ ausgelöst oder geändert werden.

Alarbenachrichtigungen für eine Mailingliste unterdrücken (Älteres System)

Sie können Alarbenachrichtigungen für eine Mailingliste unterdrücken, wenn Sie nicht mehr möchten, dass die Mailingliste Benachrichtigungen über Alarme erhalten. Beispielsweise möchten Sie Benachrichtigungen über ältere Alarme unterdrücken, nachdem Sie zu Warnmeldungen gewechselt haben.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Verwenden Sie diese Einstellungen, um E-Mail-Benachrichtigungen für das ältere Alarmsystem zu unterdrücken. Diese Einstellungen gelten nicht für E-Mail-Benachrichtigungen.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Benachrichtigungen** aus.
3. Klicken Sie Auf **Bearbeiten**  Neben der Mailingliste, für die Sie Benachrichtigungen unterdrücken möchten.
4. Aktivieren Sie unter unterdrücken das Kontrollkästchen neben der Mailingliste, die Sie unterdrücken möchten, oder wählen Sie **unterdrücken** oben in der Spalte, um alle Mailinglisten zu unterdrücken.
5. Klicken Sie Auf **Änderungen Übernehmen**.

Ältere Alarbenachrichtigungen werden für die ausgewählten Mailinglisten unterdrückt.

Anzeigen von älteren Alarmen

Alarme (Altsystem) werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Sie können die derzeit aktiven Alarme auf der Seite Aktuelle Alarme anzeigen.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Aktueller Alarm** aus.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show Records Per Page Previous < 1 > Next

Das Alarmsymbol zeigt den Schweregrad jedes Alarms wie folgt an:

Symbol	Farbe	Alarmschweregrad	Bedeutung
	Gelb	Hinweis	Der Node ist mit dem Grid verbunden. Es ist jedoch eine ungewöhnliche Bedingung vorhanden, die den normalen Betrieb nicht beeinträchtigt.
	Hellorange	Gering	Der Node ist mit dem Raster verbunden, aber es existiert eine anormale Bedingung, die den Betrieb in Zukunft beeinträchtigen könnte. Sie sollten untersuchen, um eine Eskalation zu verhindern.
	Dunkelorange	Major	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die sich derzeit auf den Betrieb auswirkt. Um eine Eskalation zu vermeiden, ist eine sofortige Aufmerksamkeit erforderlich.
	Rot	Kritisch	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die normale Vorgänge angehalten hat. Sie sollten das Problem sofort beheben.

- Um mehr über das Attribut zu erfahren, das den Alarm ausgelöst hat, klicken Sie mit der rechten Maustaste auf den Attributnamen in der Tabelle.
- Um weitere Details zu einem Alarm anzuzeigen, klicken Sie in der Tabelle auf den Servicenamen.

Die Registerkarte Alarme für den ausgewählten Dienst wird angezeigt (**SUPPORT > Tools > Grid Topology > Grid Node > Service > Alarme**).



Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes

4. Wenn Sie die Anzahl der aktuellen Alarme löschen möchten, können Sie optional Folgendes tun:

- Bestätigen Sie den Alarm. Ein bestätigter Alarm wird nicht mehr in die Anzahl der älteren Alarme einbezogen, es sei denn, er wird auf der nächsten Stufe ausgelöst oder es wird behoben und tritt erneut auf.
- Deaktivieren Sie einen bestimmten Standardalarm oder einen globalen benutzerdefinierten Alarm für das gesamte System, um eine erneute Auslösung zu verhindern.

Verwandte Informationen

["Alarmreferenz \(Altsystem\)"](#)

["Quittierung aktueller Alarme \(Legacy-System\)"](#)

["Deaktivieren von Alarmen \(Legacy-System\)"](#)

Alarmreferenz (Altsystem)

In der folgenden Tabelle sind alle alten Standardalarme aufgeführt. Wenn ein Alarm ausgelöst wird, können Sie den Alarmcode in dieser Tabelle nach den empfohlenen Maßnahmen suchen.



Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Codieren	Name	Service	Empfohlene Maßnahmen
ABRL	Verfügbare Attributrelais	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	<p>Stellen Sie die Verbindung zu einem Dienst (einem ADC-Dienst) wieder her, der einen Attributrelais-Dienst so schnell wie möglich ausführt. Wenn keine verbundenen Attributrelais vorhanden sind, kann der Grid-Knoten keine Attributwerte an den NMS-Dienst melden. So kann der NMS-Dienst den Status des Dienstes nicht mehr überwachen oder Attribute für den Dienst aktualisieren.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
ACMS	Verfügbare Metadaten	BARC, BLDR, BCMN	<p>Ein Alarm wird ausgelöst, wenn ein LDR- oder ARC-Dienst die Verbindung zu einem DDS-Dienst verliert. In diesem Fall können die Aufnahme- und Abrufvorgänge nicht verarbeitet werden. Wenn die Nichtverfügbarkeit von DDS-Diensten nur ein kurzes vorübergehendes Problem ist, können Transaktionen verzögert werden.</p> <p>Überprüfen und Wiederherstellen der Verbindungen zu einem DDS-Dienst, um diesen Alarm zu löschen und den Service auf die volle Funktionalität zurückzugeben.</p>
AKTE	Status Des Cloud Tiering Service	LICHTBOGEN	<p>Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Cloud Tiering - Simple Storage Service (S3).</p> <p>Wenn das ATTRIBUT ACTS für den Archiv-Node auf Read-Only aktiviert oder Read-Write deaktiviert ist, müssen Sie das Attribut auf Read-Write aktiviert setzen.</p> <p>Wenn ein Hauptalarm aufgrund eines Authentifizierungsfehlers ausgelöst wird, überprüfen Sie ggf. die mit dem Ziel-Bucket verknüpften Anmeldeinformationen und aktualisieren Sie Werte.</p> <p>Wenn aus irgendeinem anderen Grund ein Großalarm ausgelöst wird, wenden Sie sich an den technischen Support.</p>
ADCA	ADC-Status	ADU	<p>Wenn ein Alarm ausgelöst wird, wählen Sie SUPPORT > Tools > Grid-Topologie. Wählen Sie dann site > GRID Node > ADC > Übersicht > Main und ADC > Alarme > Main, um die Ursache des Alarms zu bestimmen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
ADCE	ADC-Status	ADU	<p>Wenn der Wert des ADC-Status Standby lautet, setzen Sie die Überwachung des Dienstes fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht.</p> <p>Wenn der Wert des ADC-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
AITE	Status Abrufen	BARC	<p>Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM).</p> <p>Wenn der Wert für „Abruffzustand“ auf „Ziel“ wartet, prüfen Sie den TSM Middleware-Server und stellen Sie sicher, dass er ordnungsgemäß funktioniert. Wenn der Archivknoten gerade zum StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass die Verbindung des Archiv-Knotens zum angestrebten externen Archiv-Speichersystem korrekt konfiguriert ist.</p> <p>Wenn der Wert des Status „Archivabrueve“ Offline lautet, versuchen Sie, den Status auf Online zu aktualisieren. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > ARC > Abruf > Konfiguration > Main, wählen Sie Archiv Status abrufen > Online und klicken Sie auf Änderungen anwenden.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AITU	Status Abrufen	BARC	<p>Wenn der Wert für „Status abrufen“ als Zielfehler gilt, prüfen Sie das ausgewählte externe Archivspeichersystem auf Fehler.</p> <p>Wenn der Wert des Status „Archivabrueve“ auf „Sitzung verloren“ lautet, prüfen Sie das ausgewählte externe Archivspeichersystem, um sicherzustellen, dass es online ist und ordnungsgemäß funktioniert. Überprüfen Sie die Netzwerkverbindung mit dem Ziel.</p> <p>Wenn der Wert des Status „Archiv abrufen“ Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.</p>
ALIS	Eingehende Attributsitzungen	ADU	<p>Wenn die Anzahl der eingehenden Attributsitzungen in einem Attributrelais zu groß wird, kann dies ein Hinweis sein, dass das StorageGRID-System unausgewogen geworden ist. Unter normalen Bedingungen sollten Attributsitzungen gleichmäßig auf ADC-Dienste verteilt werden. Ein Ungleichgewicht kann zu Performance-Problemen führen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
ALOS	Ausgehende Attributsitzungen	ADU	Der ADC-Dienst verfügt über eine hohe Anzahl von Attributsitzungen und wird überlastet. Wenn dieser Alarm ausgelöst wird, wenden Sie sich an den technischen Support.
ALUR	Nicht Erreichbare Attributdatenbanken	ADU	Überprüfen Sie die Netzwerkverbindung mit dem NMS-Service, um sicherzustellen, dass der Dienst das Attribut-Repository kontaktieren kann. Wenn dieser Alarm ausgelöst wird und die Netzwerkverbindung gut ist, wenden Sie sich an den technischen Support.
AMQS	Audit-Nachrichten In Queued	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Audit-Meldungen nicht sofort an ein Audit-Relay oder Repository weitergeleitet werden können, werden die Meldungen in einer Datenträgerwarteschlange gespeichert. Wenn die Warteschlange voll wird, können Ausfälle auftreten. Um Ihnen die Möglichkeit zu geben, rechtzeitig zu reagieren, um einen Ausfall zu verhindern, werden AMQS-Alarme ausgelöst, wenn die Anzahl der Meldungen in der Datenträgerwarteschlange die folgenden Schwellenwerte erreicht: <ul style="list-style-type: none"> • Hinweis: Mehr als 100,000 Nachrichten • Minor: Mindestens 500,000 Nachrichten • Major: Mindestens 2,000,000 Nachrichten • Kritisch: Mindestens 5,000,000 Nachrichten Wenn ein AMQS-Alarm ausgelöst wird, überprüfen Sie die Belastung des Systems. Wenn eine beträchtliche Anzahl von Transaktionen vorhanden ist, sollte sich der Alarm im Laufe der Zeit lösen. In diesem Fall können Sie den Alarm ignorieren. Wenn der Alarm weiterhin besteht und der Schweregrad erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. Verringern Sie die Betriebsrate des Clients oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie den Audit-Level auf Fehler oder aus ändern. Siehe "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Codieren	Name	Service	Empfohlene Maßnahmen
AOTE	Store State	BARC	<p>Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM).</p> <p>Wenn der Wert des Speicherstatus auf Ziel wartet, prüfen Sie das externe Archivspeichersystem und stellen Sie sicher, dass es ordnungsgemäß funktioniert. Wenn der Archivknoten gerade zum StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass die Verbindung des Archiv-Knotens zum angestrebten externen Archiv-Speichersystem korrekt konfiguriert ist.</p> <p>Wenn der Wert des Store State Offline lautet, prüfen Sie den Wert des Store Status. Beheben Sie alle Probleme, bevor Sie den Store-Status wieder auf Online verschieben.</p>
AOTU	Speicherstatus	BARC	<p>Wenn der Wert des Speicherstatus „Sitzung verloren“ lautet, prüfen Sie, ob das externe Archivspeichersystem verbunden und online ist.</p> <p>Wenn der Wert von Zielfehler ist, überprüfen Sie das externe Archivspeichersystem auf Fehler.</p> <p>Wenn der Wert des Speicherstatus Unbekannter Fehler lautet, wenden Sie sich an den technischen Support.</p>
APMS	Storage Multipath-Konnektivität	SSM	<p>Wenn der Alarm für den Multipath-Status als „Dabgestuft“ angezeigt wird (wählen Sie UNTERSTÜTZUNG > Tools > Grid-Topologie, und wählen Sie dann site > Grid-Node > SSM > Ereignisse), gehen Sie wie folgt vor:</p> <ol style="list-style-type: none"> 1. Schließen Sie das Kabel an, das keine Kontrollleuchten anzeigt, oder ersetzen Sie es. 2. Warten Sie eine bis fünf Minuten. <p>Ziehen Sie das andere Kabel erst nach mindestens fünf Minuten ab, nachdem Sie das erste Kabel angeschlossen haben. Das zu frühe Auflösen kann dazu führen, dass das Root-Volume schreibgeschützt ist, was erfordert, dass die Hardware neu gestartet wird.</p> <ol style="list-style-type: none"> 3. Kehren Sie zur Seite SSM > Ressourcen zurück, und überprüfen Sie, ob der Multipath-Status im Abschnitt Speicherhardware in „DNominal“ geändert wurde.

Codieren	Name	Service	Empfohlene Maßnahmen
ARCE	BOGENZUSTAN D	LICHTBOGEN	<p>Der ARC-Dienst verfügt über einen Standby-Status, bis alle ARC-Komponenten (Replikation, Speicher, Abrufen, Ziel) gestartet wurden. Dann geht es zu Online.</p> <p>Wenn der Wert des ARC-Status nicht von Standby auf Online übergeht, überprüfen Sie den Status der ARC-Komponenten.</p> <p>Wenn der Wert für ARC-Status Offline lautet, starten Sie den Service neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AROQ	Objekte In Queued	LICHTBOGEN	<p>Dieser Alarm kann ausgelöst werden, wenn das Wechselspeichergerät aufgrund von Problemen mit dem angestrebten externen Archivspeichersystem langsam läuft oder wenn mehrere Lesefehler auftreten. Überprüfen Sie das externe Archiv-Storage-System auf Fehler und stellen Sie sicher, dass es ordnungsgemäß funktioniert.</p> <p>In manchen Fällen kann dieser Fehler auf eine hohe Datenanforderung zurückzuführen sein. Überwachen Sie die Anzahl der Objekte, die sich in der Warteschlange befinden, bei abnehmender Systemaktivität.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
ARRF	Anfragefehler	LICHTBOGEN	<p>Wenn ein Abruf aus dem Zielspeichersystem zur externen Archivierung fehlschlägt, versucht der Archivknoten den Abruf erneut, da der Ausfall durch ein vorübergehendes Problem verursacht werden kann. Wenn die Objektdaten jedoch beschädigt sind oder als dauerhaft nicht verfügbar markiert wurden, schlägt der Abruf nicht fehl. Stattdessen wird der Archivknoten kontinuierlich erneut versucht, den Abruf erneut zu versuchen, und der Wert für Anforderungsfehler steigt weiter.</p> <p>Dieser Alarm kann darauf hinweisen, dass die Speichermedien, auf denen die angeforderten Daten gespeichert sind, beschädigt sind. Überprüfen Sie das externe Archiv-Storage-System, um das Problem weiter zu diagnostizieren.</p> <p>Wenn Sie feststellen, dass die Objektdaten nicht mehr im Archiv sind, muss das Objekt aus dem StorageGRID System entfernt werden. Weitere Informationen erhalten Sie vom technischen Support.</p> <p>Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > ARC > Abruf > Konfiguration > Main, wählen Sie Fehleranzahl der Anforderung zurücksetzen und klicken Sie auf Änderungen anwenden.</p>
ARRV	Verifizierungsfehler	LICHTBOGEN	<p>Wenden Sie sich an den technischen Support, um das Problem zu diagnostizieren und zu beheben.</p> <p>Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > ARC > Abrufen > Konfiguration > Main, wählen Sie Fehleranzahl der Überprüfung zurücksetzen und klicken Sie auf Änderungen anwenden.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
ARVF	Speicherfehler	LICHTBOGEN	<p>Dieser Alarm kann aufgrund von Fehlern im externen Archivspeichersystem auftreten. Überprüfen Sie das externe Archiv-Storage-System auf Fehler und stellen Sie sicher, dass es ordnungsgemäß funktioniert.</p> <p>Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > ARC > Abrufen > Konfiguration > Main, wählen Sie Anzahl der Fehler im Store zurücksetzen und klicken Sie auf Änderungen anwenden.</p>
ASXP	Revisionsfreigaben	AMS	<p>Ein Alarm wird ausgelöst, wenn der Wert der Revisionsfreigaben Unbekannt ist. Dieser Alarm kann auf ein Problem bei der Installation oder Konfiguration des Admin-Knotens hinweisen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AUMA	AMS-Status	AMS	<p>Wenn der Wert für AMS Status DB-Verbindungsfehler ist, starten Sie den Grid-Node neu.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AUME	AMS-Status	AMS	<p>Wenn der Wert des AMS-Status Standby lautet, fahren Sie mit der Überwachung des StorageGRID-Systems fort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p> <p>Wenn der Wert von AMS-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AUXS	Exportstatus Prüfen	AMS	<p>Wenn ein Alarm ausgelöst wird, beheben Sie das zugrunde liegende Problem und starten Sie dann den AMS-Dienst neu.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
HINZUFÜGEN	Anzahl Ausgefallener Speicher-Controller-Laufwerke	SSM	<p>Dieser Alarm wird ausgelöst, wenn ein oder mehrere Laufwerke in einem StorageGRID-Gerät ausgefallen sind oder nicht optimal sind. Ersetzen Sie die Laufwerke nach Bedarf.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
BASF	Verfügbare Objektkenne- n	CMN	<p>Wenn ein StorageGRID System bereitgestellt wird, wird dem CMN-Service eine feste Anzahl von Objekt-IDs zugewiesen. Dieser Alarm wird ausgelöst, wenn das StorageGRID-System seine Versorgung mit Objektkennungen ausgibt.</p> <p>Wenden Sie sich an den technischen Support, um weitere Kennungen zuzuweisen.</p>
BASS	Identifizier Block Zuordnungsstatu- s	CMN	<p>Standardmäßig wird ein Alarm ausgelöst, wenn Objektbezeichner nicht zugewiesen werden können, da das ADC-Quorum nicht erreicht werden kann.</p> <p>Die Zuweisung von Identifizier-Blöcken im CMN-Dienst erfordert ein Quorum (50 % + 1) der ADC-Dienste, dass sie online und verbunden sind. Wenn das Quorum nicht verfügbar ist, kann der CMN-Dienst erst dann neue Identifizierungsblöcke zuweisen, wenn das ADC-Quorum wiederhergestellt ist. Bei Verlust des ADC-Quorums entstehen im Allgemeinen keine unmittelbaren Auswirkungen auf das StorageGRID-System (Kunden können weiterhin Inhalte aufnehmen und abrufen), da die Lieferung von Identifikatoren innerhalb eines Monats an anderer Stelle im Grid zwischengespeichert wird. Wenn der Zustand jedoch fortgesetzt wird, kann das StorageGRID-System nicht mehr neue Inhalte aufnehmen.</p> <p>Wenn ein Alarm ausgelöst wird, untersuchen Sie den Grund für den Verlust von ADC-Quorum (z. B. ein Netzwerk- oder Speicherknoten-Ausfall) und ergreifen Sie Korrekturmaßnahmen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
BRDT	Temperatur Im Computing-Controller-Chassis	SSM	<p>Ein Alarm wird ausgelöst, wenn die Temperatur des Compute-Controllers in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet.</p> <p>Prüfen Sie die Hardware-Komponenten und Umweltprobleme auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	<p>Ein Alarm wird ausgelöst, wenn die Servicezeit (Sekunden) erheblich von der Betriebssystemzeit abweicht. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Servicezeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
BTSE	Uhrstatus	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	<p>Ein Alarm wird ausgelöst, wenn die Servicezeit nicht mit der vom Betriebssystem erfassten Zeit synchronisiert wird. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Zeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
CAHP	Java Heap-Nutzung In Prozent	DDS	<p>Ein Alarm wird ausgelöst, wenn Java die Garbage-Sammlung nicht mit einer Rate durchführen kann, die genügend Heap-Speicherplatz für eine ordnungsgemäße Funktion des Systems zulässt. Ein Alarm kann einen Benutzer-Workload anzeigen, der die im System verfügbaren Ressourcen für den DDS-Metadatenpeicher überschreitet. Überprüfen Sie die ILM-Aktivität im Dashboard, oder wählen Sie SUPPORT > Tools > Grid-Topologie, und wählen Sie dann site > Grid Node > DDS > Ressourcen > Übersicht > Main aus.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
CASA	Data Store-Status	DDS	<p>Wenn der Cassandra-Metadatenpeicher nicht mehr verfügbar ist, wird ein Alarm ausgelöst.</p> <p>Den Status von Cassandra überprüfen:</p> <ol style="list-style-type: none"> 1. Melden Sie sich beim Storage-Node als admin und an <code>su</code> Um das Root-Kennwort zu verwenden, das in der Datei <code>Passwords.txt</code> angegeben ist. 2. Geben Sie Ein: <code>service cassandra status</code> 3. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: <code>service cassandra restart</code> <p>Dieser Alarm kann auch zeigen, dass der Metadatenpeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert.</p> <p>Weitere Informationen zur Fehlerbehebung im Alarm <code>Services: Status - Cassandra (SVST)</code> in "Behebung von Metadatenproblemen".</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
FALL	Datenspeicherstatus	DDS	<p>Dieser Alarm wird während der Installation oder Erweiterung ausgelöst, um anzuzeigen, dass ein neuer Datenspeicher in das Raster eingespeist wird.</p>
CCNA	Computing-Hardware	SSM	<p>Dieser Alarm wird ausgelöst, wenn der Status der Hardware des Computing-Controllers in einer StorageGRID-Appliance zu beachten ist.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
CDLP	Belegter Speicherplatz Für Metadaten (Prozent)	DDS	<p>Dieser Alarm wird ausgelöst, wenn der effektive Metadatenraum (Metadaten Effective Space, CEMS) 70 % voll (kleiner Alarm), 90 % voll (Hauptalarm) und 100 % voll (kritischer Alarm) erreicht.</p> <p>Wenn dieser Alarm den Schwellenwert von 90 % erreicht, wird im Grid Manager eine Warnung auf dem Dashboard angezeigt. Sie müssen eine Erweiterung durchführen, um neue Speicherknoten so schnell wie möglich hinzuzufügen. Siehe "Erweitern Sie Ihr Raster".</p> <p>Wenn dieser Alarm den Schwellenwert von 100 % erreicht, müssen Sie die Aufnahme von Objekten beenden und Speicherknoten sofort hinzufügen. Cassandra erfordert eine bestimmte Menge an Speicherplatz zur Durchführung wichtiger Vorgänge wie Data-Compaction und Reparatur. Diese Vorgänge sind betroffen, wenn Objekt-Metadaten mehr als 100 % des zulässigen Speicherplatzes beanspruchen. Unerwünschte Ergebnisse können auftreten.</p> <p>Hinweis: Wenden Sie sich an den technischen Support, wenn Sie keine Speicherknoten hinzufügen können.</p> <p>Nachdem neue Speicherknoten hinzugefügt wurden, gleicht das System die Objektmetadaten automatisch auf alle Speicherknoten aus, und der Alarm wird gelöscht.</p> <p>Siehe auch Informationen zur Fehlerbehebung für die Warnmeldung zu niedrigem Metadaten-Speicher in "Behebung von Metadatenproblemen".</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
CMNA	CMN-Status	CMN	<p>Wenn der Wert von CMN Status Fehler ist, wählen Sie SUPPORT > Tools > Grid Topology und dann site > Grid Node > CMN > Übersicht > Main und CMN > Alarme > Main aus, um die Fehlerursache zu ermitteln und das Problem zu beheben.</p> <p>Ein Alarm wird ausgelöst, und der Wert von CMN Status ist kein Online CMN während einer Hardwareaktualisierung des primären Admin-Knotens, wenn die CMNS geschaltet werden (der Wert des alten CMN-Status ist Standby und das neue ist Online).</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
CPRC	Verbleibende Kapazität	NMS	<p>Ein Alarm wird ausgelöst, wenn die verbleibende Kapazität (Anzahl der verfügbaren Verbindungen, die für die NMS-Datenbank geöffnet werden können) unter den konfigurierten Alarmschwerwert fällt.</p> <p>Wenn ein Alarm ausgelöst wird, wenden Sie sich an den technischen Support.</p>
CPSA	Compute Controller Netzteil A	SSM	<p>Wenn ein Problem mit der Stromversorgung A im Rechencontroller eines StorageGRID-Geräts auftritt, wird ein Alarm ausgelöst.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p>
CPSB	Compute Controller Netzteil B	SSM	<p>Bei einem StorageGRID-Gerät wird ein Alarm ausgelöst, wenn ein Problem mit der Stromversorgung B im Compute-Controller auftritt.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p>
KFUT	CPU-Temperatur für Compute Controller	SSM	<p>Ein Alarm wird ausgelöst, wenn die Temperatur der CPU im Compute-Controller in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet.</p> <p>Wenn es sich bei dem Speicherknoten um eine StorageGRID-Appliance handelt, gibt das StorageGRID-System an, dass eine Warnung für den Controller erforderlich ist.</p> <p>Prüfen Sie die Probleme mit den Hardwarekomponenten und der Umgebung auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
DNST	DNS-Status	SSM	Nach Abschluss der Installation wird im SSM-Service ein DNST-Alarm ausgelöst. Nachdem der DNS konfiguriert wurde und die neuen Serverinformationen alle Grid-Knoten erreichen, wird der Alarm abgebrochen.
ECCD	Beschädigte Fragmente Erkannt	LDR	<p>Ein Alarm wird ausgelöst, wenn die Hintergrundüberprüfung ein korruptes Fragment mit Löschungscode erkennt. Wenn ein beschädigtes Fragment erkannt wird, wird versucht, das Fragment neu zu erstellen. Setzen Sie die beschädigten Fragmente zurück, und kopieren Sie verlorene Attribute auf Null, und überwachen Sie sie, um zu sehen, ob die Zählung wieder hoch geht. Wenn die Anzahl steigt, kann es ein Problem mit dem zugrunde liegenden Speicher des Storage-Node geben. Eine Kopie von Objektdaten mit Löschungscode wird erst dann als fehlend betrachtet, wenn die Anzahl der verlorenen oder korrupten Fragmente die Fehlertoleranz des Löschcodes verletzt. Daher ist es möglich, ein korruptes Fragment zu haben und das Objekt trotzdem abrufen zu können.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
ACST	Verifizierungsstatus	LDR	<p>Dieser Alarm zeigt den aktuellen Status des Hintergrundverifizierungsverfahrens für das Löschen codierter Objektdaten auf diesem Speicherknoten an.</p> <p>Bei der Hintergrundüberprüfung wird ein Großalarm ausgelöst.</p>
FOPN	Dateibeschreibung Öffnen	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Das FOPN kann während der Spitzenaktivität groß werden. Wenn der Support in Phasen mit langsamer Aktivität nicht geschmälert wird, wenden Sie sich an den technischen Support.
HSTE	HTTP-Status	BLDR	Siehe Empfohlene Maßnahmen für HSTU.

Codieren	Name	Service	Empfohlene Maßnahmen
HSTU	HTTP-Status	BLDR	<p>HSTE und HSTU beziehen sich auf HTTP für allen LDR-Datenverkehr, einschließlich S3, Swift und anderem internen StorageGRID-Datenverkehr. Ein Alarm zeigt an, dass eine der folgenden Situationen aufgetreten ist:</p> <ul style="list-style-type: none"> • HTTP wurde manuell in den Offline-Modus versetzt. • Das Attribut Auto-Start HTTP wurde deaktiviert. • Der LDR-Service wird heruntergefahren. <p>Das Attribut Auto-Start HTTP ist standardmäßig aktiviert. Wenn diese Einstellung geändert wird, kann HTTP nach einem Neustart offline bleiben.</p> <p>Warten Sie gegebenenfalls, bis der LDR-Service neu gestartet wurde.</p> <p>Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann Storage Node > LDR > Konfiguration aus. Wenn HTTP offline ist, stellen Sie es online. Vergewissern Sie sich, dass das Attribut Auto-Start HTTP aktiviert ist.</p> <p>Wenn HTTP offline bleibt, wenden Sie sich an den technischen Support.</p>
HTAS	Automatisches Starten von HTTP	LDR	<p>Gibt an, ob HTTP-Dienste beim Start automatisch gestartet werden sollen. Dies ist eine vom Benutzer angegebene Konfigurationsoption.</p>
IRSU	Status Der Eingehenden Replikation	BLDR, BARC	<p>Ein Alarm zeigt an, dass die eingehende Replikation deaktiviert wurde. Konfigurationseinstellungen bestätigen: Wählen Sie SUPPORT > Tools > Grid-Topologie. Wählen Sie dann site > Grid Node > LDR > Replikation > Konfiguration > Main aus.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
LATA	Durchschnittliche Latenz	NMS	<p>Überprüfen Sie auf Verbindungsprobleme.</p> <p>Überprüfen Sie die Systemaktivität, um zu bestätigen, dass die Systemaktivität erhöht wird. Eine Erhöhung der Systemaktivität führt zu einer Erhöhung der Attributdatenaktivität. Diese erhöhte Aktivität führt zu einer Verzögerung bei der Verarbeitung von Attributdaten. Dies kann normale Systemaktivität sein und wird unterseiten.</p> <p>Auf mehrere Alarmer prüfen. Eine Erhöhung der durchschnittlichen Latenzzeit kann durch eine übermäßige Anzahl von ausgelösten Alarmen angezeigt werden.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
LDRE	LDR-Status	LDR	<p>Wenn der Wert des LDR-Status Standby lautet, setzen Sie die Überwachung der Situation fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht.</p> <p>Wenn der Wert für den LDR-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
VERLOREN	Verlorene Objekte	DDS, LDR	<p>Wird ausgelöst, wenn das StorageGRID System eine Kopie des angeforderten Objekts von einer beliebigen Stelle im System nicht abrufen kann. Bevor ein Alarm VERLOREN GEGANGENE (verlorene Objekte) ausgelöst wird, versucht das System, ein fehlendes Objekt von einem anderen Ort im System abzurufen und zu ersetzen.</p> <p>Verloren gegangene Objekte stellen einen Datenverlust dar. Das Attribut Lost Objects wird erhöht, wenn die Anzahl der Speicherorte eines Objekts auf Null fällt, ohne dass der DDS-Service den Inhalt absichtlich löscht, um der ILM-Richtlinie gerecht zu werden.</p> <p>Untersuchen SIE VERLORENE (VERLORENE Objekte) Alarme sofort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p> <p>"Fehlerbehebung bei verlorenen und fehlenden Objektdaten"</p>

Codieren	Name	Service	Empfohlene Maßnahmen
MCEP	Ablauf Des Managementschnittstelle-Zertifikats	CMN	<p>Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf die Managementoberfläche verwendet wird, kurz vor Ablauf steht.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Grid Manager die Option KONFIGURATION > Sicherheit > Zertifikate. 2. Wählen Sie auf der Registerkarte Global die Option Management Interface Certificate aus. 3. "Laden Sie ein neues Zertifikat für die Managementoberfläche hoch."
MINQ	E-Mail-Benachrichtigungen in Warteschlange	NMS	<p>Überprüfen Sie die Netzwerkverbindungen der Server, auf denen der NMS-Dienst und der externe Mail-Server gehostet werden. Bestätigen Sie außerdem, dass die Konfiguration des E-Mail-Servers korrekt ist.</p> <p>"E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)"</p>
MIN	E-Mail-Benachrichtigungsstatus	BNMS	<p>Ein kleiner Alarm wird ausgelöst, wenn der NMS-Dienst keine Verbindung zum Mail-Server herstellen kann. Überprüfen Sie die Netzwerkverbindungen der Server, auf denen der NMS-Dienst und der externe Mail-Server gehostet werden. Bestätigen Sie außerdem, dass die Konfiguration des E-Mail-Servers korrekt ist.</p> <p>"E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)"</p>
MISS	Status der NMS-Schnittstellen-Engine	BNMS	<p>Ein Alarm wird ausgelöst, wenn die NMS-Schnittstellen-Engine auf dem Admin-Knoten, der Schnittstelleninhalte erfasst und generiert, vom System getrennt wird. Überprüfen Sie Server Manager, ob die Server-individuelle Anwendung ausgefallen ist.</p>
NANG	Einstellung Für Automatische Netzwerkaushandlung	SSM	<p>Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen.</p> <p>Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
NDUP	Einstellungen Für Den Netzwerkduplex	SSM	Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen. Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.
NLNK	Network Link Detect	SSM	Überprüfen Sie die Netzwerkverbindungen am Port und am Switch. Überprüfen Sie die Netzwerk-Router-, Switch- und Adapterkonfigurationen. Starten Sie den Server neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
RER	Fehler Beim Empfang	SSM	Die folgenden Ursachen können für NRER-Alarme sein: <ul style="list-style-type: none"> • Fehler bei der Vorwärtskorrektur (FEC) stimmen nicht überein • Switch-Port und MTU-NIC stimmen nicht überein • Hohe Link-Fehlerraten • NIC-Klingelpuffer überlaufen Weitere Informationen zur Fehlerbehebung im NRER-Alarm (Network Receive Error) in finden Sie unter "Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen" .
NRLY	Verfügbare Audit-Relais	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Überwachungsrelais nicht mit ADC-Diensten verbunden sind, können keine Überwachungsereignisse gemeldet werden. Sie werden in eine Warteschlange eingereiht und stehen Benutzern nicht zur Verfügung, bis die Verbindung wiederhergestellt ist. Stellen Sie die Verbindung so schnell wie möglich zu einem ADC-Dienst wieder her. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NSCA	NMS-Status	NMS	Wenn der Wert des NMS-Status DB-Verbindungsfehler ist, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
NSCE	Bundesland des NMS	NMS	<p>Wenn der Wert für den NMS-Status Standby lautet, setzen Sie die Überwachung fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht.</p> <p>Wenn der Wert für NMS-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
NSPD	Schnell	SSM	<p>Dies kann durch Probleme mit der Netzwerkverbindung oder der Treiberkompatibilität verursacht werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
NTBR	Freie Tablespace	NMS	<p>Wenn ein Alarm ausgelöst wird, überprüfen Sie, wie schnell sich die Datenbanknutzung geändert hat. Ein plötzlicher Abfall (im Gegensatz zu einer allmählichen Änderung im Laufe der Zeit) weist auf eine Fehlerbedingung hin. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p> <p>Durch das Anpassen des Alarmschwellenwerts können Sie proaktiv verwalten, wenn zusätzlicher Storage zugewiesen werden muss.</p> <p>Wenn der verfügbare Speicherplatz einen niedrigen Schwellenwert erreicht (siehe Alarmschwelle), wenden Sie sich an den technischen Support, um die Datenbankanweisung zu ändern.</p>
NTER	Übertragungsfehler	SSM	<p>Diese Fehler können beseitigt werden, ohne manuell zurückgesetzt zu werden. Wenn sie nicht gelöscht werden, überprüfen Sie die Netzwerkhardware. Überprüfen Sie, ob die Adapterhardware und der Treiber korrekt installiert und konfiguriert sind, um mit Ihren Netzwerk-Routern und Switches zu arbeiten.</p> <p>Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > SSM > Ressourcen > Konfiguration > Main, wählen Sie Zurücksetzen Fehleranzahl für Übertragung zurücksetzen und klicken Sie auf Änderungen anwenden.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
NTFQ	NTP-Frequenzverschiebung	SSM	Wenn der Frequenzversatz den konfigurierten Schwellenwert überschreitet, tritt wahrscheinlich ein Hardwareproblem mit der lokalen Uhr auf. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um einen Austausch zu vereinbaren.
NTLK	NTP Lock	SSM	Wenn der NTP-Daemon nicht an eine externe Zeitquelle gebunden ist, überprüfen Sie die Netzwerkverbindung zu den angegebenen externen Zeitquellen, deren Verfügbarkeit und deren Stabilität.
NTOF	NTP-Zeitverschiebung	SSM	Wenn der Zeitversatz den konfigurierten Schwellenwert überschreitet, liegt wahrscheinlich ein Hardwareproblem mit dem Oszillator der lokalen Uhr vor. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um einen Austausch zu vereinbaren.
NTSJ	Gewählte Zeitquelle Jitter	SSM	Dieser Wert gibt die Zuverlässigkeit und Stabilität der Zeitquelle an, die NTP auf dem lokalen Server als Referenz verwendet. Wenn ein Alarm ausgelöst wird, kann es ein Hinweis sein, dass der Oszillator der Zeitquelle defekt ist oder dass ein Problem mit der WAN-Verbindung zur Zeitquelle besteht.
NTSU	NTP-Status	SSM	Wenn der Wert von NTP Status nicht ausgeführt wird, wenden Sie sich an den technischen Support.
OPST	Gesamtstromstatus	SSM	Wenn die Stromversorgung eines StorageGRID-Geräts von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Überprüfen Sie den Status von Netzteil A oder B, um festzustellen, welches Netzteil normal funktioniert. Falls erforderlich, ersetzen Sie das Netzteil.

Codieren	Name	Service	Empfohlene Maßnahmen
OQRT	Objekte Isoliert	LDR	<p>Nachdem die Objekte automatisch vom StorageGRID-System wiederhergestellt wurden, können die isolierten Objekte aus dem Quarantäneverzeichnis entfernt werden.</p> <ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. 2. Wählen Sie Standort > Storage Node > LDR > Verifizierung > Konfiguration > Main. 3. Wählen Sie Gesperrte Objekte Löschen. 4. Klicken Sie Auf Änderungen Übernehmen. <p>Die isolierten Objekte werden entfernt und die Zählung wird auf Null zurückgesetzt.</p>
ORSU	Status Der Ausgehenden Replikation	BLDR, BARC	<p>Ein Alarm zeigt an, dass eine ausgehende Replikation nicht möglich ist: Der Speicher befindet sich in einem Zustand, in dem Objekte nicht abgerufen werden können. Ein Alarm wird ausgelöst, wenn die ausgehende Replikation manuell deaktiviert wird. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > LDR > Replikation > Konfiguration aus.</p> <p>Wenn der LDR-Dienst nicht zur Replikation verfügbar ist, wird ein Alarm ausgelöst. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > GRID Node > LDR > Storage aus.</p>
OSLF	Shelf-Status	SSM	<p>Ein Alarm wird ausgelöst, wenn der Status einer der Komponenten im Speicher-Shelf einer Speichereinrichtung beeinträchtigt ist. Zu den Komponenten des Lagerregals gehören die IOMs, Lüfter, Netzteile und Laufwerksfächer. Wenn dieser Alarm ausgelöst wird, lesen Sie die Wartungsanleitung für Ihr Gerät.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
PMEM	Speicherauslastung Des Service (In Prozent)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	<p>Kann einen Wert von mehr als Y% RAM haben, wobei Y den Prozentsatz des Speichers repräsentiert, der vom Server verwendet wird.</p> <p>Zahlen unter 80 % sind normal. Über 90 % wird als Problem betrachtet.</p> <p>Wenn die Speicherauslastung für einen einzelnen Dienst hoch ist, überwachen Sie die Situation und untersuchen Sie sie.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
PSAS	Stromversorgung A-Status	SSM	<p>Wenn die Stromversorgung A in einem StorageGRID-Gerät von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst.</p> <p>Ersetzen Sie bei Bedarf das Netzteil A.</p>
PSBS	Netzteil B Status	SSM	<p>Wenn die Stromversorgung B eines StorageGRID-Geräts von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst.</p> <p>Falls erforderlich, ersetzen Sie das Netzteil B.</p>
RDTE	Status Von Tivoli Storage Manager	BARC	<p>Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM).</p> <p>Wenn der Wert des Status von Tivoli Storage Manager Offline lautet, überprüfen Sie den Status von Tivoli Storage Manager, und beheben Sie alle Probleme.</p> <p>Versetzen Sie die Komponente wieder in den Online-Modus. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > ARC > Ziel > Konfiguration > Main, wählen Sie Tivoli Storage Manager State > Online und klicken Sie auf Änderungen anwenden.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
RDTU	Status Von Tivoli Storage Manager	BARC	<p>Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM).</p> <p>Wenn der Wert des Tivoli Storage Manager Status auf Konfigurationsfehler gesetzt ist und der Archivknoten gerade dem StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass der TSM Middleware-Server richtig konfiguriert ist.</p> <p>Wenn der Wert des Tivoli Storage Manager-Status auf Verbindungsfehler oder Verbindungsfehler liegt, überprüfen Sie erneut die Netzwerkkonfiguration auf dem TSM Middleware-Server und die Netzwerkverbindung zwischen dem TSM Middleware-Server und dem StorageGRID-System.</p> <p>Wenn der Wert des Tivoli Storage Manager-Status Authentifizierungsfehler oder Authentifizierungsfehler beim erneuten Verbinden lautet, kann das StorageGRID-System eine Verbindung zum TSM-Middleware-Server herstellen, kann die Verbindung jedoch nicht authentifizieren. Überprüfen Sie, ob der TSM Middleware-Server mit dem richtigen Benutzer, Kennwort und Berechtigungen konfiguriert ist, und starten Sie den Service neu.</p> <p>Wenn der Wert des Tivoli Storage Manager Status als Sitzungsfehler lautet, ist eine etablierte Sitzung unerwartet verloren gegangen. Überprüfen Sie die Netzwerkverbindung zwischen dem TSM Middleware-Server und dem StorageGRID-System. Überprüfen Sie den Middleware-Server auf Fehler.</p> <p>Wenn der Wert von Tivoli Storage Manager Status Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
RIRF	Eingehende Replikationen — Fehlgeschlagen	BLDR, BARC	<p>Eingehende Replikationen – fehlgeschlagener Alarm kann während Zeiten hoher Auslastung oder temporärer Netzwerkstörungen auftreten. Wenn die Systemaktivität verringert wird, sollte dieser Alarm gelöscht werden. Wenn die Anzahl der fehlgeschlagenen Replikationen weiter zunimmt, suchen Sie nach Netzwerkproblemen und überprüfen Sie, ob die LDR- und ARC-Quell- und Zieldienste online und verfügbar sind.</p> <p>Um die Zählung zurückzusetzen, wählen Sie SUPPORT > Tools > Grid-Topologie und dann site > Grid-Knoten > LDR > Replikation > Konfiguration > Main. Wählen Sie Anzahl der fehlgeschlagene Inbound-Replikation zurücksetzen und klicken Sie auf Änderungen anwenden.</p>
RIRQ	Eingehende Replikationen — In Warteschlange	BLDR, BARC	<p>Alarmer können in Zeiten hoher Auslastung oder temporärer Netzwerkstörungen auftreten. Wenn die Systemaktivität verringert wird, sollte dieser Alarm gelöscht werden. Wenn die Anzahl der Replikationen in der Warteschlange weiter steigt, suchen Sie nach Netzwerkproblemen und überprüfen Sie, ob die LDR- und ARC-Dienste von Quelle und Ziel online und verfügbar sind.</p>
RORQ	Ausgehende Replikationen — In Warteschlange	BLDR, BARC	<p>Die Warteschlange für ausgehende Replizierung enthält Objektdaten, die kopiert werden, um ILM-Regeln und von Clients angeforderte Objekte zu erfüllen.</p> <p>Ein Alarm kann aufgrund einer Systemüberlastung auftreten. Warten Sie, bis der Alarm gelöscht wird, wenn die Systemaktivität abnimmt. Wenn der Alarm erneut auftritt, fügen Sie die Kapazität durch Hinzufügen von Speicherknoten hinzu.</p>
SAVP	Nutzbarer Speicherplatz (Prozent)	LDR	<p>Wenn der nutzbare Speicherplatz einen niedrigen Schwellenwert erreicht, können Sie unter anderem das Erweitern des StorageGRID-Systems oder das Verschieben von Objektdaten in die Archivierung über einen Archiv-Node einschließen.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SCAS	Status	CMN	<p>Wenn der Wert des Status für die aktive Grid-Aufgabe Fehler ist, suchen Sie die Grid-Task-Meldung. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > CMN > Grid Tasks > Übersicht > Main aus. Die Grid-Aufgabenmeldung zeigt Informationen zum Fehler an (z. B. „Check failed on Node 12130011“).</p> <p>Nachdem Sie das Problem untersucht und behoben haben, starten Sie die Grid-Aufgabe neu. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > Grid Node > CMN > Grid Tasks > Konfiguration > Main aus, und wählen Sie Aktionen > Ausführen.</p> <p>Wenn der Wert für Status für eine angespendete Grid-Aufgabe „Fehler“ lautet, versuchen Sie erneut, die Grid-Aufgabe zu beenden.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SCEP	Ablaufdatum des Storage API-Service-Endpoints-Zertifikats	CMN	<p>Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, kurz vor Ablauf steht.</p> <ol style="list-style-type: none"> 1. Wählen Sie KONFIGURATION > Sicherheit > Zertifikate. 2. Wählen Sie auf der Registerkarte Global S3 und Swift API Zertifikat. 3. "Laden Sie ein neues S3- und Swift-API-Zertifikat hoch."
SCHR	Status	CMN	<p>Wenn der Wert von Status für die Aufgabe des historischen Rasters nicht belegt ist, untersuchen Sie den Grund und führen Sie die Aufgabe bei Bedarf erneut aus.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SCSA	Storage Controller A	SSM	<p>Wenn in einer StorageGRID-Appliance ein Problem mit Storage Controller A auftritt, wird ein Alarm ausgelöst.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SCSB	Storage Controller B	SSM	<p>Wenn ein Problem mit dem Storage Controller B in einer StorageGRID-Appliance auftritt, wird ein Alarm ausgelöst.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p> <p>Einige Appliance-Modelle besitzen keinen Storage Controller B.</p>
SHLH.	Systemzustand	LDR	<p>Wenn der Wert „Systemzustand“ für einen Objektspeicher „Fehler“ lautet, prüfen und korrigieren Sie Folgendes:</p> <ul style="list-style-type: none"> • Probleme mit dem zu montiertem Volume • Fehler im Filesystem
SLSA	CPU-Auslastung durchschnittlich	SSM	<p>Je höher der Wert des Busiers des Systems.</p> <p>Wenn der CPU-Lastdurchschnitt weiterhin mit einem hohen Wert besteht, sollte die Anzahl der Transaktionen im System untersucht werden, um zu ermitteln, ob dies zu diesem Zeitpunkt aufgrund einer hohen Last liegt. Ein Diagramm des CPU-Lastdurchschnitts anzeigen: Wählen Sie SUPPORT > Tools > Grid-Topologie. Wählen Sie dann site > GRID Node > SSM > Ressourcen > Berichte > Diagramme aus.</p> <p>Wenn die Belastung des Systems nicht hoch ist und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SMST	Überwachungsstatus Protokollieren	SSM	<p>Wenn der Wert des Protokollüberwachungsstatus für einen anhaltenden Zeitraum nicht verbunden ist, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SMTT	Ereignisse Insgesamt	SSM	<p>Wenn der Wert von Total Events größer als Null ist, prüfen Sie, ob bekannte Ereignisse (z. B. Netzwerkfehler) die Ursache sein können. Wenn diese Fehler nicht gelöscht wurden (d. h., die Anzahl wurde auf 0 zurückgesetzt), können Alarmer für Ereignisse insgesamt ausgelöst werden.</p> <p>Wenn ein Problem behoben ist, setzen Sie den Zähler zurück, um den Alarm zu löschen. Wählen Sie NODES > site > Grid Node > Events > Ereignisanzahl zurücksetzen aus.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung zur Konfiguration der Grid-Topologie-Seite verfügen. </div> <p>Wenn der Wert für „Total Events“ null ist oder die Anzahl erhöht wird und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SNST	Status	CMN	<p>Ein Alarm zeigt an, dass ein Problem beim Speichern der Grid-Task-Bundles vorliegt. Wenn der Wert von Status Checkpoint Error oder Quorum nicht erreicht ist, bestätigen Sie, dass ein Großteil der ADC-Dienste mit dem StorageGRID-System verbunden ist (50 Prozent plus einer) und warten Sie dann einige Minuten.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SOSS	Status Des Storage- Betriebssystems	SSM	<p>Ein Alarm wird ausgelöst, wenn SANtricity OS anzeigt, dass ein Problem mit einer Komponente in einer StorageGRID-Appliance „needs Aufmerksamkeit“ vorliegt.</p> <p>Wählen Sie KNOTEN. Wählen Sie dann Appliance Storage Node > Hardware. Blättern Sie nach unten, um den Status der einzelnen Komponenten anzuzeigen. Überprüfen Sie unter SANtricity OS die anderen Gerätekomponenten, um das Problem zu isolieren.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SSMA	SSM-Status	SSM	<p>Wenn der Wert des SSM Status Fehler ist, wählen Sie SUPPORT > Tools > Grid Topology und dann site > Grid Node > SSM > Übersicht > Main und SSM > Übersicht > Alarme, um die Ursache des Alarms zu bestimmen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SSME	SSM-Status	SSM	<p>Wenn der Wert des SSM-Status „Standby“ lautet, setzen Sie die Überwachung fort, und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht.</p> <p>Wenn der Wert für SSM-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SSTS	Storage-Status	BLDR	<p>Wenn der Wert des Speicherstatus nicht genügend verwendbarer Speicherplatz ist, ist auf dem Speicherknoten kein verfügbarer Speicherplatz mehr verfügbar. Die Datenausgabewerte werden auf andere verfügbare Speicherknoten umgeleitet. Abruf-Anfragen können weiterhin von diesem Grid-Node bereitgestellt werden.</p> <p>Zusätzlicher Speicher sollte hinzugefügt werden. Sie wirkt sich nicht auf die Funktionen des Endbenutzers aus, aber der Alarm bleibt bestehen, bis zusätzlicher Speicher hinzugefügt wird.</p> <p>Wenn der Wert für den Speicherstatus „Volume(s) nicht verfügbar“ ist, steht ein Teil des Speichers nicht zur Verfügung. Speicher und Abruf von diesen Volumes ist nicht möglich. Weitere Informationen erhalten Sie im Status des Volumes: Wählen Sie SUPPORT > Tools > Grid-Topologie. Wählen Sie dann site > GRID Node > LDR > Storage > Übersicht > Main aus. Die Gesundheit des Volumes ist unter Objektspeichern aufgeführt.</p> <p>Wenn der Wert des Speicherstatus Fehler ist, wenden Sie sich an den technischen Support.</p> <p>"Fehlersuche im SSTS-Alarm (Storage Status) durchführen"</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SVST	Status	SSM	<p>Dieser Alarm wird gelöscht, wenn andere Alarme im Zusammenhang mit einem nicht laufenden Dienst gelöst werden. Verfolgen Sie die Alarme des Quelldienstes, um den Vorgang wiederherzustellen.</p> <p>Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > GRID Node > SSM > Services > Übersicht > Main aus. Wenn der Status eines Dienstes als nicht ausgeführt angezeigt wird, ist sein Status „Administrativ ausgefallen“. Der Status des Dienstes kann aus folgenden Gründen als nicht ausgeführt angegeben werden:</p> <ul style="list-style-type: none"> • Der Dienst wurde manuell beendet (<code>/etc/init.d/<service> stop</code>). • Es liegt ein Problem mit der MySQL-Datenbank vor, und der Server Manager fährt den MI-Dienst herunter. • Ein Grid-Node wurde hinzugefügt, aber nicht gestartet. • Während der Installation ist ein Grid-Node noch nicht mit dem Admin-Node verbunden. <p>Wenn ein Dienst als nicht ausgeführt aufgeführt ist, starten Sie den Dienst neu (<code>/etc/init.d/<service> restart</code>).</p> <p>Dieser Alarm kann auch zeigen, dass der Metadatenpeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p> <p>"Fehlersuche im Alarm Services: Status - Cassandra (SVST) durchführen"</p>
TMEM.	Installierter Speicher	SSM	<p>Nodes, die mit weniger als 24 gib des installierten Speichers ausgeführt werden, können zu Performance-Problemen und Systeminstabilität führen. Die Menge des auf dem System installierten Arbeitsspeichers sollte auf mindestens 24 gib erhöht werden.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
POP	Ausstehende Vorgänge	ADU	Eine Meldungswarteschlange kann darauf hinweisen, dass der ADC-Dienst überlastet ist. Es können zu wenige ADC-Dienste an das StorageGRID-System angeschlossen werden. In einer großen Implementierung kann der ADC-Service Computing-Ressourcen hinzufügen oder das System benötigt zusätzliche ADC-Services.
UMEM	Verfügbare Speicher	SSM	Wenn der verfügbare RAM knapp wird, prüfen Sie, ob es sich um ein Hardware- oder Softwareproblem handelt. Wenn es sich nicht um ein Hardwareproblem handelt oder wenn der verfügbare Speicher unter 50 MB liegt (der Standard-Alarmschwellenwert), wenden Sie sich an den technischen Support.
VMFI	Einträge Verfügbar	SSM	Dies deutet darauf hin, dass zusätzlicher Speicherplatz benötigt wird. Wenden Sie sich an den technischen Support.
VMFR	Speicherplatz Verfügbar	SSM	Wenn der Wert des verfügbaren Speicherplatzes zu niedrig wird (siehe Alarmschwellen), muss untersucht werden, ob sich die Log-Dateien aus dem Verhältnis heraus entwickeln oder Objekte, die zu viel Speicherplatz beanspruchen (siehe Alarmschwellen), die reduziert oder gelöscht werden müssen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
VMST	Status	SSM	Ein Alarm wird ausgelöst, wenn der Wert Status für das Bereitstellungsvolumen Unbekannt ist. Der Wert Unbekannt oder Offline kann darauf hinweisen, dass das Volume aufgrund eines Problems mit dem zugrunde liegenden Speichergerät nicht bereitgestellt oder darauf zugegriffen werden kann.
VPRI	Überprüfungspriorität	BLDR, BARC	Standardmäßig ist der Wert der Überprüfungspriorität adaptiv. Wenn die Überprüfungspriorität auf hoch eingestellt ist, wird ein Alarm ausgelöst, da die Speicherüberprüfung den normalen Betrieb des Dienstes verlangsamen kann.

Codieren	Name	Service	Empfohlene Maßnahmen
VSTU	Status Der Objektüberprüfung	BLDR	<p>Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann site > GRID Node > LDR > Storage > Übersicht > Main aus.</p> <p>Überprüfen Sie das Betriebssystem auf Anzeichen von Block- oder Dateisystemfehlern.</p> <p>Wenn der Wert des Objektverifizierungsstatus Unbekannter Fehler ist, weist er in der Regel auf ein niedriges Dateisystem- oder Hardwareproblem (I/O-Fehler) hin, das den Zugriff der Speicherverifizierung auf gespeicherte Inhalte verhindert. Wenden Sie sich an den technischen Support.</p>
XAMS	Nicht Erreichbare Audit-Repositorys	BADC, BARC, BCLB, BCMN, BLDR, BNMS	<p>Überprüfen Sie die Netzwerkverbindung mit dem Server, der den Admin-Node hostet.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Referenz für Protokolldateien

Referenz für Protokolldateien: Übersicht

StorageGRID stellt Protokolle bereit, die zum Erfassen von Ereignissen, Diagnosemeldungen und Fehlerbedingungen verwendet werden. Möglicherweise werden Sie gebeten, Protokolldateien zu sammeln und an den technischen Support zu leiten, um bei der Fehlerbehebung zu helfen.

Die Protokolle werden wie folgt kategorisiert:

- ["StorageGRID-Softwareprotokolle"](#)
- ["Protokoll für Implementierung und Wartung"](#)
- ["Protokolle für Drittanbietersoftware"](#)
- ["Etwa bycast.log"](#)



Die Details, die für jeden Protokolltyp angegeben sind, dienen nur als Referenz. Die Protokolle sind für erweiterte Fehlerbehebung durch den technischen Support bestimmt. Fortschrittliche Techniken, die die Wiederherstellung des Problemverlaufs mit Hilfe der Audit-Protokolle und der Anwendung Log-Dateien beinhalten, liegen über den Umfang dieser Anweisungen hinaus.

Greifen Sie auf die Protokolle zu

Um auf die Protokolle zuzugreifen, können Sie ["Erfassen von Protokolldateien und Systemdaten"](#) Von einem oder mehreren Knoten als Single-Log-Datei-Archiv. Wenn der primäre Admin-Node nicht verfügbar ist oder einen bestimmten Knoten nicht erreichen kann, können Sie für jeden Grid-Knoten wie folgt auf einzelne Protokolldateien zugreifen:

1. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
2. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
3. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
4. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Kategorien von Protokolldateien

Das Archiv der StorageGRID-Protokolldatei enthält die für jede Kategorie beschriebenen Protokolle sowie zusätzliche Dateien, die Metriken und die Ausgabe des Debug-Befehls enthalten.

Speicherort der Archivierung	Beschreibung
Prüfung	Während des normalen Systembetriebs erzeugte Überwachungsmeldungen.
Protokolle von Base-os	Informationen zu Betriebssystemen, einschließlich StorageGRID-Image-Versionen
Pakete	Globale Konfigurationsinformationen (Bundles)
cassandra	Cassandra Datenbankinformationen und Reaper Reparaturprotokolle.
eg	VCSs-Informationen über den aktuellen Knoten und EC-Gruppeninformationen nach Profil-ID.
Raster	Allgemeine Grid-Protokolle einschließlich Debug (<code>bycast.log</code>) Und <code>servermanager</code> Protokolle:
grid.xml	Die Grid-Konfigurationsdatei ist über alle Nodes hinweg freigegeben.
Hagroups	Hochverfügbarkeitsgruppen – Kennzahlen und Protokolle
Installieren	<code>Gdu-server</code> Und installieren Protokolle.
lumberjack.log	Debug-Meldungen im Zusammenhang mit Protokollerfassung.
Lambda-Schiedsrichter	Protokolle in Verbindung mit der S3 Select Proxy-Anforderung.
Metriken	Service-Protokolle für Grafana, Jaeger, Node Exporter und Prometheus.
Falsch	Miscd-Zugriffs- und Fehlerprotokolle.
mysql	Die Konfiguration der MariaDB-Datenbank und die zugehörigen Protokolle.
Netz	Protokolle, die von netzwerkbezogenen Skripten und dem dynIP-Dienst erstellt werden.

Speicherort der Archivierung	Beschreibung
Nginx	Konfigurationsdateien und Protokolle für den Load Balancer und den Grid Federation Beinhaltet außerdem Traffic-Protokolle: Grid Manager und Tenant Manager.
Nginx-gw	Konfigurationsdateien und Protokolle für den Load Balancer und den Grid Federation
ntp	NTP-Konfigurationsdatei und -Protokolle
betriebssystem	Node- und Grid-Statusdatei, einschließlich Services <code>pid</code> .
Andere	Log-Dateien unter <code>/var/local/log</code> Die nicht in anderen Ordnern gesammelt werden.
perf-	Performance-Informationen für CPU-, Netzwerk- und Festplatten-I/O.
prometheus-Data	Aktuelle Prometheus-Kennzahlen, wenn die Log-Sammlung Prometheus-Daten enthält.
Bereitstellung	Protokolle im Zusammenhang mit dem Grid-Bereitstellungsprozess.
Floß	Protokolle aus dem in Plattformservices verwendeten Raft-Cluster.
ssh	Protokolle für SSH-Konfiguration und -Dienst.
snmp	SNMP-Agent-Konfiguration und Alarmzulassungs-/Deny-Listen, die für das Senden von SNMP-Benachrichtigungen verwendet werden.
Steckdosen-Daten	Sockendaten für Netzwerk-Debug.
system-commands.txt	Ausgabe von StorageGRID-Containerbefehlen. Enthält Systeminformationen wie z. B. Netzwerk- und Festplattenverwendung.

StorageGRID-Softwareprotokolle

Sie können StorageGRID-Protokolle verwenden, um Probleme zu beheben.



Wenn Sie Ihre Protokolle an einen externen Syslog-Server senden möchten oder das Ziel von Audit-Informationen wie z. B. den ändern möchten `bycast.log` und `nms.log`, Siehe ["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#).

Allgemeine StorageGRID-Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/bycast.log	Die primäre StorageGRID-Fehlerbehebungsdatei. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann Site > Node > SSM > Events aus.	Alle Nodes
/Var/local/log/bycast-err.log	Enthält eine Untergruppe von <code>bycast.log</code> (Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“). WICHTIGE Meldungen werden auch im System angezeigt. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann Site > Node > SSM > Events aus.	Alle Nodes
/Var/local/Core/	Enthält alle Core Dump-Dateien, die erstellt wurden, wenn das Programm normal beendet wird. Mögliche Ursachen sind Assertion Failures, Verstöße oder Thread Timeouts. Hinweis: Die Datei <code>`/var/local/core/kexec_cmd</code> ist normalerweise auf Appliance-Knoten vorhanden und weist keinen Fehler auf.	Alle Nodes

Verschlüsselungsbezogene Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/ssh-config-generation.log	Enthält Protokolle zum Generieren von SSH-Konfigurationen und zum Neuladen von SSH-Services.	Alle Nodes
/Var/local/log/nginx/config-generation.log	Enthält Protokolle zum Generieren von nginx-Konfigurationen und zum Neuladen von nginx-Diensten.	Alle Nodes
/Var/local/log/nginx-gw/config-generation.log	Enthält Protokolle zur Erstellung von nginx-gw-Konfigurationen (und zum Neuladen von nginx-gw-Diensten).	Admin- und Gateway-Nodes
/Var/local/log/update-cipher-configurations.log	Enthält Protokolle zur Konfiguration von TLS- und SSH-Richtlinien.	Alle Nodes

Protokolle der Grid-Föderation

Dateiname	Hinweise	Gefunden am
/Var/local/log/update_grid_federation_config.log	Enthält Protokolle zur Erstellung von nginx- und nginx-gw-Konfigurationen für Netzverbundverbindungen.	Alle Nodes

NMS-Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/nms.log	<ul style="list-style-type: none"> • Erfasst Benachrichtigungen vom Grid Manager und dem Tenant Manager. • Erfasst Ereignisse im Zusammenhang mit dem Betrieb des NMS-Dienstes, z. B. Alarmverarbeitung, E-Mail-Benachrichtigungen und Konfigurationsänderungen. • Enthält XML-Paketaktualisierungen, die aus Konfigurationsänderungen im System resultieren. • Enthält Fehlermeldungen zum Attribut Downsampling, das einmal täglich ausgeführt wird. • Enthält Java-Web-Server-Fehlermeldungen, z. B. Fehler beim Generieren der Seite und HTTP-Status 500-Fehler. 	Admin-Nodes
/Var/local/log/nms.errlog	<p>Enthält Fehlermeldungen bezüglich der MySQL-Datenbank-Upgrades.</p> <p>Enthält den Standardfehlerstrom (Stderr) der entsprechenden Dienste. Pro Dienst gibt es eine Protokolldatei. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.</p>	Admin-Nodes
/Var/local/log/nms.requestlog	Enthält Informationen über ausgehende Verbindungen von der Management-API zu internen StorageGRID-Diensten.	Admin-Nodes

Server Manager-Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/servermanager.log	Protokolldatei für die auf dem Server ausgeführte Server Manager-Anwendung.	Alle Nodes
/Var/local/log/GridstatBackend.errlog	Protokolldatei für die Back-End-Anwendung der Server Manager-GUI.	Alle Nodes
/Var/local/log/gridstat.errlog	Protokolldatei für die Benutzeroberfläche von Server Manager.	Alle Nodes

StorageGRID Serviceprotokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/acct.errlog		Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/adc.errlog	Enthält den Standardfehlerstrom (Stderr) der entsprechenden Dienste. Pro Dienst gibt es eine Protokolldatei. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/ams.errlog		Admin-Nodes
/Var/local/log/Arc.errlog		Archiv-Nodes
/Var/local/log/cassandra/system.log	Informationen für den Metadatenpeicher (Cassandra-Datenbank), die verwendet werden können, wenn Probleme beim Hinzufügen neuer Storage-Nodes auftreten oder wenn der nodetool-Reparaturauftrag abgestellt wird.	Storage-Nodes
/Var/local/log/cassandra-reaper.log	Informationen zum Cassandra Reaper Service, der Reparaturen der Daten in der Cassandra-Datenbank durchführt.	Storage-Nodes
/Var/local/log/cassandra-reaper.errlog	Fehlerinformationen für den Cassandra Reaper Service.	Storage-Nodes
/Var/local/log/chunk.errlog		Storage-Nodes

Dateiname	Hinweise	Gefunden am
/Var/local/log/cmn.errlog		Admin-Nodes
/Var/local/log/cms.errlog	Diese Protokolldatei ist möglicherweise auf Systemen vorhanden, die von einer älteren StorageGRID-Version aktualisiert wurden. Er enthält Informationen zu Altsystemen.	Storage-Nodes
/Var/local/log/cts.errlog	Diese Protokolldatei wird nur erstellt, wenn der Zieltyp Cloud Tiering - Simple Storage Service (S3) ist.	Archiv-Nodes
/Var/local/log/dds.errlog		Storage-Nodes
/Var/local/log/dmv.errlog		Storage-Nodes
/Var/local/log/dynap*	Enthält Protokolle zum Dynap-Dienst, der das Grid auf dynamische IP-Änderungen überwacht und die lokale Konfiguration aktualisiert.	Alle Nodes
/Var/local/log/grafana.log	Das mit dem Grafana-Service verknüpfte Protokoll, das für die Visualisierung von Kennzahlen im Grid Manager verwendet wird.	Admin-Nodes
/Var/local/log/hagroups.log	Das Protokoll, das mit Hochverfügbarkeitsgruppen verknüpft ist.	Admin-Nodes und Gateway-Nodes
/Var/local/log/hagroups_events.log	Verfolgt Statusänderungen, beispielsweise den Übergang von BACKUP zu MASTER oder FEHLER.	Admin-Nodes und Gateway-Nodes
/Var/local/log/idnt.errlog		Speicherknotten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/jaeger.log	Das Protokoll, das mit dem jaeger-Dienst verknüpft ist, das für die Trace-Erfassung verwendet wird.	Alle Nodes
/Var/local/log/kstn.errlog		Speicherknotten, auf denen der ADC-Service ausgeführt wird

Dateiname	Hinweise	Gefunden am
/Var/local/log/Lambda*	Enthält Protokolle für den S3 Select-Service.	Admin- und Gateway-Nodes Dieses Protokoll enthält nur bestimmte Admin- und Gateway-Knoten. Siehe " S3 Select Anforderungen und Einschränkungen für Admin und Gateway Nodes ".
/Var/local/log/ldr.errlog		Storage-Nodes
/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 sowie zum Verwalten von Umgebungsconfigurationen auf dem Node bereitstellt, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Nodes
/Var/local/log/nginx/*.log	Enthält Protokolle für den nginx-Dienst, der als Authentifizierung 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 Nodes
/Var/local/log/nginx-gw/*.log	Enthält allgemeine Protokolle für den nginx-gw-Dienst, einschließlich Fehlerprotokolle und Protokolle für die eingeschränkten Admin-Ports auf Admin-Knoten.	Admin-Nodes und Gateway-Nodes
/Var/local/log/nginx-gw/cgr-access.log.gz	Enthält Zugriffsprotokolle für den Grid-übergreifenden Replikationsdatenverkehr.	Admin-Nodes, Gateway-Nodes oder beides, basierend auf der Grid-Federation-Konfiguration. Nur im Zielraster für die Grid-übergreifende Replikation gefunden.

Dateiname	Hinweise	Gefunden am
/Var/local/log/nginx-gw/endpoint-access.log.gz	Die Lösung enthält Zugriffsprotokolle für den Load Balancer, der einen Lastausgleich für den S3- und Swift-Datenverkehr von Clients zu Storage Nodes ermöglicht.	Admin-Nodes und Gateway-Nodes
/Var/local/log/persistence*	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Root-Festplatte verwaltet, die bei einem Neustart erhalten bleiben müssen.	Alle Nodes
/Var/local/log/prometheus.log	Enthält für alle Knoten das Service-Protokoll für den Knoten-Exporter und das Kennzahlungsprotokoll der ade-Exporter. Für Admin-Knoten enthält auch Protokolle für die Prometheus- und Alert Manager-Dienste.	Alle Nodes
/Var/local/log/raft.log	Enthält die Ausgabe der Bibliothek, die vom RSM-Dienst für das Raft-Protokoll verwendet wird.	Storage-Nodes mit RSM-Service
/Var/local/log/RMS.errlog	Enthält Protokolle für den RSM-Service (Replicated State Machine Service), der für S3-Plattformservices verwendet wird.	Storage-Nodes mit RSM-Service
/Var/local/log/ssm.errlog		Alle Nodes
/Var/local/log/update-s3vs-domains.log	Enthält Protokolle zur Verarbeitung von Updates für die Konfiguration virtueller gehosteter S3-Domänennamen. Siehe Anweisungen für die Implementierung von S3-Client-Applikationen.	Admin- und Gateway-Nodes
/Var/local/log/Update-snmp-Firewall.*	Enthalten Protokolle im Zusammenhang mit den Firewall-Ports, die für SNMP verwaltet werden.	Alle Nodes
/Var/local/log/update-syslog.log	Enthält Protokolle in Bezug auf Änderungen an der Syslog-Konfiguration des Systems.	Alle Nodes
/Var/local/log/update-traffic-classes.log	Enthält Protokolle, die sich auf Änderungen an der Konfiguration von Traffic-Klassifikatoren beziehen.	Admin- und Gateway-Nodes

Dateiname	Hinweise	Gefunden am
/Var/local/log/update-utcn.log	Enthält Protokolle, die sich auf diesem Knoten im Netzwerk des nicht vertrauenswürdigen Clients beziehen.	Alle Nodes

Verwandte Informationen

["Etwa bycast.log"](#)

["S3-REST-API VERWENDEN"](#)

Protokoll für Implementierung und Wartung

Sie können die Bereitstellungs- und Wartungsprotokolle verwenden, um Probleme zu beheben.

Dateiname	Hinweise	Gefunden am
/Var/local/log/install.log	Während der Softwareinstallation erstellt. Enthält eine Aufzeichnung der Installationsereignisse.	Alle Nodes
/Var/local/log/expansion-progress.log	Während Erweiterungsvorgängen erstellt. Enthält eine Aufzeichnung der Erweiterungsereignisse.	Storage-Nodes
/Var/local/log/pa-move.log	Wurde während der Ausführung des erstellt <code>pa-move.sh</code> Skript:	Primärer Admin-Node
/Var/local/log/pa-move-new_pa.log	Wurde während der Ausführung des erstellt <code>pa-move.sh</code> Skript:	Primärer Admin-Node
/Var/local/log/pa-move-old_pa.log	Wurde während der Ausführung des erstellt <code>pa-move.sh</code> Skript:	Primärer Admin-Node
/Var/local/log/gdu-server.log	Erstellt durch den GDU-Dienst. Enthält Ereignisse im Zusammenhang mit Provisioning- und Wartungsverfahren, die vom primären Admin-Node verwaltet werden.	Primärer Admin-Node
/Var/local/log/send_admin_hw.log	Während der Installation erstellt. Enthält Debugging-Informationen zur Kommunikation eines Knotens mit dem primären Admin-Knoten.	Alle Nodes
/Var/local/log/upgrade.log	Wird während eines Software-Upgrades erstellt. Enthält eine Aufzeichnung der Softwareaktualisierungs-Ereignisse.	Alle Nodes

Protokolle für Drittanbietersoftware

Sie können die Softwareprotokolle von Drittanbietern verwenden, um Probleme zu beheben.

Kategorie	Dateiname	Hinweise	Gefunden am
Archivierung	/Var/local/log/dsierror.log	Fehlerinformationen für TSM Client APIs.	Archiv-Nodes
MySQL	/Var/local/log/mysql.err /var/local/log/mysql-slow.log	Protokolldateien von MySQL erstellt. mysql.err Erfasst Datenbankfehler und Ereignisse wie Start-ups und Herunterfahren. mysql-slow.log (Das langsame Abfrageprotokoll) erfasst die SQL-Anweisungen, die mehr als 10 Sekunden in Anspruch genommen haben.	Admin-Nodes
Betriebssystem	/Var/local/log/messages	Dieses Verzeichnis enthält Protokolldateien für das Betriebssystem. Die in diesen Protokollen enthaltenen Fehler werden auch im Grid Manager angezeigt. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Wählen Sie dann Topologie > Site > Node > SSM > Events aus.	Alle Nodes
NTP	/Var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	/var/local/log/ntp.log Enthält die Protokolldatei für NTP-Fehlermeldungen. /var/lib/ntp/var/log/ntpstats/ Verzeichnis enthält NTP-Zeitstatistiken. loopstats Statistikdaten für Datensätze-Loop-Filter. peerstats Zeichnet Informationen zu Peer-Statistiken auf.	Alle Nodes

Etwa bycast.log

Die Datei `/var/local/log/bycast.log` ist die primäre Fehlerbehebungsdatei für die StorageGRID-Software. Es gibt ein `bycast.log` Datei für jeden Grid-Node. Die Datei enthält für diesen Grid-Node spezifische Meldungen.

Die Datei `/var/local/log/bycast-err.log` ist eine Untergruppe von `bycast.log`. Er enthält Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“.

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)".

Dateirotation für bycast.log

Wenn der `bycast.log` Die Datei erreicht 1 GB, die vorhandene Datei wird gespeichert und eine neue

Protokolldatei wird gestartet.

Die gespeicherte Datei wird umbenannt `bycast.log.1`, Und die neue Datei wird benannt `bycast.log`. Wenn das neue `bycast.log` Erreicht 1 GB, `bycast.log.1` Wird umbenannt und komprimiert zu werden `bycast.log.2.gz`, und `bycast.log` Wird umbenannt `bycast.log.1`.

Die Rotationsgrenze für `bycast.log` Sind 21 Dateien. Wenn die 22. Version des `bycast.log` Datei wird erstellt, die älteste Datei wird gelöscht.

Die Rotationsgrenze für `bycast-err.log` Sind sieben Dateien.



Wenn eine Protokolldatei komprimiert wurde, dürfen Sie sie nicht auf den gleichen Speicherort dekomprimieren, an dem sie geschrieben wurde. Die Dekomprimierung der Datei an demselben Speicherort kann die Drehskripte des Protokolls beeinträchtigen.

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)".

Verwandte Informationen

["Erfassen von Protokolldateien und Systemdaten"](#)

Nachrichten in `bycast.log`

Nachrichten in `bycast.log` Geschrieben werden durch die ADE (Asynchronous Distributed Environment). ADE ist die Laufzeitumgebung, die von den Services jedes Grid-Node verwendet wird.

Beispielmeldung für ADE:

```
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-Meldungen enthalten die folgenden Informationen:

Nachrichtensegment	Wert im Beispiel
Node-ID	12455685
PROZESS-ID WIRD ADDIEREN	0357819531
Modulname	SVMR
Nachrichtenkennung	EVHF
UTC-Systemzeit	2019-05-05T27T17:10:29.784677 (JJJJ-MM-DDTHH:MM:SS.UUUUUU)
Schweregrad	FEHLER

Nachrichtensegment	Wert im Beispiel
Interne Tracking-Nummer	0906
Nachricht	SVMR: Integritätsprüfung auf Volume 3 mit Grund 'AUSWEG' fehlgeschlagen

Nachrichten-Schweregrade in bycast.log

Die Meldungen in `bycast.log` Werden Schweregrade zugewiesen.

Beispiel:

- **HINWEIS** — ein Ereignis, das aufgezeichnet werden soll, ist aufgetreten. Die meisten Protokollmeldungen befinden sich auf dieser Ebene.
- **WARNUNG** — ein unerwarteter Zustand ist aufgetreten.
- **ERROR** — ein großer Fehler ist aufgetreten, der sich auf den Betrieb auswirkt.
- **KRITISCH** — Es ist ein anormaler Zustand aufgetreten, der den normalen Betrieb gestoppt hat. Sie sollten umgehend mit dem zugrunde liegenden Zustand beginnen. Kritische Meldungen werden auch im Grid Manager angezeigt. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus. Wählen Sie dann **Standort > Knoten > SSM > Events** aus.

Fehlercodes in bycast.log

Die meisten Fehlermeldungen in `bycast.log` Fehlercodes enthalten.

In der folgenden Tabelle sind häufig nicht-numerische Codes in aufgeführt `bycast.log`. Die genaue Bedeutung eines nicht-numerischen Codes hängt vom Kontext ab, in dem er gemeldet wird.

Fehlercode	Bedeutung
SUKZ	Kein Fehler
GERR	Unbekannt
STORNO	Storniert
ABRT	Abgebrochen
TOUT	Zeitüberschreitung
INVL	Ungültig
NFND	Nicht gefunden
ROVER	Version

Fehlercode	Bedeutung
CONF	Konfiguration
FEHLER	Fehlgeschlagen
ICPL	Unvollständig
FERTIG	Fertig
SUNV	Service nicht verfügbar

In der folgenden Tabelle sind die numerischen Fehlercodes in aufgeführt `bycast.log`.

Fehlernummer	Fehlercode	Bedeutung
001	EPERM	Vorgang nicht zulässig
002	ENOENT	Keine solche Datei oder Verzeichnis
003	ESRCH	Kein solcher Prozess
004	EINTR	Unterbrochener Systemanruf
005	EIO	I/O-Fehler
006	ENXIO	Dieses Gerät oder diese Adresse ist nicht vorhanden
007	E2BIG	Argumentliste zu lang
008	ENOEXEC	Fehler im Executive-Format
009	EBADF	Ungültige Dateinummer
010	ECHILD	Keine Kinderprozesse
011	EAGAIN	Versuchen Sie es erneut
012	ENOMEM	Nicht genügend Arbeitsspeicher
013	EACCES	Berechtigung verweigert
014	FAULT	Ungültige Adresse
015	ENOTBLK	Blockgerät erforderlich

Fehlernummer	Fehlercode	Bedeutung
016	EBUSY	Gerät oder Ressource beschäftigt
017	EEXIST	Datei vorhanden
018	EXDEV	Geräteübergreifende Verbindung
019	ENODEV	Kein solches Gerät
020	ENOTDIR	Kein Verzeichnis
021	EISDIR	Ist ein Verzeichnis
022	EINVAL	Ungültiges Argument
023	DATEI	Dateitabelle-Überlauf
024	EMFILE	Zu viele geöffnete Dateien
025	ENOTTY	Keine Schreibmaschine
026	ETXTBSY	Textdatei belegt
027	EFBIG	Datei zu groß
028	ENOSPC	Kein Platz mehr auf dem Gerät
029	ESPIPE	Illegale Suche
030	EROFS	Schreibgeschütztes Dateisystem
031	EMLINK	Zu viele Links
032	E-ROHR	Gebrochenes Rohr
033	EDOM	Math Argument aus Domäne der Funktion
034	ERANGE	Math Ergebnis nicht darstellbar
035	EDEADLK	Ressourcen-Deadlock würde eintreten
036	ENAMETOOLONG	Dateiname zu lang
037	ENOLCK	Keine Datensatzsperrern verfügbar

Fehlernummer	Fehlercode	Bedeutung
038	ENOSYS	Funktion nicht implementiert
039	ENOTEMPTY	Verzeichnis nicht leer
040	ELOOP	Es wurden zu viele symbolische Links gefunden
041		
042	ENOMSG	Keine Nachricht vom gewünschten Typ
043	EIDRM	Kennung entfernt
044	ECHRNG	Kanalnummer außerhalb des Bereichs
045	EL2NSYNC	Ebene 2 nicht synchronisiert
046	EL3HLT	Stufe 3 angehalten
047	EL3RST	Stufe 3 zurücksetzen
048	ELNRNG	Verbindungsnummer außerhalb des Bereichs
049	EUNATCH	Protokolltreiber nicht angeschlossen
050	ENOCSI	Keine CSI-Struktur verfügbar
051	EL2HLT	Stufe 2 angehalten
052	EBADE	Ungültiger Austausch
053	EBADR	Ungültiger Anforderungsdeskriptor
054	EXFULL	Exchange voll
055	ENOANO	Keine Anode
056	EBADRQC	Ungültiger Anforderungscode
057	EBADSLT	Ungültiger Steckplatz
058		
059	EBFONT	Schlechtes Schriftdateiformat

Fehlernummer	Fehlercode	Bedeutung
060	ENOSTR	Gerät kein Strom
061	ENODATA	Keine Daten verfügbar
062	ETIME	Timer abgelaufen
063	ENOSR	Aus Datenströmen: Ressourcen
064	ENONET	Die Maschine befindet sich nicht im Netzwerk
065	ENOPKG	Paket nicht installiert
066	EREMOTE	Das Objekt ist Remote
067	ENOLINK	Verbindung wurde getrennt
068	ADV	Fehler anzeigen
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	EOVERFLOW	Wert zu groß für definierten Datentyp
076	ENOTUNIQ	Name nicht eindeutig im Netzwerk
077	EBADFD	Dateideskriptor im schlechten Zustand
078	EREMCHG	Remote-Adresse geändert
079	ELIBACC	Kein Zugriff auf eine erforderliche freigegebene Bibliothek möglich
080	ELIBBAD	Zugriff auf eine beschädigte, gemeinsam genutzte Bibliothek

Fehlernummer	Fehlercode	Bedeutung
081	ELIBSCN	
082	ELIBMAX	Es wird versucht, zu viele gemeinsam genutzte Bibliotheken zu verbinden
083	ELIBEXEC	Eine gemeinsam genutzte Bibliothek kann nicht direkt exec
084	EILSEQ	Ungültige Byte-Sequenz
085	ERESTART	Unterbrochener Systemanruf sollte neu gestartet werden
086	ESTRPIPE	Leitungsfehler
087	EUSERS	Zu viele Benutzer
088	ENOTSOCK	Buchsenbetrieb an nicht-Socket
089	EDESTADDRREQ	Zieladresse erforderlich
090	EMSGSIZE	Nachricht zu lang
091	EPROTOTYPE	Protokoll falscher Typ für Socket
092	ENOPROTOOPT	Protokoll nicht verfügbar
093	EPROTONOSUPPORT	Protokoll nicht unterstützt
094	ESOCKTNOSUPPORT	Socket-Typ nicht unterstützt
095	EOPNOTSUPP	Der Vorgang wird auf dem Transportendpunkt nicht unterstützt
096	EPFNOSUPPORT	Protokollfamilie wird nicht unterstützt
097	EAFNOSUPPORT	Adressfamilie wird nicht durch Protokoll unterstützt
098	EADDRINUSE	Die Adresse wird bereits verwendet
099	EADDRNOTAVAIL	Angeforderte Adresse kann nicht zugewiesen werden
100	ENETDOWN	Netzwerk ausgefallen

Fehlernummer	Fehlercode	Bedeutung
101	ENETUNREACH	Netzwerk nicht erreichbar
102	ENETRESET	Die Verbindung wurde aufgrund von Reset unterbrochen
103	ECONNABORTED	Die Verbindung wurde durch die Software beendet
104	ECONNRESET	Verbindungsrücksetzung durch Peer
105	ENOBUFS	Kein Pufferspeicher verfügbar
106	EISCONN	Transportendpunkt ist bereits verbunden
107	ENOTCONN	Transportendpunkt ist nicht verbunden
108	ESHUTDOWN	Senden nach dem Herunterfahren des Transportendpunkts nicht möglich
109	ETOMANYREFS	Zu viele Referenzen: Spleißen nicht möglich
110	ETIMEDOUT	Zeitüberschreitung bei Verbindung
111	ECONNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHOSTUNREACH	Keine Route zum Host
114	EALREADY	Der Vorgang wird bereits ausgeführt
115	EINPROGRESS	Vorgang wird jetzt ausgeführt
116		
117	EUCLEAN	Struktur muss gereinigt werden
118	ENOTNAM	Keine XENIX-Datei mit dem Namen
119	ENAVAIL	Keine XENIX-Semaphore verfügbar
120	EISNAM	Ist eine Datei mit dem Namen
121	EREMOTEIO	Remote-I/O-Fehler

Fehlernummer	Fehlercode	Bedeutung
122	EDQUOT	Kontingent überschritten
123	ENOMEDIUM	Kein Medium gefunden
124	EMEDIUMTYPE	Falscher Medientyp
125	ECANCELED	Vorgang Abgebrochen
126	ENOKEY	Erforderlicher Schlüssel nicht verfügbar
127	EKEYEXPIRED	Schlüssel abgelaufen
128	EKEYREVOKED	Schlüssel wurde widerrufen
129	EKEYREJECTED	Schlüssel wurde vom Dienst abgelehnt
130	EOWNERDEAD	Für robuste Mutexe: Besitzer starb
131	ENOTRECOVERABLE	Bei robusten Mutation: Status nicht wiederherstellbar

Konfigurieren von Überwachungsmeldungen und Protokollzielen

Audit-Meldungen und -Protokolle zeichnen Systemaktivitäten und Sicherheitsereignisse auf und sind wichtige Tools für das Monitoring und die Fehlerbehebung. Sie können die Auditrelevel anpassen, um die Art und Anzahl der aufgezeichneten Audit-Meldungen zu erhöhen oder zu verringern. Optional können Sie alle HTTP-Anforderungs-Header definieren, die Sie in Client-Audit-Nachrichten lesen und schreiben möchten. Sie können auch einen externen Syslog-Server konfigurieren und das Ziel der Audit-Informationen ändern.

Weitere Informationen zu Überwachungsmeldungen finden Sie unter ["Prüfung von Audit-Protokollen"](#).

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.

Über diese Aufgabe

Alle StorageGRID Nodes generieren Audit-Meldungen und -Protokolle, um die Systemaktivität und -Ereignisse nachzuverfolgen. Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können die Überwachungsstufen anpassen, um die Art und Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu erhöhen oder zu verringern. Optional können Sie die Audit-Informationen so konfigurieren, dass sie vorübergehend auf den ursprünglichen Knoten für die manuelle Erfassung gespeichert werden.



Wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Applikationen verwenden oder alle Audit-Daten behalten möchten, konfigurieren Sie einen externen Syslog-Server und speichern Sie Audit-Informationen Remote. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Audit-Nachrichten auf die Performance minimiert, ohne dass die Vollständigkeit der Audit-Daten reduziert wird. Siehe "[Überlegungen für externen Syslog-Server](#)" Entsprechende Details.

Ändern Sie die Meldungsebenen im Auditprotokoll

Sie können für jede der folgenden Meldungskategorien im Prüfprotokoll eine andere Überwachungsstufe festlegen:

Audit-Kategorie	Beschreibung
System	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe " Systemaudits Meldungen ".
Storage	Diese Ebene ist standardmäßig auf Fehler festgelegt. Siehe " Audit-Meldungen zu Objekt-Storage ".
Vereinfachtes	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe " Management-Audit-Nachricht ".
Client-Lesevorgänge	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe " Client liest Audit-Meldungen ".
Client-Schreibvorgänge	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe " Audit-Meldungen des Clients schreiben ".
ILM-Betrieb	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe " Prüfmeldungen für den ILM-Betrieb ".



Diese Standardeinstellungen gelten, wenn Sie StorageGRID ursprünglich mit Version 10.3 oder höher installiert haben. Wenn Sie ein Upgrade von einer früheren Version von StorageGRID durchgeführt haben, ist die Standardeinstellung für alle Kategorien auf „Normal“ gesetzt.



Bei Upgrades sind Audit-Level-Konfigurationen nicht sofort wirksam.

Schritte

1. Wählen Sie **CONFIGURATION > Monitoring > Audit und Syslog-Server**.
2. Wählen Sie für jede Kategorie der Überwachungsmeldung eine Überwachungsstufe aus der Dropdown-Liste aus:

Audit-Level	Beschreibung
Aus	Es werden keine Überwachungsmeldungen aus der Kategorie protokolliert.

Audit-Level	Beschreibung
Fehler	Nur Fehlermeldungen sind protokollierte - Audit-Meldungen, für die der Ergebniscode nicht „erfolgreich“ (SUCS) war.
Normal	Standardtransaktionsmeldungen werden protokolliert – die in diesen Anweisungen für die Kategorie aufgeführten Nachrichten.
Debuggen	Veraltet. Dieser Level verhält sich mit dem normalen Prüfstand.

Die Meldungen, die für eine bestimmte Ebene enthalten sind, enthalten diejenigen, die auf den höheren Ebenen protokolliert werden würden. Die normale Ebene umfasst beispielsweise alle Fehlermeldungen.



Wenn Sie für Ihre S3-Anwendungen keine detaillierte Aufzeichnung der Client-Leseoperationen benötigen, ändern Sie optional die Einstellung **Client-Lesevorgänge** auf **Fehler**, um die Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu verringern.

3. Definieren Sie optional unter **Prüfprotokoll-Header** alle HTTP-Anforderungsheader, die Sie in die Lese- und Schreibnachrichten des Clients einbeziehen möchten. Verwenden Sie ein Sternchen (*) als Platzhalter, um Null oder mehr Zeichen zu entsprechen. Verwenden Sie die Escape-Sequenz (*), um mit einem wortwörtliche Sternchen überein.



Header für Prüfprotokolle sind nur auf S3 und Swift Anfragen anwendbar.

4. Wählen Sie **Einen anderen Header hinzufügen** aus, um ggf. zusätzliche Header zu erstellen.

Wenn HTTP-Header in einer Anfrage gefunden werden, sind sie in der Überwachungsmeldung unter dem Feld HTRH enthalten.



Header für Auditprotokoll-Anfragen werden nur protokolliert, wenn die Audit-Ebene für **Client** oder **Client-Schreibvorgänge** nicht **aus** ist.

5. Wählen Sie **Speichern**

Ein grünes Banner zeigt an, dass Ihre Konfiguration erfolgreich gespeichert wurde.

Verwenden Sie einen externen Syslog-Server

Sie können einen externen Syslog-Server konfigurieren, wenn Sie Audit-Informationen Remote speichern möchten.

- Wenn Sie Audit-Informationen auf einem externen Syslog-Server speichern möchten, gehen Sie zu ["Konfigurieren Sie einen externen Syslog-Server"](#).
- Wenn Sie keinen externen Syslog-Server verwenden, gehen Sie zu [Wählen Sie Ziele für Audit-Informationen aus](#).

Wählen Sie Ziele für Audit-Informationen aus

Sie können festlegen, wo Audit-Protokolle, Sicherheitsereignisprotokolle und Anwendungsprotokolle gesendet

werden.



Einige Ziele sind nur verfügbar, wenn Sie einen externen Syslog-Server verwenden. Siehe ["Konfigurieren Sie einen externen Syslog-Server"](#) So konfigurieren Sie einen externen Syslog-Server:



Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter ["StorageGRID-Softwareprotokolle"](#).

1. Wählen Sie auf der Seite Audit- und Syslog-Server aus den aufgeführten Optionen das Ziel für Audit-Informationen aus:

Option	Beschreibung
Standard (Admin-Nodes/lokale Nodes)	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten werden Sicherheitsereignisprotokolle und Anwendungsprotokolle auf den Knoten gespeichert, in denen sie erzeugt wurden (auch als "der lokale Knoten" bezeichnet).
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Node und externer Syslog-Server	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Nur lokale Nodes	Es werden keine Audit-Informationen an einen Admin-Node oder Remote-Syslog-Server gesendet. Audit-Informationen werden nur auf den generierten Nodes gespeichert. Hinweis: StorageGRID entfernt regelmäßig diese lokalen Protokolle in einer Drehung, 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 beträgt 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Auf jedem Node werden durchschnittlich etwa 20 GB an Protokoll Daten gespeichert.



In werden Audit-Informationen, die für jeden lokalen Node generiert werden, gespeichert `/var/local/log/localaudit.log`

2. Wählen Sie **Speichern**.

Es wird eine Warnmeldung angezeigt.

3. Wählen Sie **OK**, um zu bestätigen, dass Sie das Ziel für die Audit-Informationen ändern möchten.

Ein grünes Banner wird angezeigt, um Sie darüber zu informieren, dass Ihre Überwachungskonfiguration gespeichert wurde.

Neue Protokolle werden an die ausgewählten Ziele gesendet. Vorhandene Protokolle verbleiben an ihrem aktuellen Speicherort.

Verwandte Informationen

["Überlegungen für externen Syslog-Server"](#)

["StorageGRID verwalten"](#)

["Fehlerbehebung für den externen Syslog-Server"](#)

Verwenden Sie einen externen Syslog-Server

Überlegungen für externen Syslog-Server

Anhand der folgenden Richtlinien können Sie die Größe des benötigten externen Syslog-Servers einschätzen.

Was ist ein externer Syslog-Server?

Ein externer Syslog-Server ist ein Server außerhalb von StorageGRID, mit dem Sie Audit-Informationen zum System an einem Ort sammeln können. Mithilfe eines externen Syslog-Servers können Sie die Ziele Ihrer Audit-Informationen konfigurieren, sodass Sie den Netzwerkverkehr auf Ihren Admin-Knoten reduzieren und die Informationen effizienter verwalten können. Folgende Arten von Audit-Informationen können Sie an den externen Syslog-Server senden:

- Prüfprotokolle mit den während des normalen Systembetriebs erzeugten Audit-Meldungen
- Sicherheitsbezogene Ereignisse wie Anmeldungen und Eskalationen im Root-Bereich
- Anwendungsprotokolle, die angefordert werden können, wenn ein Support-Fall geöffnet werden muss, um die Behebung eines aufgetretenen Problems zu beheben

Wie schätzen Sie die Größe des externen Syslog-Servers ein

In der Regel wird das Grid so dimensioniert, dass es einen erforderlichen Durchsatz erzielt, der mit S3-Operationen pro Sekunde oder Byte pro Sekunde definiert wird. Möglicherweise müssen Sie z. B. angeben, dass Ihr Grid 1,000 S3-Operationen pro Sekunde oder 2,000 MB pro Sekunde der Objektingest und -Abruf verarbeiten muss. Sie sollten die Größe Ihres externen Syslog-Servers entsprechend den Datenanforderungen Ihres Grid festlegen.

Dieser Abschnitt enthält einige heuristische Formeln, mit denen Sie die Rate und die durchschnittliche Größe von Protokollmeldungen verschiedener Arten bewerten können, die Ihr externer Syslog-Server in der Lage sein muss, anhand der bekannten oder gewünschten Performance-Merkmale des Grid (S3-Operationen pro Sekunde) auszuführen.

In Schätzformeln S3-Operationen pro Sekunde verwenden

Wenn Ihr Grid für einen Durchsatz in Byte pro Sekunde ausgedrückt wurde, müssen Sie diese Größe in S3-Vorgänge pro Sekunde konvertieren, um die Abschätzung-Formeln zu verwenden. Um den Grid-Durchsatz zu konvertieren, müssen Sie zunächst die durchschnittliche Objektgröße festlegen, die Sie anhand der Informationen in vorhandenen Audit-Protokollen und -Metriken (falls vorhanden) durchführen können, oder indem Sie Ihre Kenntnisse über die Anwendungen nutzen, die StorageGRID verwenden. Beispiel: Wenn Ihr Grid einen Durchsatz von 2,000 MB/s erreicht hat und die durchschnittliche Objektgröße 2 MB beträgt, wurde das Grid so dimensioniert, dass es 1,000 S3-Operationen pro Sekunde (2,000 MB/2 MB) verarbeiten kann.



Die Formeln für die externe Syslog-Server-Größenbemessung in den folgenden Abschnitten liefern allgemeine Schätzungen (und nicht die Schlimmstfall-Schätzungen). Je nach Konfiguration und Workload wird möglicherweise eine höhere oder niedrigere Rate von Syslog-Meldungen oder ein höheres Volumen an Syslog-Daten angezeigt als die Formel „Predict“. Die Formeln sind nur als Richtlinien zu verwenden.

Schätzformeln für Prüfprotokolle

Wenn Sie über keine Informationen zu Ihrem S3-Workload verfügen außer der Anzahl der S3-Vorgänge pro Sekunde, die Ihr Grid unterstützen soll, können Sie die Menge der Audit-Protokolle schätzen, die Ihr externer Syslog-Server anhand der folgenden Formeln verarbeiten muss. Unter der Annahme, dass Sie die Audit-Level auf die Standardwerte (alle Kategorien sind auf Normal gesetzt, außer Speicher, der auf Fehler gesetzt ist):

```
Audit Log Rate = 2 x S3 Operations Rate  
Audit Log Average Size = 800 bytes
```

Wenn Ihr Grid beispielsweise für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, sollte der externe Syslog-Server entsprechend angepasst werden und 2,000 Syslog-Nachrichten pro Sekunde unterstützen. Er sollte Audit-Protokoll Daten von 1.6 MB pro Sekunde empfangen (und in der Regel speichern) können.

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Die wichtigsten zusätzlichen Variablen sind für Audit-Protokolle der Prozentsatz der am häufigsten verwendeten S3-Vorgänge (im Vergleich zu RUFT) und die mittlere Größe der folgenden S3-Felder in Byte (in der Tabelle werden 4-Zeichen-Abkürzungen verwendet):

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
S3BK	S3-Bucket	Der S3-Bucket-Name

Codieren	Feld	Beschreibung
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.

Verwenden wir P, um den Prozentsatz der an Put-Vorgängen abzubilden, wobei $0 \leq P \leq 1$ (für einen 100 % PUT-Workload, $P = 1$ und für einen 100 % GET-Workload, $P = 0$).

Verwenden wir K als Darstellung der durchschnittlichen Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann ist der Wert von K 90 (13+13+28+36).

Wenn Sie Werte für P und K festlegen können, können Sie die Menge der Audit-Protokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten muss. Dabei wird davon ausgegangen, dass Sie die Audit-Level auf die Standardwerte setzen (alle Kategorien sind auf Normal gesetzt, außer Speicher, Die auf Fehler gesetzt ist):

$$\text{Audit Log Rate} = ((2 \times P) + (1 - P)) \times \text{S3 Operations Rate}$$

$$\text{Audit Log Average Size} = (570 + K) \text{ bytes}$$

Wenn Ihr Grid beispielsweise 1,000 S3-Operationen pro Sekunde angepasst ist, beträgt der Workload 50 % Put-Vorgänge sowie die S3-Kontonamen und Bucket-Namen Und Objektnamen durchschnittlich 90 Byte, Ihr externer Syslog-Server sollte Größe haben, um 1,500 Syslog-Nachrichten pro Sekunde zu unterstützen. Er sollte Audit-Protokolldaten mit einer Rate von ca. 1 MB pro Sekunde empfangen (und in der Regel speichern) können.

Schätzformeln für nicht standardmäßige Audit-Level

Die für Prüfprotokolle bereitgestellten Formeln setzen voraus, dass die standardmäßigen Einstellungen für die Revisionsstufe verwendet werden (alle Kategorien sind auf Normal gesetzt, außer Speicher, der auf Fehler gesetzt ist). Detaillierte Formeln zur Schätzung der Rate und der durchschnittlichen Größe von Überwachungsmeldungen für nicht standardmäßige Überwachungseinstellungen sind nicht verfügbar. Die folgende Tabelle kann jedoch verwendet werden, um eine grobe Schätzung der Rate zu machen; Sie können die Formel für die durchschnittliche Größe von Audit-Protokollen verwenden, aber beachten Sie, dass sie wahrscheinlich zu einer Überschätzung führen wird, da die „zusätzlichen“ Audit-Meldungen im Durchschnitt kleiner sind als die standardmäßigen Audit-Meldungen.

Zustand	Formel
Replikation: Audit-Level alle auf Debug oder Normal eingestellt	Audit-Protokollrate = 8 x S3-Betriebsrate
Verfahren zur Einhaltung von Datenkonsistenz: Für Audit-Level ist Debug oder Normal festgelegt	Verwenden Sie die gleiche Formel wie für die Standardeinstellungen

Schätzformeln für Sicherheitsereignisse

Sicherheitsereignisse werden nicht mit S3-Vorgängen in Beziehung gesetzt und erzeugen in der Regel eine vernachlässigbare Menge an Protokollen und Daten. Aus diesen Gründen werden keine Schätzformeln bereitgestellt.

Schätzformeln für Anwendungsprotokolle

Wenn neben der Anzahl der S3-Vorgänge pro Sekunde, die Ihr Grid unterstützen soll, keine Informationen zu Ihrem S3-Workload vorhanden sind, können Sie das Volumen der Anwendungen schätzen. Protokolle, die Ihr externer Syslog-Server verarbeiten muss, werden gemäß den folgenden Formeln verwendet:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Wenn Ihr Grid also für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, sollte der externe Syslog-Server entsprechend dimensioniert sein, um 3,300 Applikations-Logs pro Sekunde zu unterstützen und Applikations-Protokolldaten von etwa 1.2 MB pro Sekunde zu empfangen (und zu speichern).

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Die wichtigsten zusätzlichen Variablen sind für Applikations-Protokolle die Datensicherungsstrategie (Replizierung vs Erasure Coding) – der Prozentsatz der S3-Operationen, die durchgeführt werden (im Vergleich zu Ruft/Other) und die durchschnittliche Größe der folgenden S3-Felder (in der Tabelle werden 4-Zeichen-Abkürzungen verwendet):

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.

Beispiel für eine Einschätzung der Dimensionierung

In diesem Abschnitt werden Beispielbeispiele erläutert, wie man die Schätzformeln für Raster mit den folgenden Methoden der Datensicherung verwendet:

- Replizierung
- Verfahren Zur Einhaltung Von Datenkonsistenz

Wenn Sie Replizierung für die Datensicherung verwenden

Stellen Sie P den Prozentsatz der an Put-Vorgängen dar, wobei $0 \leq P \leq 1$ (für einen 100 % PUT-Workload, $P = 1$ und für einen 100 % GET-Workload, $P = 0$).

K stellen die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel dar. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten 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-Vorgänge pro Sekunde dimensioniert ist, beträgt der Workload 50 % und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte, sollte der externe Syslog-Server entsprechend angepasst werden, um 1800 Applikations-Logs pro Sekunde zu unterstützen, und erhalten Applikationsdaten mit einer Rate von 0.5 MB pro Sekunde (und in der Regel auch dort).

Bei Verwendung von Erasure Coding zur Datensicherung

Stellen Sie P den Prozentsatz der an Put-Vorgängen dar, wobei $0 \leq P \leq 1$ (für einen 100 % PUT-Workload, $P = 1$ und für einen 100 % GET-Workload, $P = 0$).

K stellen die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel dar. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten 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 1,000 S3-Vorgänge pro Sekunde beträgt, beträgt der Workload 50 % der Put-Vorgänge sowie Ihre S3-Kontonamen und Bucket-Namen und Objektnamen durchschnittlich 90 Byte, Ihr externer Syslog-Server sollte Größe haben, um 2,250 Anwendungsprotokolle pro Sekunde zu unterstützen. Sie sollten in der Lage sein, Anwendungsdaten zu empfangen und zu empfangen (und in der Regel speichern) mit einer Rate von 0.6 MB pro Sekunde.

Weitere Informationen zum Konfigurieren von Meldungsebenen und einem externen Syslog-Server finden Sie unter:

- ["Konfigurieren Sie einen externen Syslog-Server"](#)
- ["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#)

Konfigurieren Sie einen externen Syslog-Server

Wenn Sie Audit-Protokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Speicherort außerhalb des Grid speichern möchten, konfigurieren Sie einen externen Syslog-Server mithilfe dieses Verfahrens.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.
- Sie verfügen über einen Syslog-Server mit der Kapazität, die Protokolldateien zu empfangen und zu speichern. Weitere Informationen finden Sie unter ["Überlegungen für externen Syslog-Server"](#).
- Sie haben die richtigen Server- und Client-Zertifizierungen, wenn Sie TLS oder RELP/TLS verwenden möchten.

Über diese Aufgabe

Wenn Sie Audit-Informationen an einen externen Syslog-Server senden möchten, müssen Sie zuerst den externen Server konfigurieren.

Durch das Senden von Audit-Informationen an einen externen Syslog-Server können Sie:

- Effizientere Erfassung und Verwaltung von Audit-Informationen wie Audit-Nachrichten, Applikationsprotokollen und Sicherheitsereignissen
- Reduzieren Sie den Netzwerkverkehr auf Ihren Admin-Knoten, da Audit-Informationen direkt von den verschiedenen Speicherknoten auf den externen Syslog-Server übertragen werden, ohne über einen Admin-Knoten gehen zu müssen



Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle mit einer Größe von mehr als 8192 Byte am Ende der Nachricht gekürzt, um den allgemeinen Einschränkungen in externen Syslog-Server-Implementierungen zu entsprechen.



Um die Optionen für eine vollständige Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers zu maximieren, werden auf jedem Knoten bis zu 20 GB an lokalen Protokollen von Audit-Datensätzen (localaudit.log) aufbewahrt.



Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihre Anforderungen zu erfüllen, können zusätzliche Konfigurationsoptionen mithilfe der privaten API angewendet werden `audit-destinations` Endpunkte: So ist es beispielsweise möglich, unterschiedliche Syslog-Server für unterschiedliche Node-Gruppen zu verwenden.

Konfigurieren Sie den externen Server

Greifen Sie auf den Assistenten zu

Rufen Sie zum Starten den Assistenten zum Konfigurieren des externen Syslog-Servers auf.

Schritte

1. Wählen Sie **CONFIGURATION > Monitoring > Audit und Syslog-Server**.

2. Wählen Sie auf der Seite Audit- und Syslog-Server die Option **externen Syslog-Server konfigurieren** aus. Wenn Sie zuvor einen externen Syslog-Server konfiguriert haben, wählen Sie **Externe Syslog-Server bearbeiten**.

Der Assistent zum Konfigurieren des externen Syslog-Servers wird angezeigt.

Syslog-Informationen eingeben

Sie müssen die Informationen angeben, die StorageGRID für den Zugriff auf den externen Syslog-Server benötigt.

Schritte

1. Geben Sie für den Schritt **Enter syslog info** des Assistenten einen gültigen vollständig qualifizierten Domännennamen oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server in das Feld **Host** ein.
2. Geben Sie den Zielport auf dem externen Syslog-Server ein (muss eine Ganzzahl zwischen 1 und 65535 sein). Der Standardport ist 514.
3. 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 verwenden zu können. Mithilfe von Zertifikaten lassen sich die Verbindungen zwischen dem Grid und dem externen Syslog-Server sichern. Weitere Informationen finden Sie unter ["Verwalten von Sicherheitszertifikaten"](#).

Für alle Protokolloptionen muss der externe Syslog-Server unterstützt und konfiguriert werden. Sie müssen eine Option wählen, die mit dem externen Syslog-Server kompatibel ist.



Reliable Event Logging Protocol (RELP) erweitert die Funktionalität des Syslog-Protokolls für eine zuverlässige Bereitstellung von Ereignismeldungen. Mithilfe von RELP können Sie den Verlust von Audit-Informationen verhindern, wenn Ihr externer Syslog-Server neu gestartet werden muss.

4. Wählen Sie **Weiter**.
5. Wenn Sie **TLS** oder **RELP/TLS** ausgewählt haben, laden Sie die folgenden Zertifikate hoch:
 - **Server CA-Zertifikate**: Ein oder mehrere vertrauenswürdige CA-Zertifikate zur Überprüfung des externen Syslog-Servers (in PEM-Codierung). Wenn nicht angegeben, wird das Standard-Grid-CA-Zertifikat verwendet. Die Datei, die Sie hier hochladen, kann ein CA-Bundle sein.
 - **Clientzertifikat**: Das Clientzertifikat zur Authentifizierung an den externen Syslog-Server (in PEM-Codierung).
 - **Privater Client-Schlüssel**: Privater Schlüssel für das Clientzertifikat (in PEM-Kodierung).



Wenn Sie ein Clientzertifikat verwenden, müssen Sie auch einen privaten Clientschlüssel verwenden. Wenn Sie einen verschlüsselten privaten Schlüssel angeben, müssen Sie auch die Passphrase angeben. Die Verwendung eines verschlüsselten privaten Schlüssels bietet keine wesentlichen Sicherheitsvorteile, da Schlüssel und Passphrase gespeichert werden müssen. Aus Gründen der Einfachheit wird die Verwendung eines unverschlüsselten privaten Schlüssels empfohlen.

- i. Wählen Sie **Durchsuchen** für das Zertifikat oder den Schlüssel, das Sie verwenden möchten.

- ii. Wählen Sie die Zertifikatdatei oder die Schlüsseldatei aus.
- iii. Wählen Sie **Öffnen**, um die Datei hochzuladen.

Neben dem Zertifikat- oder Schlüsseldateinamen wird eine grüne Prüfung angezeigt, die Sie darüber informiert, dass das Zertifikat erfolgreich hochgeladen wurde.

6. Wählen Sie **Weiter**.

Syslog-Inhalte managen

Sie können auswählen, welche Informationen an den externen Syslog-Server gesendet werden sollen.

Schritte

1. Wählen Sie für den Schritt **syslog-Inhalt verwalten** des Assistenten jeden Typ von Audit-Informationen aus, die Sie an den externen syslog-Server senden möchten.
 - **Audit-Protokolle senden:** Sendet StorageGRID-Ereignisse und Systemaktivitäten
 - **Sicherheitsereignisse senden:** Sendet Sicherheitsereignisse, z. B. wenn ein nicht autorisierter Benutzer versucht sich anzumelden oder sich ein Benutzer als root anmeldet
 - **Send Application logs:** Sendet Log-Dateien nützlich für die Fehlersuche einschließlich:
 - `bycast-err.log`
 - `bycast.log`
 - `jaeger.log`
 - `nms.log` (Nur Admin-Nodes)
 - `prometheus.log`
 - `raft.log`
 - `hagroups.log`
2. Verwenden Sie die Dropdown-Menüs, um den Schweregrad und die Einrichtung (Nachrichtentyp) für die Kategorie der zu sendenden Audit-Informationen auszuwählen.

Wenn Sie **Passthrough** für Schweregrad und Einrichtung auswählen, erhalten die an den Remote-Syslog-Server gesendeten Informationen denselben Schweregrad und dieselbe Einrichtung wie bei der lokalen Anmeldung am Node. Durch die Festlegung von Standort und Schweregrad können Sie die Protokolle individuell zusammenlegen und so die Analyse erleichtern.



Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter "[StorageGRID-Softwareprotokolle](#)".

- a. Wählen Sie für **Severity Passthrough** aus, wenn jede Nachricht, die an das externe Syslog gesendet wird, den gleichen Schweregrad wie im lokalen Syslog hat.

Wenn Sie für Überwachungsprotokolle **Passthrough** auswählen, lautet der Schweregrad 'Info'.

Wenn Sie für Sicherheitsereignisse **Passthrough** auswählen, werden die Schweregrade von der Linux-Distribution auf den Knoten generiert.

Wenn Sie bei Anwendungsprotokollen **Passthrough** auswählen, variieren die Schweregrade je nach Problem zwischen 'info' und 'Hinweis'. Wenn Sie beispielsweise einen NTP-Server hinzufügen und eine

HA-Gruppe konfigurieren, wird der Wert „Info“ angezeigt, während der SSM- oder RSM-Dienst absichtlich angehalten wird, wird der Wert „Hinweis“ angezeigt.

- b. Wenn Sie den Passthrough-Wert nicht verwenden möchten, wählen Sie einen Schweregrad zwischen 0 und 7 aus.

Der ausgewählte Wert wird auf alle Meldungen dieses Typs angewendet. Informationen zu den verschiedenen Schweregraden gehen verloren, wenn Sie den Schweregrad mit einem festen Wert überschreiben.

Schweregrad	Beschreibung
0	Notfall: System ist unbrauchbar
1	Warnung: Maßnahmen müssen sofort ergriffen werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber bedeutender Zustand
6	Information: Informationsmeldungen
7	Debug: Debug-Level-Meldungen

- c. Wählen Sie für **Einrichtung Passthrough** aus, wenn jede Nachricht, die an das externe Syslog gesendet wird, den gleichen Wert wie im lokalen Syslog hat.

Wenn Sie für Überwachungsprotokolle **Passthrough** auswählen, lautet die an den externen Syslog-Server gesendete Einrichtung „local7“.

Wenn Sie bei Sicherheitsereignissen **Passthrough** wählen, werden die Facility-Werte durch die linux-Distribution auf den Knoten generiert.

Wenn Sie bei Anwendungsprotokollen **Passthrough** auswählen, haben die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Facility-Werte:

Applikationsprotokoll	Durchlasswert
bycast.log	Benutzer oder Daemon
bycast-err.log	Benutzer, Daemon, local3 oder local4
jaeger.log	local2
nms.log	Lokalisierung 3

Applikationsprotokoll	Durchlasswert
prometheus.log	local4
raft.log	Lokalisierung 5
hagroups.log	Lokalisierung 6

- d. Wenn Sie den Passthrough-Wert nicht verwenden möchten, wählen Sie den Einrichtungswert zwischen 0 und 23 aus.

Der ausgewählte Wert wird auf alle Meldungen dieses Typs angewendet. Informationen über verschiedene Einrichtungen gehen verloren, wenn Sie eine Anlage mit einem festen Wert überschreiben möchten.

Anlage	Beschreibung
0	kern (Kernelmeldungen)
1	Benutzer (Meldungen auf Benutzerebene)
2	E-Mail
3	Daemon (Systemdemonen)
4	Auth (Sicherheits-/Autorisierungsmeldungen)
5	Syslog (intern erzeugte Nachrichten durch syslogd)
6	lpr (Liniendrucker-Subsystem)
7	nachrichten (Netzwerk-News-Subsystem)
8	UUCP
9	Cron (Clock Daemon)
10	Sicherheit (Sicherheits-/Autorisierungsmeldungen)
11	FTP
12	NTP
13	Logaudit (Protokollaudit)
14	Logalert (Protokollwarnung)

Anlage	Beschreibung
15	Uhr (Uhrzeitdaemon)
16	Local0
17	local1
18	local2
19	Lokalisierung 3
20	local4
21	Lokalisierung 5
22	Lokalisierung 6
23	Local7

3. Wählen Sie **Weiter**.

Versenden von Testmeldungen

Bevor Sie beginnen, einen externen Syslog-Server zu verwenden, sollten Sie anfordern, dass alle Knoten im Raster Testmeldungen an den externen Syslog-Server senden. Sie sollten diese Testmeldungen verwenden, um Sie bei der Validierung Ihrer gesamten Protokollierungs-Infrastruktur zu unterstützen, bevor Sie Daten an den externen Syslog-Server senden.



Verwenden Sie die Konfiguration des externen Syslog-Servers erst, wenn Sie bestätigen, dass der externe Syslog-Server von jedem Knoten in Ihrem Raster eine Testmeldung erhalten hat und dass die Nachricht erwartungsgemäß verarbeitet wurde.

Schritte

1. Wenn Sie keine Testnachrichten senden möchten, weil Sie sicher sind, dass Ihr externer Syslog-Server korrekt konfiguriert ist und Audit-Informationen von allen Knoten in Ihrem Raster empfangen kann, wählen Sie **Überspringen und Beenden**.

Ein grünes Banner zeigt an, dass Ihre Konfiguration erfolgreich gespeichert wurde.

2. Andernfalls wählen Sie **Testmeldungen senden** (empfohlen).

Die Testergebnisse werden kontinuierlich auf der Seite angezeigt, bis Sie den Test beenden. Während der Test läuft, werden Ihre Audit-Meldungen weiterhin an Ihre zuvor konfigurierten Ziele gesendet.

3. Wenn Sie Fehler erhalten, korrigieren Sie diese und wählen Sie **Testmeldungen senden** erneut.

Siehe "[Fehlerbehebung beim externen Syslog-Server](#)" Um Ihnen bei der Behebung von Fehlern zu helfen.

4. Warten Sie, bis ein grünes Banner angezeigt wird, dass alle Nodes die Tests bestanden haben.

5. Überprüfen Sie den Syslog-Server, ob Testmeldungen empfangen und verarbeitet werden wie erwartet.



Wenn Sie UDP verwenden, überprüfen Sie Ihre gesamte Log-Collection-Infrastruktur. Das UDP-Protokoll ermöglicht keine so strenge Fehlererkennung wie die anderen Protokolle.

6. Wählen Sie **Stop and Finish**.

Sie gelangen zurück zur Seite **Audit und Syslog Server**. Ein grünes Banner zeigt an, dass Ihre Syslog-Serverkonfiguration erfolgreich gespeichert wurde.



Die StorageGRID-Audit-Informationen werden erst an den externen Syslog-Server gesendet, wenn Sie ein Ziel auswählen, das den externen Syslog-Server enthält.

Wählen Sie Ziele für Audit-Informationen aus

Sie können festlegen, wo Sicherheitsereignisprotokolle, Anwendungsprotokolle und Prüfmeldungsprotokolle gesendet werden.



Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter "[StorageGRID-Softwareprotokolle](#)".

Schritte

1. Wählen Sie auf der Seite Audit- und Syslog-Server aus den aufgeführten Optionen das Ziel für Audit-Informationen aus:

Option	Beschreibung
Standard (Admin-Nodes/lokale Nodes)	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten werden Sicherheitsereignisprotokolle und Anwendungsprotokolle auf den Knoten gespeichert, in denen sie erzeugt wurden (auch als "der lokale Knoten" bezeichnet).
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Node und externer Syslog-Server	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.

Option	Beschreibung
Nur lokale Nodes	<p>Es werden keine Audit-Informationen an einen Admin-Node oder Remote-Syslog-Server gesendet. Audit-Informationen werden nur auf den generierten Nodes gespeichert.</p> <p>Hinweis: StorageGRID entfernt regelmäßig diese lokalen Protokolle in einer Drehung, 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 beträgt 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Auf jedem Node werden durchschnittlich etwa 20 GB an Protokoll Daten gespeichert.</p>



In werden Audit-Informationen, die für jeden lokalen Node generiert werden, gespeichert
`/var/local/log/localaudit.log`

2. Wählen Sie **Speichern**. Wählen Sie dann **OK**, um die Änderung am Protokollziel zu akzeptieren.
3. Wenn Sie entweder **Externer Syslog-Server** oder **Admin-Knoten und externer Syslog-Server** als Ziel für Audit-Informationen ausgewählt haben, wird eine zusätzliche Warnung angezeigt. Überprüfen Sie den Warntext.



Sie müssen bestätigen, dass der externe Syslog-Server Test-StorageGRID-Meldungen empfangen kann.

4. Wählen Sie **OK**, um zu bestätigen, dass Sie das Ziel für die Audit-Informationen ändern möchten.

Ein grünes Banner zeigt an, dass Ihre Audit-Konfiguration erfolgreich gespeichert wurde.

Neue Protokolle werden an die ausgewählten Ziele gesendet. Vorhandene Protokolle verbleiben an ihrem aktuellen Speicherort.

Verwandte Informationen

["Übersicht über Überwachungsnachrichten"](#)

["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#)

["Systemaudits Meldungen"](#)

["Audit-Meldungen zu Objekt-Storage"](#)

["Management-Audit-Nachricht"](#)

["Client liest Audit-Meldungen"](#)

["StorageGRID verwalten"](#)

Verwenden Sie SNMP-Überwachung

Verwenden Sie SNMP-Überwachung: Übersicht

Wenn Sie StorageGRID mit dem Simple Network Management Protocol (SNMP) überwachen möchten, müssen Sie den SNMP-Agent konfigurieren, der in StorageGRID enthalten ist.

- ["Konfigurieren Sie den SNMP-Agent"](#)
- ["Aktualisieren Sie den SNMP-Agent"](#)

Sorgen

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder -Daemon ausgeführt, der eine MIB bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Alarmer und Alarme. Die MIB enthält auch Informationen zur Systembeschreibung wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID-Knoten unterstützt auch eine Untergruppe von MIB-II-Objekten.



Siehe ["Zugriff auf MIB-Dateien"](#) Wenn Sie die MIB-Dateien auf Ihrem Grid-Knoten herunterladen möchten.

Zunächst ist SNMP auf allen Knoten deaktiviert. Wenn Sie den SNMP-Agent konfigurieren, erhalten alle StorageGRID-Knoten die gleiche Konfiguration.

Der StorageGRID SNMP Agent unterstützt alle drei Versionen des SNMP-Protokolls. Es bietet schreibgeschützten MIB-Zugriff für Abfragen, und es kann zwei Arten von ereignisgesteuerten Benachrichtigungen an ein Verwaltungssystem senden:

- **Traps** sind Benachrichtigungen, die vom SNMP-Agenten gesendet werden und keine Bestätigung durch das Managementsystem erfordern. Traps dienen dazu, das Managementsystem über etwas innerhalb von StorageGRID zu informieren, wie z. B. eine Warnung, die ausgelöst wird.

Traps werden in allen drei Versionen von SNMP unterstützt.

- **Informiert** sind ähnlich wie Traps, aber sie erfordern eine Bestätigung durch das Management-System. Wenn der SNMP-Agent innerhalb einer bestimmten Zeit keine Bestätigung erhält, wird die Benachrichtigung erneut gesendet, bis eine Bestätigung empfangen wurde oder der maximale Wiederholungswert erreicht wurde.

Die Informationsunterstützung wird in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden in folgenden Fällen versendet:

- Eine Standardwarnung oder eine benutzerdefinierte Meldung wird für jeden Schweregrad ausgelöst. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, müssen Sie eine Stille für die Warnung konfigurieren. Warnmeldungen werden vom gesendet ["Administratorknoten des bevorzugten Absenders"](#).

Jeder Alarm wird einem von drei Trap-Typen basierend auf dem Schweregrad des Alarms zugeordnet: ActiveMinorAlert, activeMajorAlert und activeCriticalAlert. Eine Liste der Warnmeldungen, mit denen diese Traps ausgelöst werden können, finden Sie im ["Alerts Referenz"](#).

- Bestimmte Alarmer (Altsystem) werden mit einem bestimmten Schweregrad oder höher ausgelöst.



SNMP-Benachrichtigungen werden nicht für jeden Alarm oder für jeden Schweregrad des Alarms gesendet.

Unterstützung von SNMP-Versionen

Die Tabelle bietet eine allgemeine Zusammenfassung der unterstützten SNMP-Versionen.

	SNMPv1	SNMPv2c	SNMPv3
Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-Zeichenfolge	Community-Zeichenfolge	Benutzer des benutzerbasierten Sicherheitsmodells (USM)
Benachrichtigungen	Nur Traps	Traps und informiert	Traps und informiert
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 Nodes im Grid erhalten dieselbe 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.

Verwandte Informationen

- ["Alerts Referenz"](#)
- ["Alarmreferenz \(Altsystem\)"](#)
- ["Benachrichtigung über Stille"](#)

Konfigurieren Sie den SNMP-Agent

Sie können den StorageGRID SNMP-Agent konfigurieren, wenn Sie ein Drittanbieter-SNMP-Verwaltungssystem für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwenden möchten.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Der StorageGRID SNMP Agent unterstützt alle drei Versionen des SNMP-Protokolls. Sie können den Agent für eine oder mehrere Versionen konfigurieren.

Schritte

1. Wählen Sie **KONFIGURATION > Überwachung > SNMP-Agent**.

Die Seite SNMP-Agent wird angezeigt.

SNMP agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, and SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration. The following MIB files define the objects and notifications for StorageGRID:

-  **NETAPP-STORAGEGRID-MIB.txt**: Defines the alert table and notifications (traps) accessible on all Admin Nodes.
-  **ES-NETAPP-06-MIB.mib**: Defines objects and notifications for E-Series-based appliances.
-  **MIB_1_10.zip**: Defines objects and notifications for appliances with a BMC interface.

Enable SNMP 

Save

2. Um den SNMP-Agent auf allen Grid-Knoten zu aktivieren, aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.

Die Felder zum Konfigurieren eines SNMP-Agenten werden angezeigt.

Enable SNMP ?

System Contact ?

System Location ?

Enable SNMP Agent Notifications ?

Enable Authentication Traps ?

Community Strings

Default Trap Community ?

Read-Only Community ?

String 1 +

Other Configurations

Agent Addresses (0) USM Users (0) Trap Destinations (0)

[+ Create](#) [Edit](#) [Remove](#)

Internet Protocol	Transport Protocol	StorageGRID Network	Port
No results found			

3. Geben Sie im Feld **Systemkontakt** den Wert ein, den StorageGRID in SNMP-Nachrichten für sysContact bereitstellen soll.

Der Systemkontakt ist in der Regel eine E-Mail-Adresse. Der von Ihnen auslieferen Wert gilt für alle Nodes im StorageGRID System. **Systemkontakt** kann maximal 255 Zeichen lang sein.

4. Geben Sie im Feld **Systemstandort** den Wert ein, den StorageGRID in SNMP-Nachrichten für sysLocation bereitstellen soll.

Der Systemstandort kann alle Informationen sein, die für die Identifizierung des Standortes Ihres StorageGRID-Systems nützlich sind. Sie können beispielsweise die Straßenadresse einer Einrichtung

verwenden. Der von Ihnen auslieferte Wert gilt für alle Nodes im StorageGRID System. **Systemposition** kann maximal 255 Zeichen enthalten.

5. Lassen Sie das Kontrollkästchen **SNMP-Agentenbenachrichtigungen aktivieren** aktiviert, wenn der StorageGRID SNMP-Agent Trap- und Benachrichtigungen senden soll.

Wenn dieses Kontrollkästchen deaktiviert ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.

6. Aktivieren Sie das Kontrollkästchen **Authentifizierungs-Traps aktivieren**, wenn der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap senden soll, wenn er eine nicht ordnungsgemäß authentifizierte Protokollnachricht erhält.
7. Wenn Sie SNMPv1 oder SNMPv2c verwenden, füllen Sie den Abschnitt „Gemeinschaftsfolgen“ aus.

Die Felder in diesem Abschnitt werden für die Community-basierte Authentifizierung in SNMPv1 oder SNMPv2c verwendet. Diese Felder gelten nicht für SNMPv3.

- a. Geben Sie im Feld **Default Trap Community** optional die Standard-Community-Zeichenfolge ein, die Sie für Trap-Ziele verwenden möchten.

Bei Bedarf können Sie eine andere („Custom“-)Community-Zeichenfolge angeben [Definieren Sie ein bestimmtes Trap-Ziel](#).

Default Trap Community darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.

- b. Geben Sie für **Read-Only Community** eine oder mehrere Community-Strings ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agent-Adressen zu ermöglichen. Wählen Sie das Pluszeichen aus **+** Um mehrere Zeichenfolgen hinzuzufügen.

Wenn das Verwaltungssystem die StorageGRID-MIB abfragt, sendet es eine Community-Zeichenfolge. Wenn die Community-Zeichenfolge einem der hier angegebenen Werte entspricht, sendet der SNMP-Agent eine Antwort an das Managementsystem.

Jede Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten. Es sind bis zu fünf Zeichenfolgen zulässig.



Um die Sicherheit Ihres StorageGRID-Systems zu gewährleisten, verwenden Sie „public“ nicht als Community-String. Wenn Sie keine Community-Zeichenfolge eingeben, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID-Systems als Community-String.

8. Wählen Sie optional im Abschnitt andere Konfigurationen die Registerkarte Agentenadressen aus.

Verwenden Sie diese Registerkarte, um eine oder mehrere „Listening-Adressen“ anzugeben. Dies sind die StorageGRID-Adressen, auf denen der SNMP-Agent Anfragen erhalten kann. Jede Agentenadresse umfasst ein Internetprotokoll, ein Transportprotokoll, ein StorageGRID-Netzwerk und optional einen Port.

Wenn Sie keine Agentenadresse konfigurieren, ist die standardmäßige Abhöradresse in allen StorageGRID-Netzwerken UDP-Port 161.

- a. Wählen Sie **Erstellen**.

Das Dialogfeld Agentenadresse erstellen wird angezeigt.

Create Agent Address

Internet Protocol IPv4 IPv6

Transport Protocol UDP TCP

StorageGRID Network

Port

b. Wählen Sie für **Internet Protocol** aus, ob diese Adresse IPv4 oder IPv6 verwendet.

Standardmäßig verwendet SNMP IPv4.

c. Wählen Sie für **Transport Protocol** aus, ob diese Adresse UDP oder TCP verwenden soll.

Standardmäßig verwendet SNMP UDP.

d. Wählen Sie im Feld **StorageGRID-Netzwerk** das StorageGRID-Netzwerk aus, auf dem die Abfrage empfangen wird.

- Grid-, Admin- und Client-Netzwerke: StorageGRID sollte SNMP-Abfragen in allen drei Netzwerken abhören.
- Grid-Netzwerk
- Admin-Netzwerk
- Client-Netzwerk



Um sicherzustellen, dass die Clientkommunikation mit StorageGRID sicher bleibt, sollten Sie keine Agentenadresse für das Clientnetzwerk erstellen.

e. Geben Sie im Feld **Port** optional die Portnummer ein, die der SNMP-Agent anhören soll.

Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch alle nicht verwendeten Portnummern eingeben.



Wenn Sie den SNMP-Agent speichern, öffnet StorageGRID automatisch die Agent-Adressen-Ports in der internen Firewall. Sie müssen sicherstellen, dass alle externen Firewalls den Zugriff auf diese Ports zulassen.

f. Wählen Sie **Erstellen**.

Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

Other Configurations

Agent Addresses (2) USM Users (2) Trap Destinations (2)

+ Create **Edit** **Remove**

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

9. Wenn Sie SNMPv3 verwenden, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

Über diese Registerkarte können Sie USM-Benutzer definieren, die berechtigt sind, die MIB abzufragen oder Traps zu empfangen und zu informieren.



Dieser Schritt gilt nicht, wenn Sie nur SNMPv1 oder SNMPv2c verwenden.

a. Wählen Sie **Erstellen**.

Das Dialogfeld USM-Benutzer erstellen wird angezeigt.

Create USM User

Username 

Read-Only MIB Access 

Authoritative Engine ID 

Security Level  authPriv authNoPriv

Authentication

Protocol  SHA

Password

Confirm Password

Privacy

Protocol  AES

Password

Confirm Password

b. Geben Sie einen eindeutigen **Benutzername** für diesen USM-Benutzer ein.

Benutzernamen dürfen maximal 32 Zeichen enthalten und dürfen keine Leerzeichen enthalten. Der Benutzername kann nach dem Erstellen des Benutzers nicht mehr geändert werden.

c. Aktivieren Sie das Kontrollkästchen **schreibgeschützter MIB-Zugriff**, wenn dieser Benutzer schreibgeschützten Zugriff auf die MIB haben soll.

Wenn Sie **schreibgeschütztes MIB Access** auswählen, ist das Feld **autoritative Engine ID**

deaktiviert.



USM-Benutzer mit schreibgeschütztem MIB-Zugriff können keine Engine-IDs haben.

- d. Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, geben Sie die **autoritative Engine-ID** für diesen Benutzer ein.



SNMPv3-Inform-Ziele müssen Benutzer mit Engine-IDs haben. Das SNMPv3-Trap-Ziel kann keine Benutzer mit Engine-IDs haben.

Die autoritative Engine-ID kann zwischen 5 und 32 Byte hexadezimal sein.

- e. Wählen Sie eine Sicherheitsstufe für den USM-Benutzer aus.

- **AuthPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort sowie ein Datenschutzprotokoll und ein Passwort angeben.
- **AuthNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort angeben.

- f. Geben Sie das Passwort ein, das dieser Benutzer zur Authentifizierung verwenden soll, und bestätigen Sie es.



Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).

- g. Wenn Sie **authPriv** ausgewählt haben, geben Sie das Passwort ein und bestätigen Sie es.



Das einzige unterstützte Datenschutzprotokoll ist AES.

- h. Wählen Sie **Erstellen**.

Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

Other Configurations

Agent Addresses (2)

USM Users (3)

Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	✓	authNoPriv	
<input type="radio"/>	user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3		authPriv	59D39E801256

10. Wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Trap-Ziele aus.

Auf der Registerkarte Trap-Ziele können Sie ein oder mehrere Ziele für StorageGRID-Trap definieren oder Benachrichtigungen informieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen,

sendet StorageGRID Benachrichtigungen an jedes definierte Ziel. Benachrichtigungen werden gesendet, wenn Warnungen ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

a. Wählen Sie **Erstellen**.

Das Dialogfeld Trap-Ziel erstellen wird angezeigt.

Create Trap Destination

Version SNMPv1 SNMPv2C SNMPv3

Type Trap

Host

Port

Protocol UDP TCP

Community String Use the default trap community: No default found (Specify the default on the SNMP Agent page.)

Use a custom community string

Custom Community String

a. Wählen Sie im Feld **Version** die SNMP-Version für diese Benachrichtigung aus.

b. Füllen Sie das Formular aus, basierend auf der ausgewählten Version

Version	Geben Sie diese Informationen an
<p>SNMPv1</p> <p>(Bei SNMPv1 kann der SNMP-Agent nur Traps senden. Informationen werden nicht unterstützt.)</p>	<ul style="list-style-type: none"> i. Geben Sie im Feld Host eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. ii. Verwenden Sie für Port den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iii. Verwenden Sie für Protokoll den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) iv. Verwenden Sie die Standard-Trap-Community, wenn eine auf der Seite SNMP Agent angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. <p>Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.</p>
<p>SNMPv2c</p>	<ul style="list-style-type: none"> i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird. ii. Geben Sie im Feld Host eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. iii. Verwenden Sie für Port den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iv. Verwenden Sie für Protokoll den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) v. Verwenden Sie die Standard-Trap-Community, wenn eine auf der Seite SNMP Agent angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. <p>Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.</p>

Version	Geben Sie diese Informationen an
SNMPv3	<ul style="list-style-type: none"> i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird. ii. Geben Sie im Feld Host eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. iii. Verwenden Sie für Port den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iv. Verwenden Sie für Protokoll den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) v. Wählen Sie den USM-Benutzer aus, der zur Authentifizierung verwendet werden soll. <ul style="list-style-type: none"> ◦ Wenn Sie Trap ausgewählt haben, werden nur USM-Benutzer ohne maßgebliche Engine-IDs angezeigt. ◦ Wenn Sie Inform ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt.

c. Wählen Sie **Erstellen**.

Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

11. Wenn Sie die SNMP-Agent-Konfiguration abgeschlossen haben, wählen Sie **Speichern**.

Die neue SNMP-Agent-Konfiguration wird aktiv.

Verwandte Informationen

["Benachrichtigung über Stille"](#)

Aktualisieren Sie den SNMP-Agent

Sie können SNMP-Benachrichtigungen deaktivieren, Community-Strings aktualisieren oder Agent-Adressen, USM-Benutzer und Trap-Ziele hinzufügen oder entfernen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein ["Unterstützter Webbrowser"](#).
- Sie müssen über die Root-Zugriffsberechtigung verfügen.

Über diese Aufgabe

Jedes Mal, wenn Sie den aktualisieren ["SNMP-Agent-Konfiguration"](#) Beachten Sie, dass Sie unten auf der SNMP Agent-Seite **Speichern** auswählen müssen, um alle Änderungen zu übernehmen, die Sie auf jeder Registerkarte vorgenommen haben.

Schritte

1. Wählen Sie **KONFIGURATION > Überwachung > SNMP-Agent**.

Die Seite SNMP-Agent wird angezeigt.

2. Wenn Sie den SNMP-Agent auf allen Grid-Knoten deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **SNMP aktivieren**, und wählen Sie **Speichern**.

Der SNMP-Agent ist für alle Grid-Knoten deaktiviert. Wenn Sie den Agent später wieder aktivieren, werden alle vorherigen SNMP-Konfigurationseinstellungen beibehalten.

3. Aktualisieren Sie optional die Werte, die Sie für **Systemkontakt** und **Systemstandort** eingegeben haben.
4. Deaktivieren Sie optional das Kontrollkästchen **SNMP-Agentenbenachrichtigungen aktivieren**, wenn Sie nicht mehr möchten, dass der StorageGRID SNMP-Agent Trap- und Benachrichtigungen sendet.

Wenn dieses Kontrollkästchen deaktiviert ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.

5. Deaktivieren Sie optional das Kontrollkästchen **Enable Authentication Traps**, wenn Sie nicht mehr möchten, dass der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap sendet, wenn er eine falsch authentifizierte Protokollnachricht empfängt.
6. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren Sie optional den Abschnitt Community Strings.

Die Felder in diesem Abschnitt werden für die Community-basierte Authentifizierung in SNMPv1 oder SNMPv2c verwendet. Diese Felder gelten nicht für SNMPv3.



Wenn Sie den Standard-Community-String entfernen möchten, müssen Sie zunächst sicherstellen, dass alle Trap-Ziele eine benutzerdefinierte Community-Zeichenfolge verwenden.

7. Wenn Sie Agentenadressen aktualisieren möchten, wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Agentenadressen aus.

Other Configurations

Agent Addresses (2) USM Users (2) Trap Destinations (2)

+ Create **Edit** **✕ Remove**

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

Verwenden Sie diese Registerkarte, um eine oder mehrere „Listening-Adressen“ anzugeben. Dies sind die StorageGRID-Adressen, auf denen der SNMP-Agent Anfragen erhalten kann. Jede Agentenadresse umfasst ein Internetprotokoll, ein Transportprotokoll, ein StorageGRID-Netzwerk und einen Port.

- a. Um eine Agentenadresse hinzuzufügen, wählen Sie **Create**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.
- b. Um eine Agentenadresse zu bearbeiten, aktivieren Sie das Optionsfeld für die Adresse und wählen **Bearbeiten**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des

SNMP-Agenten.

- c. Um eine Agentenadresse zu entfernen, aktivieren Sie das Optionsfeld für die Adresse und wählen **Entfernen** aus. Wählen Sie dann **OK**, um zu bestätigen, dass Sie diese Adresse entfernen möchten.
 - d. Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der SNMP Agent-Seite aus.
8. Wenn Sie USM-Benutzer aktualisieren möchten, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

Other Configurations

Agent Addresses (2) USM Users (3) Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	✓	authNoPriv	
<input type="radio"/>	user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3		authPriv	59D39E801256

Über diese Registerkarte können Sie USM-Benutzer definieren, die berechtigt sind, die MIB abzufragen oder Traps zu empfangen und zu informieren.

- a. Um einen USM-Benutzer hinzuzufügen, wählen Sie **Create**. Lesen Sie dann den Schritt für USM-Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.
- b. Um einen USM-Benutzer zu bearbeiten, aktivieren Sie das Optionsfeld für den Benutzer und wählen Sie **Bearbeiten**. Lesen Sie dann den Schritt für USM-Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.

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 autorisierende Engine-ID eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen, wie in Schritt beschrieben [SNMP-Trap-Ziel](#). Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

- a. Um einen USM-Benutzer zu entfernen, aktivieren Sie das Optionsfeld für den Benutzer und wählen Sie **Entfernen** aus. Wählen Sie dann **OK**, um zu bestätigen, dass Sie diesen Benutzer entfernen möchten.



Wenn der Benutzer, den Sie entfernt haben, derzeit für ein Trap-Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen, wie in Schritt beschrieben [SNMP-Trap-Ziel](#). Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

- b. Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der SNMP Agent-Seite aus.
9. Wenn Sie Trap-Ziele aktualisieren möchten, wählen Sie im Abschnitt andere Konfigurationen die

Registerkarte Trap-Ziele aus.

Auf der Registerkarte Trap-Ziele können Sie ein oder mehrere Ziele für StorageGRID-Trap definieren oder Benachrichtigungen informieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel. Benachrichtigungen werden gesendet, wenn Warnungen und Alarme ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

- a. Um ein Trap-Ziel hinzuzufügen, wählen Sie **Create**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
 - b. Um ein Trap-Ziel zu bearbeiten, aktivieren Sie das Optionsfeld für den Benutzer und wählen **Bearbeiten**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
 - c. Um ein Trap-Ziel zu entfernen, aktivieren Sie das Optionsfeld für das Ziel und wählen Sie **Entfernen** aus. Wählen Sie dann **OK**, um zu bestätigen, dass Sie dieses Ziel entfernen möchten.
 - d. Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der SNMP Agent-Seite aus.
10. Wenn Sie die SNMP-Agent-Konfiguration aktualisiert haben, wählen Sie **Speichern**.

Zugriff auf MIB-Dateien

MIB-Dateien enthalten Definitionen und Informationen über die Eigenschaften der verwalteten Ressourcen und Dienste für die Knoten in der Tabelle. Sie können auf MIB-Dateien zugreifen, die die Objekte und Benachrichtigungen für StorageGRID definieren. Diese Dateien können für die Überwachung Ihres Grids nützlich sein.

Siehe "[Verwenden Sie SNMP-Überwachung](#)" Weitere Informationen zu SNMP- und MIB-Dateien.

Zugriff auf MIB-Dateien

Schritte

1. Wählen Sie **KONFIGURATION > Überwachung > SNMP-Agent**.
2. Wählen Sie auf der Seite des SNMP-Agenten die Datei aus, die Sie herunterladen möchten:
 - **NETAPP-STORAGEGRID-MIB.txt**: Definiert die Alarmtabelle und Benachrichtigungen (Traps), auf die auf allen Admin-Knoten zugegriffen werden kann.
 - **Es-NETAPP-06-MIB.mib**: Definiert Objekte und Benachrichtigungen für E-Series-basierte Appliances.
 - **MIB_1_10.zip**: Definiert Objekte und Benachrichtigungen für Geräte mit BMC-Schnittstelle.
3. Optional können Sie auf MIB-Dateien am folgenden Speicherort auf einem beliebigen StorageGRID-Knoten zugreifen:

```
/usr/share/snmp/mibs
```

4. Um den zu extrahieren `storagegrid` OIDs aus der MIB-Datei:

- a. Erhalten Sie die OID des Stamms 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. Grüße dann für die StorageGRID-OID in der gesamten Struktur (mit Einfügen, um Linien zu verbinden):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



Der `snmptranslate` Befehl hat viele Optionen, die nützlich sind, um die MIB zu erkunden. Dieser Befehl ist auf jedem StorageGRID-Node verfügbar.

MIB-Dateiinhalte

Alle Objekte befinden sich unter der StorageGRID-OID.

Objektname	Objekt-ID (OID)	Beschreibung
		Das MIB-Modul für NetApp StorageGRID Entities.

MIB-Objekte

Objektname	Objekt-ID (OID)	Beschreibung
ActiveAlertCount		Die Anzahl der aktiven Warnungen in der activeAlertTable.
ActiveAlertTable		Eine Tabelle mit aktiven Warnmeldungen in StorageGRID.
ActiveAlertId		Die ID der Warnmeldung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
ActiveAlertName		Der Name der Warnmeldung.
ActiveAlertInstance		Der Name der Entität, die die Warnmeldung generiert hat, normalerweise der Knotenname.
ActiveAlertSchweregrad		Der Schweregrad der Meldung.
ActiveAlertStartTime		Datum und Uhrzeit der Auslösung der Warnmeldung.

Benachrichtigungstypen (Traps)

Alle Benachrichtigungen enthalten die folgenden Variablen als verbindendes:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSchweregrad
- ActiveAlertStartTime

Benachrichtigungstyp	Objekt-ID (OID)	Beschreibung
ActiveMinorAlert		Ein Alarm mit geringem Schweregrad
ActiveMajorAlert		Ein Alarm mit dem Hauptschweregrad
ActiveCriticalAlert		Eine Meldung mit dem Schweregrad „kritisch“

Erfassung zusätzlicher StorageGRID-Daten

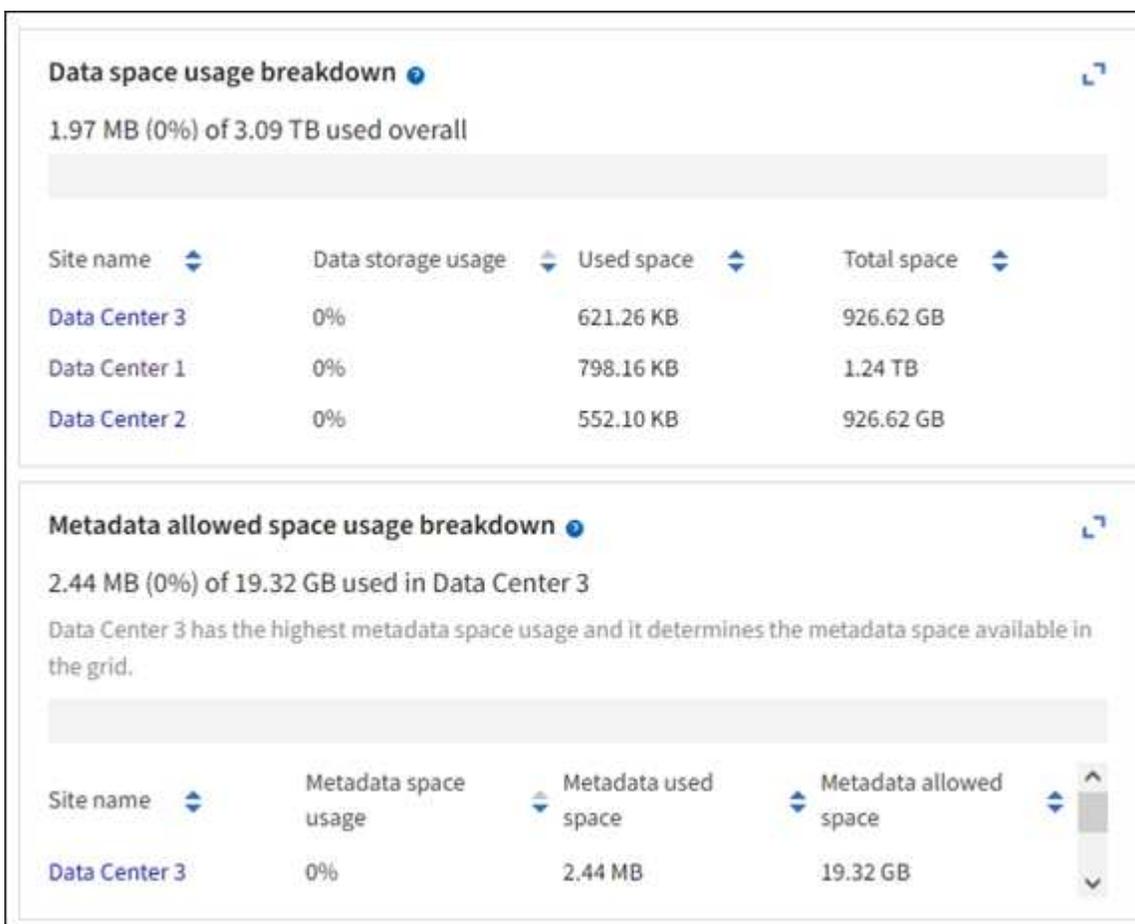
Verwenden Sie Diagramme und Diagramme

Mithilfe von Diagrammen und Berichten lässt sich der Zustand des StorageGRID Systems überwachen und Probleme beheben.

Diagrammtypen

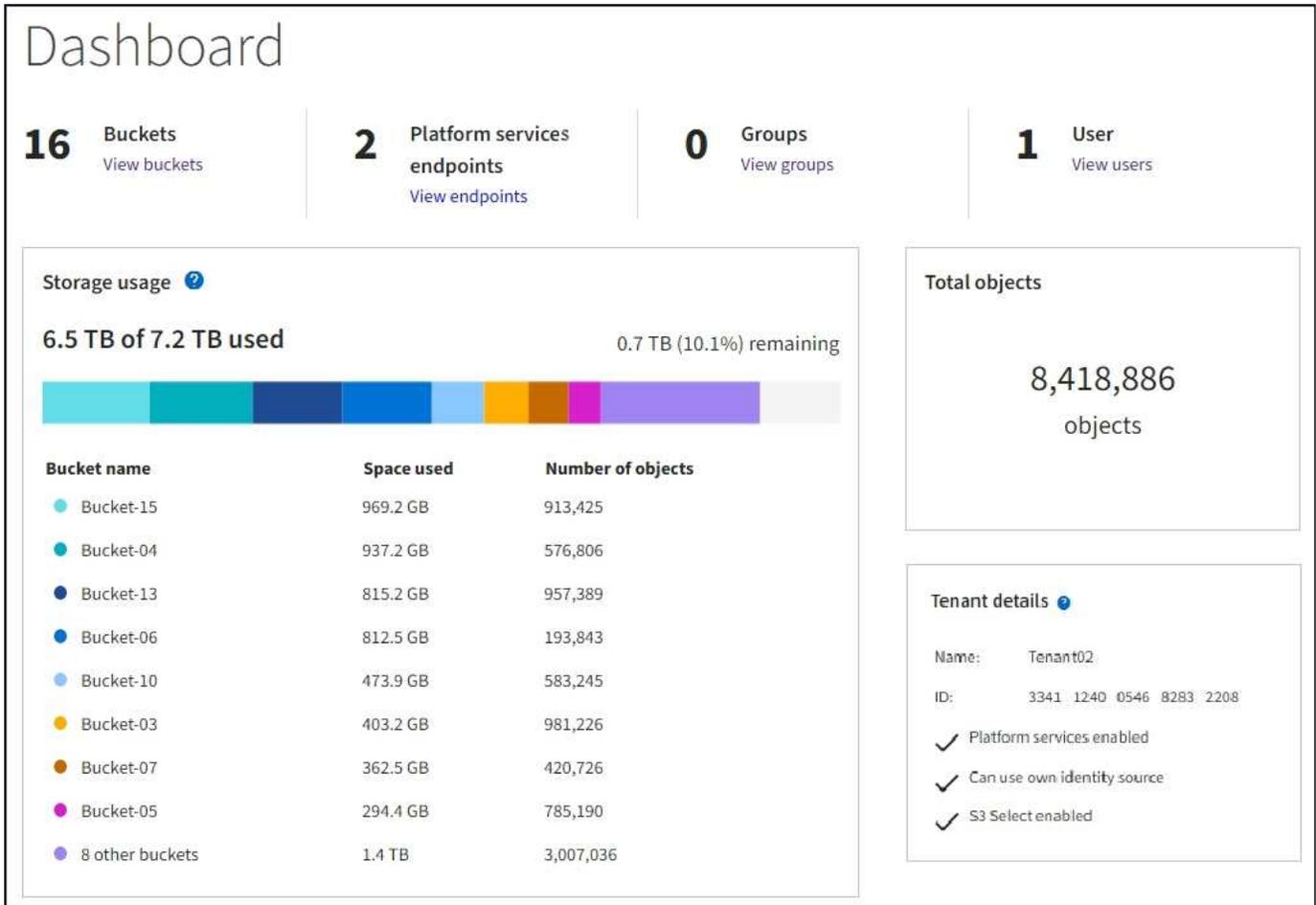
Diagramme und Diagramme fassen die Werte bestimmter StorageGRID-Metriken und -Attribute zusammen.

Das Grid Manager-Dashboard enthält Karten, die den verfügbaren Speicher für das Grid und jeden Standort zusammenfassen.



Im Fenster Storage Usage im Tenant Manager-Dashboard werden folgende Informationen angezeigt:

- Eine Liste der größten Buckets (S3) oder Container (Swift) für die Mandanten
- Ein Balkendiagramm, das die relative Größe der größten Buckets oder Container darstellt
- Der insgesamt verwendete Speicherplatz und, wenn ein Kontingent festgelegt ist, die Menge und der Prozentsatz des verbleibenden Speicherplatzes



Darüber hinaus stehen Diagramme zur Verfügung, die zeigen, wie sich StorageGRID-Metriken und -Attribute im Laufe der Zeit ändern, auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG > Tools > Grid-Topologie**.

Es gibt vier Arten von Diagrammen:

- **Grafana-Diagramme:** Auf der Seite Knoten werden Grafana-Diagramme verwendet, um die Werte der Prometheus-Kennzahlen im Laufe der Zeit zu zeichnen. Die Registerkarte **NODES > Netzwerk** für einen Storage Node enthält beispielsweise ein Grafana-Diagramm für den Netzwerk-Traffic.

DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

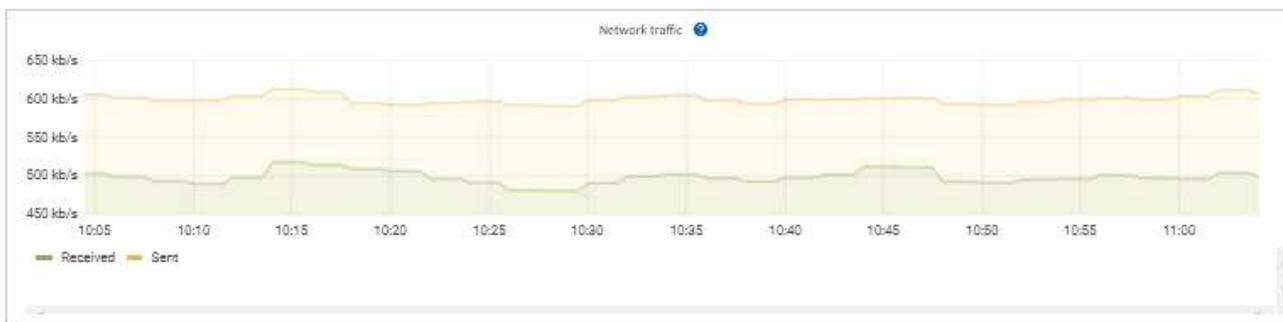
1 hour

1 day

1 week

1 month

Custom



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

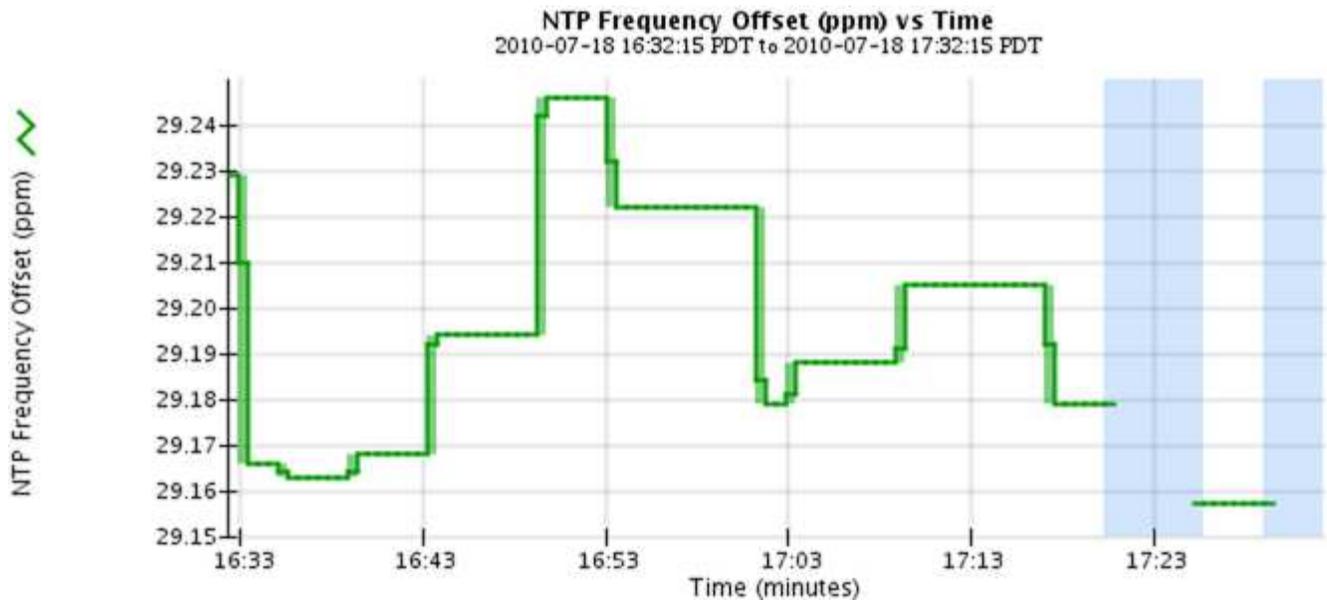
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

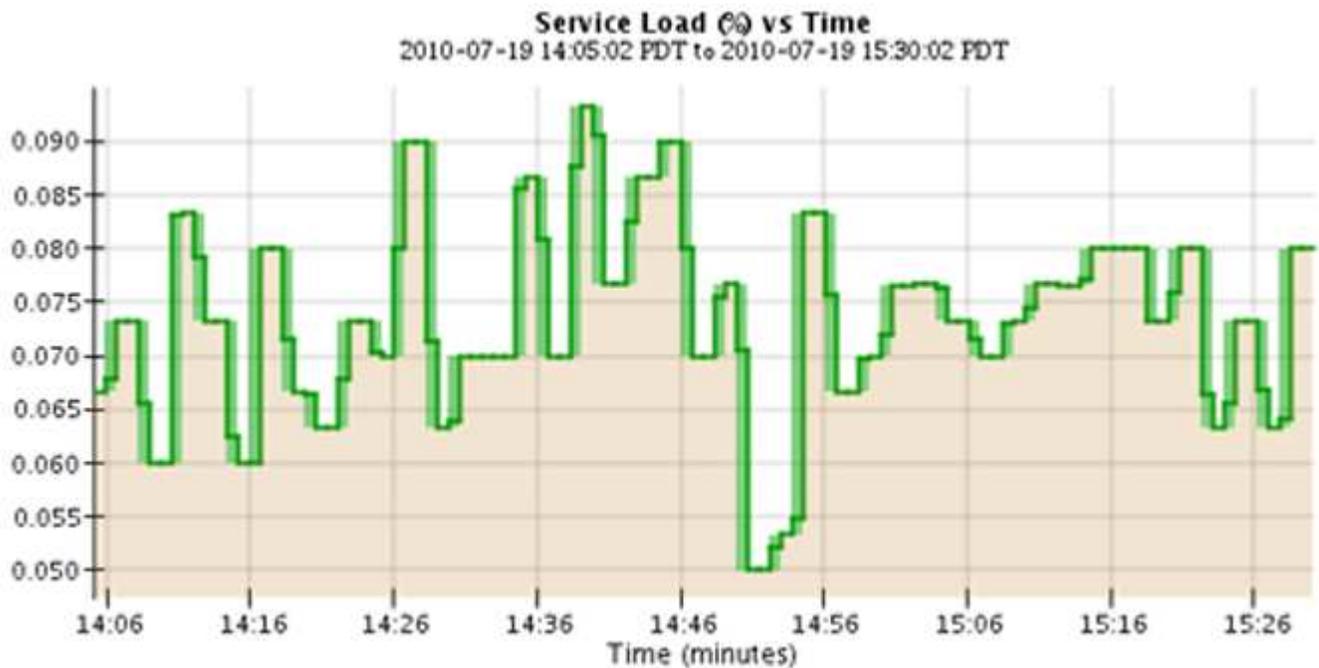


Grafana-Diagramme sind auch auf den vorkonfigurierten Dashboards enthalten, die auf der Seite **UNTERSTÜTZUNG > Tools > Metriken** verfügbar sind.

- **Liniendiagramme:** Verfügbar auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG > Tools > Grid Topologie** (wählen Sie das Diagrammsymbol  Nach einem Datenwert) werden Liniendiagramme verwendet, um die Werte von StorageGRID-Attributen zu zeichnen, die einen Einheitenwert haben (z. B. NTP-Frequenzversatz in ppm). Die Wertänderungen werden im Laufe der Zeit in regelmäßigen Datenintervallen (Bins) dargestellt.



- **Flächendiagramme:** Verfügbar auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG > Tools > Grid-Topologie** (wählen Sie das Diagrammsymbol  Nach einem Datenwert) werden Flächendiagramme verwendet, um volumetrische Attributmengen zu zeichnen, z. B. Objektanzahl oder Dienstlastwerte. Die Flächendiagramme ähneln den Liniendiagrammen, enthalten jedoch eine hellbraune Schattierung unter der Linie. Die Wertänderungen werden im Laufe der Zeit in regelmäßigen Datenintervallen (Bins) dargestellt.



- Einige Diagramme sind mit einem anderen Diagrammsymbol gekennzeichnet  Und haben ein anderes Format:

1 hour 1 day 1 week 1 month Custom

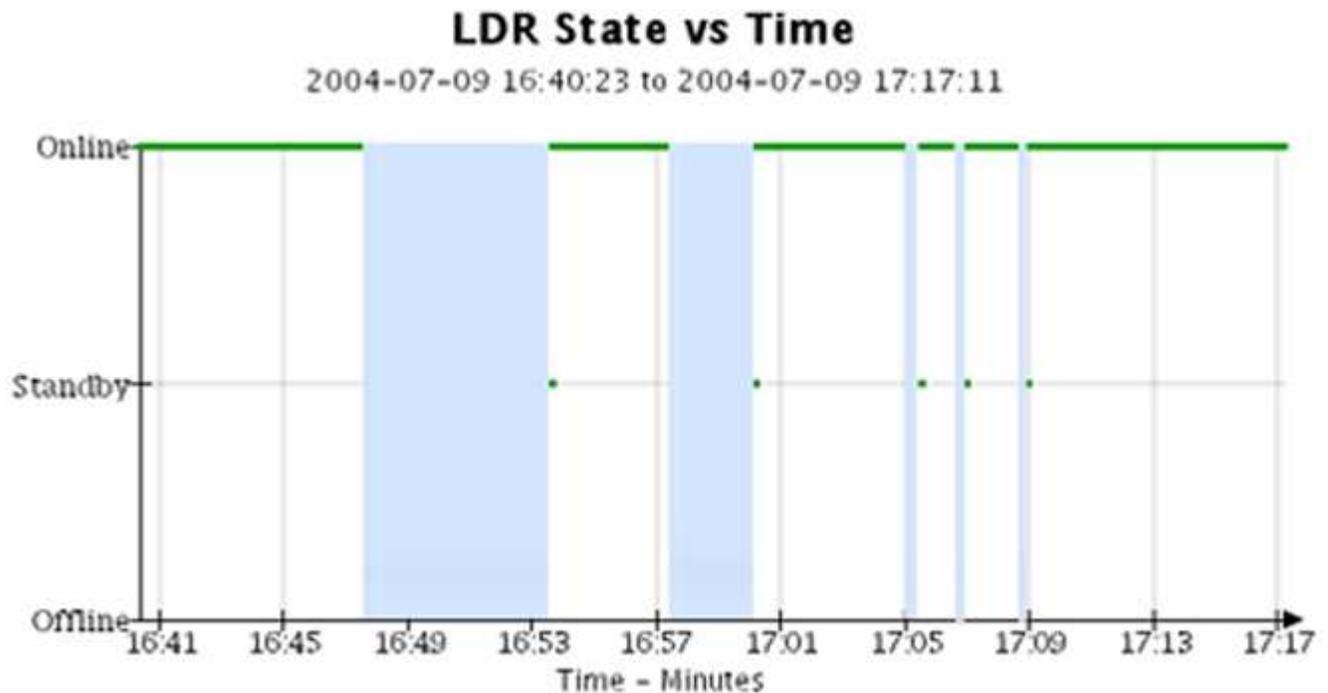
From: 2020-10-01 [calendar icon] 12 : 45 PM PDT

To: 2020-10-01 [calendar icon] 01 : 10 PM PDT Apply



Close

- **Zustandsdiagramm:** Verfügbar über die Seite **UNTERSTÜTZUNG > Tools > Grid-Topologie** (wählen Sie das Diagrammsymbol Nach einem Datenwert) werden Zustandsdiagramme verwendet, um Attributwerte zu zeichnen, die unterschiedliche Zustände darstellen, z. B. einen Servicestatus, der online, Standby oder offline sein kann. Statusdiagramme sind ähnlich wie Liniendiagramme, aber der Übergang ist ununterbrochen, d. h. der Wert springt von einem Statuswert zum anderen.



Verwandte Informationen

"Zeigen Sie die Seite Knoten an"

"Sehen Sie sich den Baum der Grid Topology an"

"Prüfen von Support-Kennzahlen"

Diagrammlegende

Die Linien und Farben, die zum Zeichnen von Diagrammen verwendet werden, haben eine besondere Bedeutung.

Probe	Bedeutung
	Gemeldete Attributwerte werden mit dunkelgrünen Linien dargestellt.
	Hellgrüne Schattierungen um dunkelgrüne Linien zeigen an, dass die tatsächlichen Werte in diesem Zeitbereich variieren und für eine schnellere Plottierung „binnt“ wurden. Die dunkle Linie stellt den gewichteten Durchschnitt dar. Der Bereich in hellgrün zeigt die maximalen und minimalen Werte innerhalb des Fachs an. Für Flächendiagramme wird ein hellbrauner Schattierung verwendet, um volumetrische Daten anzuzeigen.
	Leere Bereiche (keine Daten dargestellt) 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.
	Hellblaue Schattierung zeigt an, dass einige oder alle Attributwerte zu diesem Zeitpunkt unbestimmt waren; das Attribut war keine Meldung von Werten, da der Dienst sich in einem unbekanntem Zustand befand.
	Graue Schattierung zeigt an, dass einige oder alle Attributwerte zu diesem Zeitpunkt nicht bekannt waren, da der Dienst, der die Attribute meldet, administrativ herabgesetzt war.
	Eine Mischung aus grauem und blauem Schatten zeigt an, dass einige der Attributwerte zu diesem Zeitpunkt unbestimmt waren (weil der Dienst sich in einem unbekanntem Zustand befand), während andere nicht bekannt waren, weil der Dienst, der die Attribute meldet, administrativ nach unten lag.

Zeigen Sie Diagramme und Diagramme an

Die Seite Nodes enthält die Diagramme und Diagramme, auf die Sie regelmäßig zugreifen sollten, um Attribute wie Speicherkapazität und Durchsatz zu überwachen. In einigen Fällen, vor allem bei der Arbeit mit technischem Support, können Sie die Seite **SUPPORT > Tools > Grid Topology** verwenden, um auf zusätzliche Diagramme zuzugreifen.

Bevor Sie beginnen

Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".

Schritte

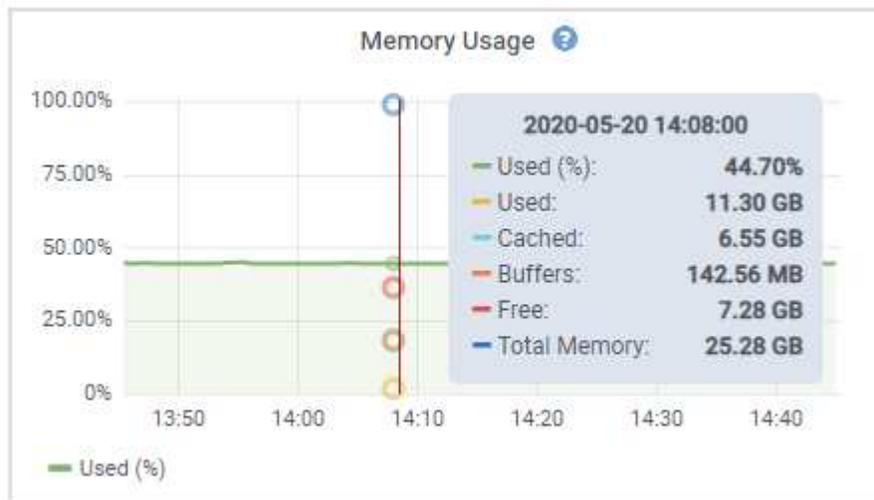
1. Wählen Sie **KNOTEN**. Wählen Sie dann einen Knoten, einen Standort oder das gesamte Raster aus.

2. Wählen Sie die Registerkarte aus, auf der Informationen angezeigt werden sollen.

Einige Registerkarten enthalten eine oder mehrere Grafana-Diagramme, mit denen die Werte der Prometheus-Kennzahlen im Laufe der Zeit dargestellt werden. Die Registerkarte **NODES > Hardware** für einen Knoten enthält beispielsweise zwei Grafana-Diagramme.



3. Setzen Sie den Cursor optional auf das Diagramm, um detailliertere Werte für einen bestimmten Zeitpunkt anzuzeigen.



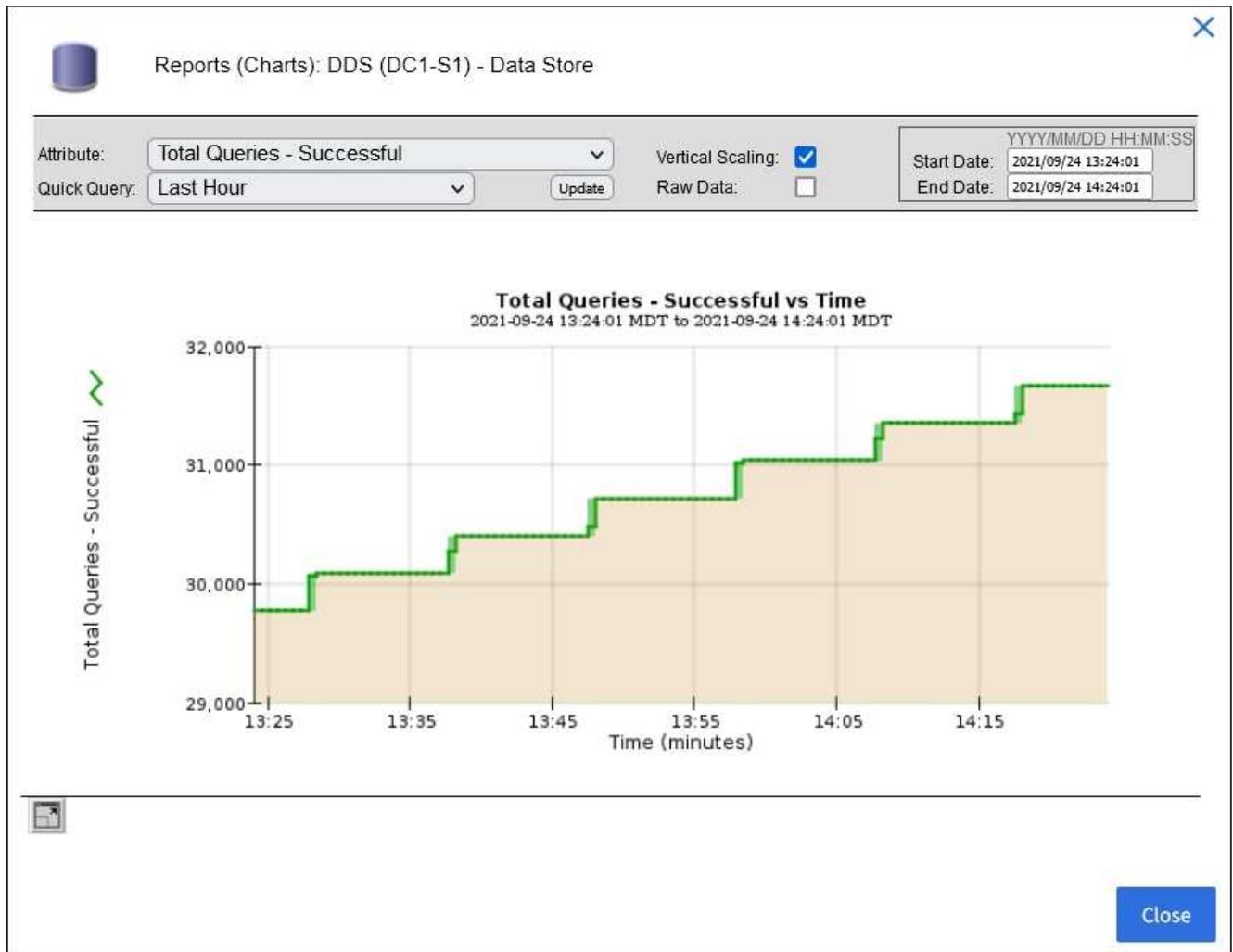
4. Bei Bedarf können Sie oft ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Wählen Sie in der Tabelle auf der Seite Knoten das Diagrammsymbol aus  Rechts neben dem Attributnamen.

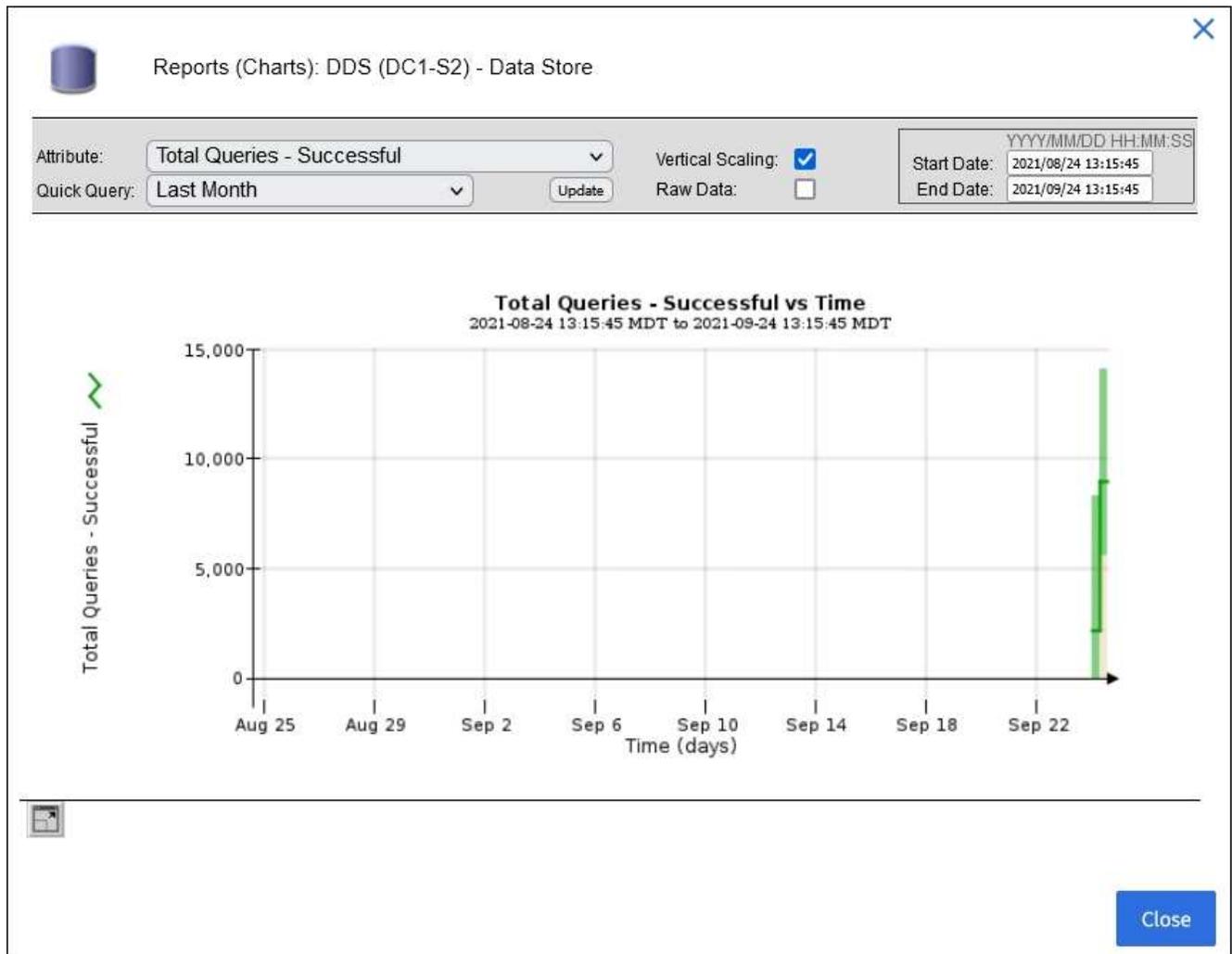


Diagramme sind nicht für alle Metriken und Attribute verfügbar.

Beispiel 1: Auf der Registerkarte Objekte für einen Speicherknoten können Sie das Diagrammsymbol auswählen  Um die Gesamtzahl der erfolgreichen Metadaten-Speicherabfragen für den Speicherknoten

anzuzeigen.

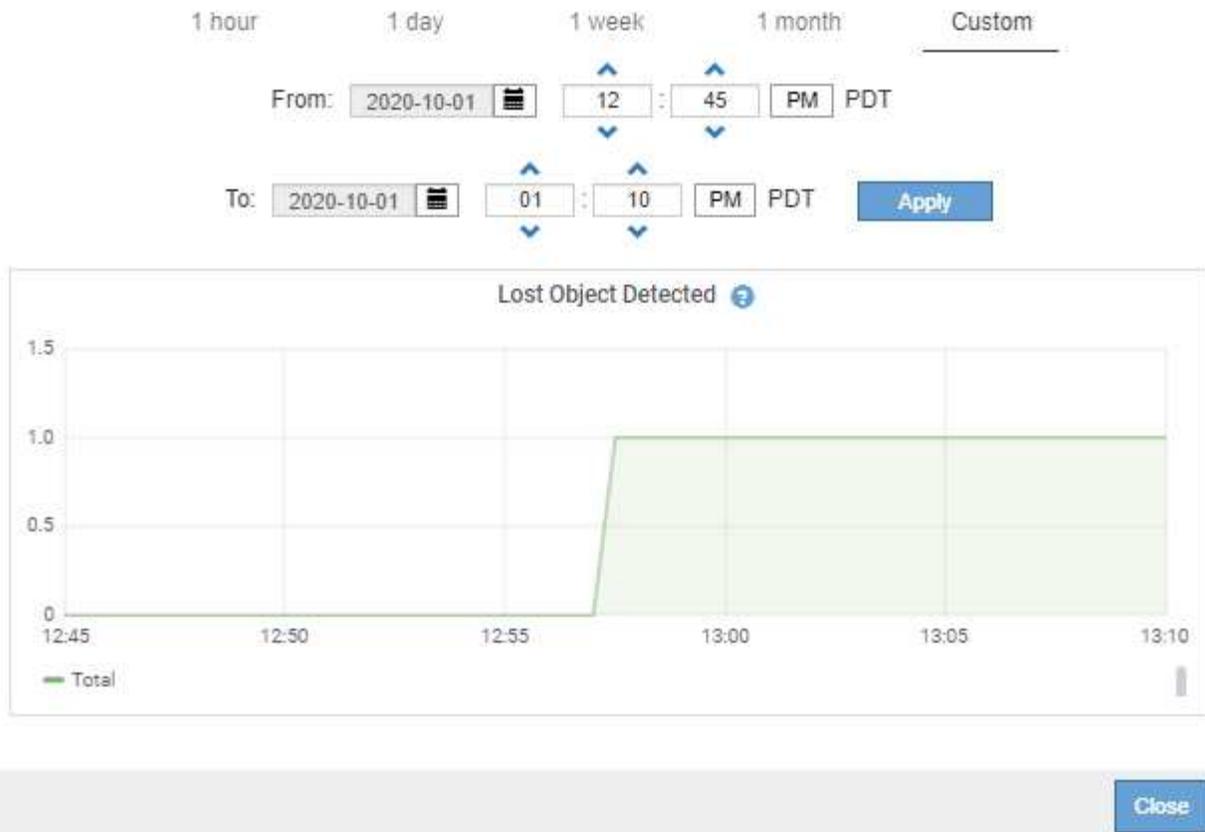




Beispiel 2: Auf der Registerkarte Objekte für einen Speicherknoten können Sie das Diagrammsymbol auswählen . Zeigt die Grafana-Grafik der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte an.

Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





5. Um Diagramme für Attribute anzuzeigen, die nicht auf der Seite Knoten angezeigt werden, wählen Sie **SUPPORT > Tools > Grid-Topologie**.
6. Wählen Sie **Grid Node > Component oder Service > Übersicht > Main** aus.
7. Wählen Sie das Diagrammsymbol aus  Neben dem Attribut.

Das Display wechselt automatisch zur Seite **Berichte > Diagramme**. Das Diagramm zeigt die Daten des Attributs über den letzten Tag an.

Diagramme generieren

Diagramme zeigen eine grafische Darstellung der Attributdatenwerte an. Die Berichte können an Datacenter-Standorten, Grid-Node, Komponenten oder Service erstellt werden.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Grid Node > Component oder Service > Berichte > Diagramme** aus.
3. Wählen Sie das Attribut aus der Dropdown-Liste **Attribut** aus, für das ein Bericht erstellt werden soll.
4. Um den Start der Y-Achse bei Null zu erzwingen, deaktivieren Sie das Kontrollkästchen **Vertikale Skalierung**.

- Um Werte mit voller Genauigkeit anzuzeigen, aktivieren Sie das Kontrollkästchen **Rohdaten** oder um Werte auf maximal drei Dezimalstellen zu runden (z. B. für als Prozentsätze gemeldete Attribute), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
- Wählen Sie den Zeitraum aus der Dropdown-Liste **Quick Query** aus, für den Sie einen Bericht erstellen möchten.

Wählen Sie die Option Benutzerdefinierte Abfrage aus, um einen bestimmten Zeitbereich auszuwählen.

Das Diagramm erscheint nach wenigen Augenblicken. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen.

- Wenn Sie Benutzerdefinierte Abfrage ausgewählt haben, passen Sie den Zeitraum für das Diagramm an, indem Sie die Optionen **Startdatum** und **Enddatum** eingeben.

Verwenden Sie das Format *YYYY/MM/DDHH:MM:SS* Ortszeit verwendet. Führende Nullen sind für das Format erforderlich. Beispiel: 2017/4/6 7:30:00 schlägt die Validierung fehl. Das richtige Format ist: 2017/04/06 07:30:00.

- Wählen Sie **Aktualisieren**.

Nach einigen Sekunden wird ein Diagramm erzeugt. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen. Abhängig von der für die Abfrage festgelegten Dauer wird entweder ein RAW-Textbericht oder ein aggregierter Textbericht angezeigt.

Verwenden Sie Textberichte

Textberichte zeigen eine textuelle Darstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Es gibt zwei Arten von Berichten, die je nach Zeitraum erstellt werden, für den Sie einen Bericht erstellen: RAW-Textberichte für Zeiträume unter einer Woche und Zusammenfassung von Textberichten für Zeiträume, die länger als eine Woche sind.

RAW-Textberichte

In einem RAW-Textbericht werden Details zum ausgewählten Attribut angezeigt:

- Empfangene Zeit: Lokales Datum und Uhrzeit, zu der ein Beispielwert der Daten eines Attributs vom NMS-Dienst verarbeitet wurde.
- Probenzeit: Lokales Datum und Uhrzeit, zu der ein Attributwert an der Quelle erfasst oder geändert wurde.
- Wert: Attributwert zur Probenzeit.

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 %

Zusammenfassen von Textberichten

Ein zusammengefasster Textbericht zeigt Daten über einen längeren Zeitraum (in der Regel eine Woche) an als einen reinen Textbericht. Jeder Eintrag ist das Ergebnis einer Zusammenfassung mehrerer Attributwerte (ein Aggregat von Attributwerten) durch den NMS-Dienst über einen Zeitraum in einem einzigen Eintrag mit durchschnittlichen, maximalen und minimalen Werten, die aus der Aggregation abgeleitet sind.

In jedem Eintrag werden die folgenden Informationen angezeigt:

- Aggregatzeit: Letztes lokales Datum und Zeitpunkt, zu dem der NMS-Dienst einen Satz von geänderten Attributwerten aggregiert (gesammelt) hat.
- Durchschnittswert: Der Mittelwert des Attributs 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

Erstellen von Textberichten

Textberichte zeigen eine textuelle Darstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Die Berichte können an Datacenter-Standorten, Grid-Node, Komponenten oder Service erstellt werden.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Für Attributdaten, die voraussichtlich kontinuierlich geändert werden, werden diese Attributdaten in regelmäßigen Abständen vom NMS-Dienst (an der Quelle) erfasst. Bei selten veränderlichen Attributdaten (z. B. Daten, die auf Ereignissen wie Statusänderungen basieren) wird ein Attributwert an den NMS-Dienst gesendet, wenn sich der Wert ändert.

Der angezeigte Berichtstyp hängt vom konfigurierten Zeitraum ab. Standardmäßig werden zusammengefasste Textberichte für Zeiträume generiert, die länger als eine Woche sind.

Der graue Text zeigt an, dass der Dienst während der Probenahme administrativ unten war. Blauer Text zeigt an, dass der Dienst in einem unbekanntem Zustand war.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Grid Node > Component oder Service > Berichte > Text** aus.
3. Wählen Sie das Attribut aus der Dropdown-Liste **Attribut** aus, für das ein Bericht erstellt werden soll.
4. Wählen Sie aus der Dropdown-Liste **Ergebnisse pro Seite** die Anzahl der Ergebnisse pro Seite aus.
5. Um Werte auf maximal drei Dezimalstellen zu runden (z. B. für als Prozentsätze gemeldete Attribute), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
6. Wählen Sie den Zeitraum aus der Dropdown-Liste **Quick Query** aus, für den Sie einen Bericht erstellen möchten.

Wählen Sie die Option Benutzerdefinierte Abfrage aus, um einen bestimmten Zeitbereich auszuwählen.

Der Bericht erscheint nach wenigen Augenblicken. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen.

7. Wenn Sie „Benutzerdefinierte Abfrage“ ausgewählt haben, müssen Sie den Zeitraum anpassen, an dem Sie einen Bericht erstellen möchten, indem Sie die Optionen **Startdatum** und **Enddatum** eingeben.

Verwenden Sie das Format YYYY/MM/DDHH:MM:SS Ortszeit verwendet. Führende Nullen sind für das Format erforderlich. Beispiel: 2017/4/6 7:30:00 schlägt die Validierung fehl. Das richtige Format ist: 2017/04/06 07:30:00.

8. Klicken Sie Auf **Aktualisieren**.

Nach wenigen Augenblicken wird ein Textbericht erstellt. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen. Abhängig von der für die Abfrage festgelegten Dauer wird entweder ein RAW-Textbericht oder ein aggregierter Textbericht angezeigt.

Exportieren von Textberichten

Exportierte Textberichte öffnen eine neue Browser-Registerkarte, auf der Sie die Daten auswählen und kopieren können.

Über diese Aufgabe

Die kopierten Daten können dann in einem neuen Dokument (z. B. in einer Tabelle) gespeichert und zur Analyse der Performance des StorageGRID-Systems verwendet werden.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Erstellen Sie einen Textbericht.
3. Klicken Sie Auf *Exportieren* .

Das Fenster Textbericht exportieren wird geöffnet, in dem der Bericht angezeigt wird.

Grid ID: 000 000

OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200

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 jetzt in ein Dokument eines Drittanbieters wie z. B. in eine Tabelle eingefügt werden.

PUT- und GET-Performance werden überwacht

Sie können die Performance bestimmter Vorgänge, z. B. Objektspeicher und -Abruf, überwachen, um Änderungen zu identifizieren, die möglicherweise weitere Untersuchungen erfordern.

Über diese Aufgabe

Um DIE PUT- und GET-Leistung zu überwachen, können Sie S3- und Swift-Befehle direkt von einer Workstation aus oder über die Open-Source S3tester-Anwendung ausführen. Mit diesen Methoden können Sie die Leistung unabhängig von Faktoren bewerten, die außerhalb von StorageGRID liegen, z. B. Probleme mit einer Client-Applikation oder Probleme mit einem externen Netzwerk.

Wenn SIE Tests für PUT- und GET-Vorgänge durchführen, beachten Sie folgende Richtlinien:

- Objektgrößen sind vergleichbar mit den Objekten, die normalerweise in das Grid eingespeist werden.
- Durchführung von Vorgängen an lokalen und Remote Standorten

Meldungen in "[Prüfprotokoll](#)" Geben Sie die Gesamtzeit an, die für die Ausführung bestimmter Vorgänge erforderlich ist. Um z. B. die Gesamtverarbeitungszeit für eine S3-GET-Anforderung zu bestimmen, können Sie den Wert des ZEITATTRIBUTS in der SGET-Audit-Nachricht prüfen. Das ZEITATTRIBUT finden Sie auch in den Audit-Meldungen für die folgenden Vorgänge:

- **S3:** LÖSCHEN, HOLEN, KOPF, Metadaten aktualisiert, POST, PUT
- **SWIFT:** LÖSCHEN, HOLEN, KOPF, SETZEN

Bei der Analyse von Ergebnissen sollten Sie die durchschnittliche Zeit zur Erfüllung einer Anfrage sowie den Gesamtdurchsatz betrachten, den Sie erreichen können. Wiederholen Sie die gleichen Tests regelmäßig, und notieren Sie die Ergebnisse, damit Sie Trends identifizieren können, die eine Untersuchung erfordern könnten.

- Das können Sie "[Laden Sie S3tester von Github herunter](#)".

Überwachen von Objektverifizierungsvorgängen

Das StorageGRID System kann die Integrität von Objektdaten auf Storage-Nodes überprüfen und sowohl beschädigte als auch fehlende Objekte prüfen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über die Berechtigung Maintenance oder Root verfügen.

Über diese Aufgabe

Zwei "[Verifizierungsprozesse](#)" Gewährleisten Sie gemeinsam die Datenintegrität:

- **Hintergrundüberprüfung** läuft automatisch und überprüft kontinuierlich die Richtigkeit der Objektdaten.

Hintergrund-Verifizierung überprüft automatisch und kontinuierlich alle Storage-Nodes, um festzustellen, ob es beschädigte Kopien von replizierten und mit Erasure Coding verschlüsselten Objektdaten gibt. Falls

Probleme gefunden werden, versucht das StorageGRID System automatisch, die beschädigten Objektdaten durch Kopien zu ersetzen, die an anderer Stelle im System gespeichert sind. Die Hintergrundüberprüfung wird nicht auf Archiv-Nodes oder auf Objekten in einem Cloud-Speicherpool ausgeführt.



Die Warnung **Unidentified Corrupt Object Detected** wird ausgelöst, wenn das System ein korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann.

- **Objektexistenz-Prüfung** kann von einem Nutzer ausgelöst werden, um die Existenz (obwohl nicht die Richtigkeit) von Objektdaten schneller zu überprüfen.

Die ObjektExistenz überprüft, ob alle erwarteten replizierten Kopien von Objekten und mit Erasure Coding verschlüsselten Fragmenten auf einem Storage Node vorhanden sind. Die Prüfung des Objektbestandes bietet eine Möglichkeit zur Überprüfung der Integrität von Speichergeräten, insbesondere dann, wenn kürzlich Probleme mit der Hardware die Datenintegrität beeinträchtigen könnten.

Sie sollten die Ergebnisse aus Hintergrundverifizierungen und Objektprüfungen regelmäßig überprüfen. Untersuchen Sie alle Instanzen beschädigter oder fehlender Objektdaten sofort, um die Ursache zu ermitteln.

Schritte

1. Prüfen Sie die Ergebnisse aus Hintergrundverifizierungen:

a. Wählen Sie **NODES > Storage Node > Objekte** aus.

b. Überprüfen Sie die Überprüfungsergebnisse:

- Um die Verifizierung replizierter Objektdaten zu prüfen, sehen Sie sich die Attribute im Abschnitt Überprüfung an.

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
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	

- Um die Überprüfung von Fragment mit Lösungscode zu überprüfen, wählen Sie **Storage Node > ILM** aus, und sehen Sie sich die Attribute im Abschnitt zur Verifizierung von Erasure-Coding an.

Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Wählen Sie das Fragezeichen aus ? Neben dem Namen eines Attributs wird Hilfetext angezeigt.

2. Überprüfen Sie die Ergebnisse von Objektprüfaufträgen:

a. Wählen Sie **WARTUNG > Objekt Existenzprüfung > Jobverlauf**.

b. Scannen Sie die Spalte „fehlende Objektkopien erkannt“. Wenn bei Jobs 100 oder mehr fehlende Objektkopien vorhanden waren und die Warnmeldung **Objects lost** ausgelöst wurde, wenden Sie sich an den technischen Support.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify if objects defined by your ILM policy, still exist on the volumes.

Active job | **Job history**

<input type="checkbox"/>	Job ID ?	Status	Nodes (volumes) ?	Missing object copies detected ?
<input type="checkbox"/>	15816859223101303015	Completed	DC2-S1 (3 volumes)	0
<input type="checkbox"/>	12538643155010477372	Completed	DC1-S3 (1 volume)	0
<input type="checkbox"/>	5490044849774982476	Completed	DC1-S2 (1 volume)	0
<input type="checkbox"/>	3395284277055907678	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and <u>7 more</u>	0

Monitoring von Ereignissen

Sie können Ereignisse überwachen, die von einem Grid-Node erkannt werden, einschließlich benutzerdefinierter Ereignisse, die Sie erstellt haben, um Ereignisse zu verfolgen, die auf dem Syslog-Server protokolliert werden. Die Meldung Letztes Ereignis, die im Grid Manager angezeigt wird, enthält weitere Informationen zum letzten Ereignis.

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log` Protokolldatei. Siehe "[Referenz für Protokolldateien](#)".

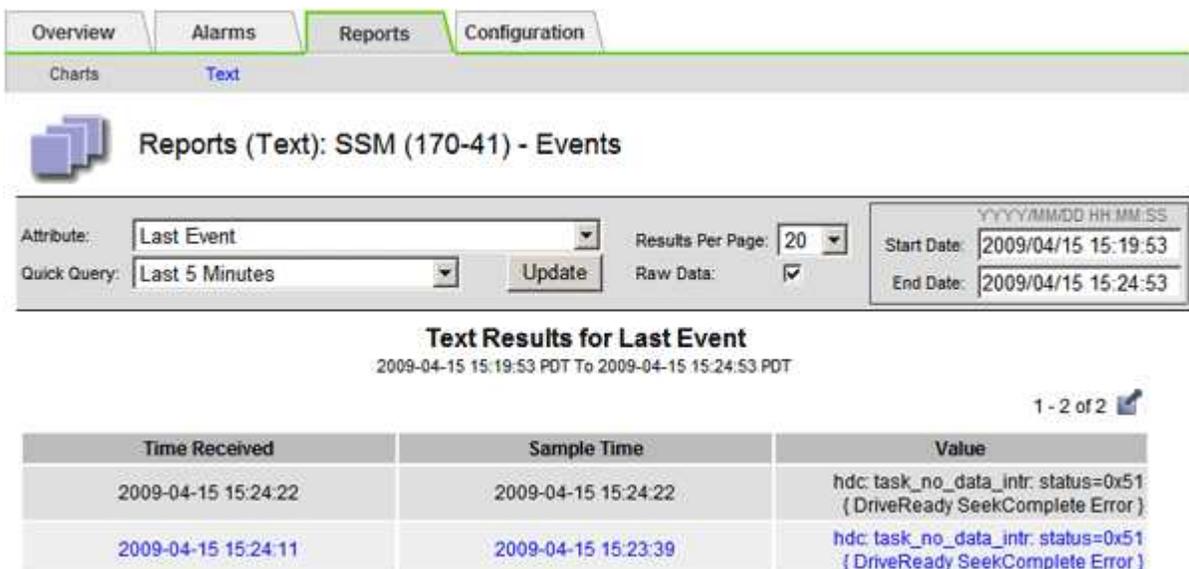
Der SMTT-Alarm (Total Events) kann wiederholt durch Probleme wie Netzwerkprobleme, Stromausfälle oder Upgrades ausgelöst werden. Dieser Abschnitt enthält Informationen zur Untersuchung von Ereignissen, sodass Sie besser verstehen können, warum diese Alarmer aufgetreten sind. Wenn ein Ereignis aufgrund eines bekannten Problems aufgetreten ist, können die Ereigniszähler sicher zurückgesetzt werden.

Schritte

- Überprüfen Sie die Systemereignisse für jeden Grid-Node:
 - Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - Wählen Sie **site > GRID Node > SSM > Events > Übersicht > Main**.
- Erstellen Sie eine Liste früherer Ereignismeldungen, um Probleme zu isolieren, die in der Vergangenheit aufgetreten sind:
 - Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - Wählen Sie **site > GRID Node > SSM > Events > Berichte** aus.
 - Wählen Sie **Text**.

Das Attribut **Letztes Ereignis** wird im nicht angezeigt "[Diagrammansicht](#)". So zeigen Sie es an:

- Ändern Sie **Attribut** in **Letztes Ereignis**.
- Wählen Sie optional einen Zeitraum für **Quick Query** aus.
- Wählen Sie **Aktualisieren**.



Overview Alarms Reports Configuration

Charts Text

Reports (Text): SSM (170-41) - Events

Attribute: Last Event Results Per Page: 20 Start Date: 2009/04/15 15:19:53
Quick Query: Last 5 Minutes Update Raw Data: End Date: 2009/04/15 15:24:53

Text Results for Last Event
2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

1 - 2 of 2

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Erstellen benutzerdefinierter Syslog-Ereignisse

Benutzerdefinierte Ereignisse ermöglichen die Verfolgung aller Kernel-, Daemon-, Fehler- und kritischen Benutzerereignisse auf der Ebene, die beim Syslog-Server protokolliert werden. Ein benutzerdefiniertes Ereignis kann nützlich sein, um das Auftreten von Systemprotokollmeldungen zu überwachen (und damit Netzwerksicherheitsereignisse und Hardwarefehler).

Über diese Aufgabe

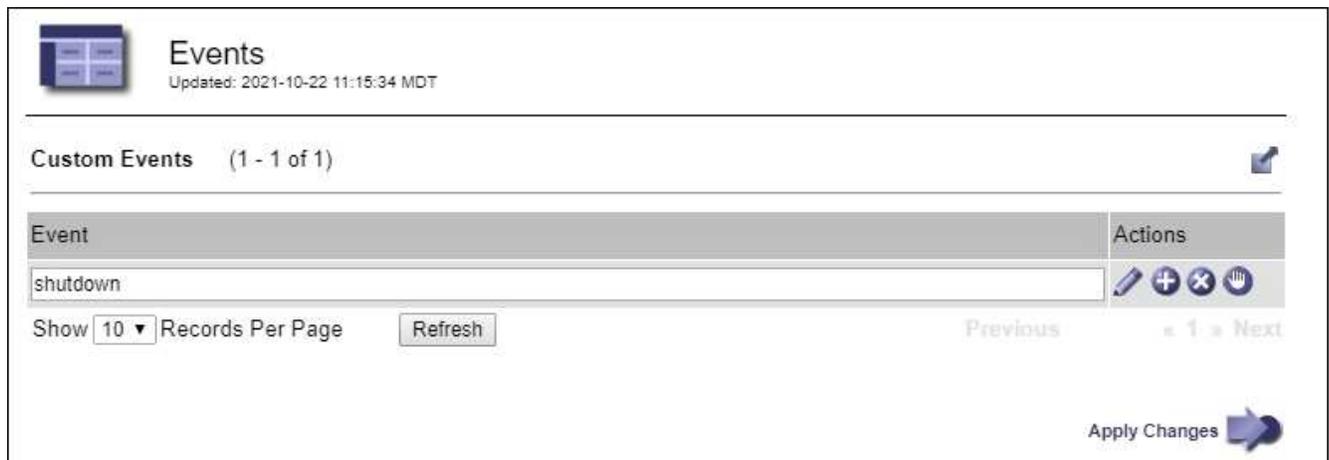
Ziehen Sie in Betracht, benutzerdefinierte Ereignisse zu erstellen, um wiederkehrende Probleme zu überwachen. Die folgenden Überlegungen gelten für benutzerdefinierte Ereignisse.

- Nach der Erstellung eines benutzerdefinierten Ereignisses wird jeder Vorgang überwacht.
- So erstellen Sie ein benutzerdefiniertes Ereignis basierend auf Schlüsselwörtern im `/var/local/log/messages` Dateien, die Protokolle in diesen Dateien müssen:
 - Vom Kernel generiert
 - Wird vom Daemon oder vom Benutzerprogramm auf der Fehler- oder kritischen Ebene generiert

Hinweis: nicht alle Einträge im `/var/local/log/messages` Die Dateien werden abgeglichen, sofern sie nicht die oben genannten Anforderungen erfüllen.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Benutzerdefinierte Ereignisse**.
2. Klicken Sie Auf **Bearbeiten**  (Oder **Einfügen**  Wenn dies nicht das erste Ereignis ist).
3. Geben Sie eine benutzerdefinierte Ereigniszeichenfolge ein, z. B. Herunterfahren



4. Wählen Sie **Änderungen Anwenden**.
5. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
6. Wählen Sie **Grid Node > SSM > Events** aus.
7. Suchen Sie den Eintrag für benutzerdefinierte Ereignisse in der Ereignistabelle, und überwachen Sie den Wert für **Zählung**.

Wenn die Anzahl erhöht wird, wird ein benutzerdefiniertes Ereignis, das Sie überwachen, auf diesem Grid-Node ausgelöst.

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC1-ADM1) - Events

Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State:	Connected	
Total Events:	0	
Last Event:	No Events	

Description	Count	
Abnormal Software Events	0	
Account Service Events	0	
Cassandra Errors	0	
Cassandra Heap Out Of Memory Errors	0	
Chunk Service Events	0	
Custom Events	0	
Data-Mover Service Events	0	
File System Errors	0	
Forced Termination Events	0	
Grid Node Errors	0	
Hotfix Installation Failure Events	0	
I/O Errors	0	
IDE Errors	0	
Identity Service Events	0	
Kernel Errors	0	
Kernel Memory Allocation Failure	0	
Keystone Service Events	0	
Network Receive Errors	0	
Network Transmit Errors	0	
Out Of Memory Errors	0	
Replicated State Machine Service Events	0	
SCSI Errors	0	

Setzen Sie die Anzahl der benutzerdefinierten Ereignisse auf Null zurück

Wenn Sie den Zähler nur für benutzerdefinierte Ereignisse zurücksetzen möchten, müssen Sie die Seite Grid Topology im Menü Support verwenden.

Beim Zurücksetzen eines Zählers wird der Alarm durch das nächste Ereignis ausgelöst. Wenn Sie einen Alarm quittieren, wird dieser Alarm dagegen nur erneut ausgelöst, wenn der nächste Schwellwert erreicht wird.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Grid Node > SSM > Events > Konfiguration > Main** aus.
3. Aktivieren Sie das Kontrollkästchen **Zurücksetzen** für benutzerdefinierte Ereignisse.

Configuration		
Main Alarms		
 Configuration: SSM (DC2-ADM1) - Events Updated: 2018-04-11 10:35:44 MDT		
Description	Count	Reset
Abnormal Software Events	0	<input type="checkbox"/>
Account Service Events	0	<input type="checkbox"/>
Cassandra Errors	0	<input type="checkbox"/>
Cassandra Heap Out Of Memory Errors	0	<input type="checkbox"/>
Custom Events	0	<input checked="" type="checkbox"/>
File System Errors	0	<input type="checkbox"/>
Forced Termination Events	0	<input type="checkbox"/>

4. Wählen Sie **Änderungen Anwenden**.

Audit-Meldungen prüfen

Audit-Meldungen helfen Ihnen, die detaillierten Vorgänge Ihres StorageGRID Systems besser zu verstehen. Sie können mithilfe von Audit-Protokollen Probleme beheben und die Performance bewerten.

Während des normalen Systembetriebs generieren alle StorageGRID Services wie folgt Audit-Meldungen:

- Systemaudits-Meldungen betreffen das Auditing des Systems selbst, den Status von Grid-Nodes, systemweite Task-Aktivitäten und Service-Backup-Vorgänge.
- Audit-Nachrichten zum Objekt-Storage beziehen sich auf die Storage- und das Management von Objekten in StorageGRID, einschließlich Objekt-Storage und -Abruf, Grid-Node- zu Grid-Node-Transfers und Verifizierungen.
- Lese- und Schreibvorgänge von Clients werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Erstellen, Ändern oder Abrufen eines Objekts vorgibt.
- Managementaudits protokollieren Benutzeranfragen an die Management-API.

Jeder Admin-Knoten speichert Audit-Meldungen in Textdateien. Die Revisionsfreigabe enthält die aktive Datei (Audit.log) sowie komprimierte Audit-Protokolle aus früheren Tagen. Jeder Node im Raster speichert auch eine Kopie der auf dem Node generierten Audit-Informationen.

Für den einfachen Zugriff auf Audit-Protokolle können Sie ["Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS"](#). Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe ["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#).

Einzelheiten zur Audit-Log-Datei, zum Format der Audit-Meldungen, zu den Typen der Audit-Meldungen und zu den zur Analyse von Audit-Meldungen verfügbaren Tools finden Sie unter ["Prüfung von Audit-Protokollen"](#).

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 auf dem primären Admin-Knoten unter Verwendung eines beim Grid-Manager angemeldet sein ["Unterstützter Webbrowser"](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Über diese Aufgabe

Sie können den Grid Manager zum Sammeln verwenden ["Log-Dateien"](#), Systemdaten und Konfigurationsdaten von einem beliebigen Grid-Knoten für den von Ihnen ausgewählten Zeitraum. Die Daten werden in einer .tar.gz-Datei gesammelt und archiviert, die Sie dann auf Ihren lokalen Computer herunterladen können.

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe ["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#).

Schritte

1. Wählen Sie **SUPPORT > Extras > Protokolle**.

2. Wählen Sie die Grid-Knoten aus, für die Sie Protokolldateien sammeln möchten.

Je nach Bedarf können Sie Log-Dateien für das gesamte Grid oder einen gesamten Datacenter-Standort sammeln.

3. Wählen Sie eine **Startzeit** und **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, könnte das Protokollarchiv zu groß werden, um auf einem Knoten gespeichert zu werden, oder zu groß, um zum Download an den 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 für die Fehlerbehebung verwendet. Die gesammelten Protokolle sind eine Teilmenge der verfügbaren Anwendungsprotokolle.
- **Audit Logs:** Protokolle, die die während des normalen Systembetriebs erzeugten Audit-Meldungen enthalten.
- **Network Trace:** Protokolle, die für das Debuggen von Netzwerken verwendet werden.
- **Prometheus Datenbank:** Zeitreihenkenzahlen aus den Diensten auf allen Knoten.

5. Geben Sie optional Notizen zu den Protokolldateien ein, die Sie im Textfeld **Hinweise** sammeln.

Mithilfe dieser Hinweise können Sie Informationen zum technischen Support über das Problem geben, das Sie zum Erfassen der Protokolldateien aufgefordert hat. Ihre Notizen werden einer Datei namens

hinzugefügt `info.txt`, Zusammen mit anderen Informationen über die Log-Datei-Sammlung. Der `info.txt` Die Datei wird im Archivpaket der Protokolldatei gespeichert.

6. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System im Textfeld **Provisioning-Passphrase** ein.
7. Wählen Sie **Protokolle Sammeln**.

Wenn Sie eine neue Anforderung senden, wird die vorherige Sammlung von Protokolldateien gelöscht.

Auf der Seite „Protokolle“ können Sie den Fortschritt der Sammlung von Protokolldateien für jeden Grid-Knoten überwachen.

Wenn Sie eine Fehlermeldung über die Protokollgröße erhalten, versuchen Sie, Protokolle für einen kürzeren Zeitraum oder für weniger Nodes zu sammeln.

8. Wählen Sie **Download**, wenn die Sammlung der Protokolldatei abgeschlossen ist.

Die Datei `.tar.gz` enthält alle Protokolldateien aller Grid-Knoten, in denen die Protokollsammlung erfolgreich war. In der kombinierten `.tar.gz`-Datei gibt es für jeden Grid-Knoten ein Log-File-Archiv.

Nachdem Sie fertig sind

Sie können das Archivpaket für die Protokolldatei später erneut herunterladen, wenn Sie es benötigen.

Optional können Sie **Löschen** wählen, um das Archiv-Paket der Protokolldatei zu entfernen und Speicherplatz freizugeben. Das aktuelle Archivpaket für die Protokolldatei wird beim nächsten Erfassen von Protokolldateien automatisch entfernt.

Senden Sie manuell eine AutoSupport Meldung aus

Um den technischen Support bei der Fehlerbehebung bei Problemen mit Ihrem StorageGRID System zu unterstützen, können Sie manuell eine AutoSupport Meldung auslösen, die gesendet werden soll.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über die Berechtigung Root-Zugriff oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **SUPPORT > Werkzeuge > AutoSupport**.
2. Wählen Sie auf der Registerkarte **Einstellungen** die Option **vom Benutzer ausgelöste AutoSupport** senden.

StorageGRID versucht, eine AutoSupport Nachricht an den technischen Support zu senden. Wenn der Versuch erfolgreich ist, werden die **aktuellsten Ergebnisse** und **Letzte erfolgreiche Zeit** Werte auf der Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, werden die **neuesten Ergebnisse**-Werte auf „Fehlgeschlagen“ aktualisiert, und StorageGRID versucht nicht, die AutoSupport-Nachricht erneut zu senden.

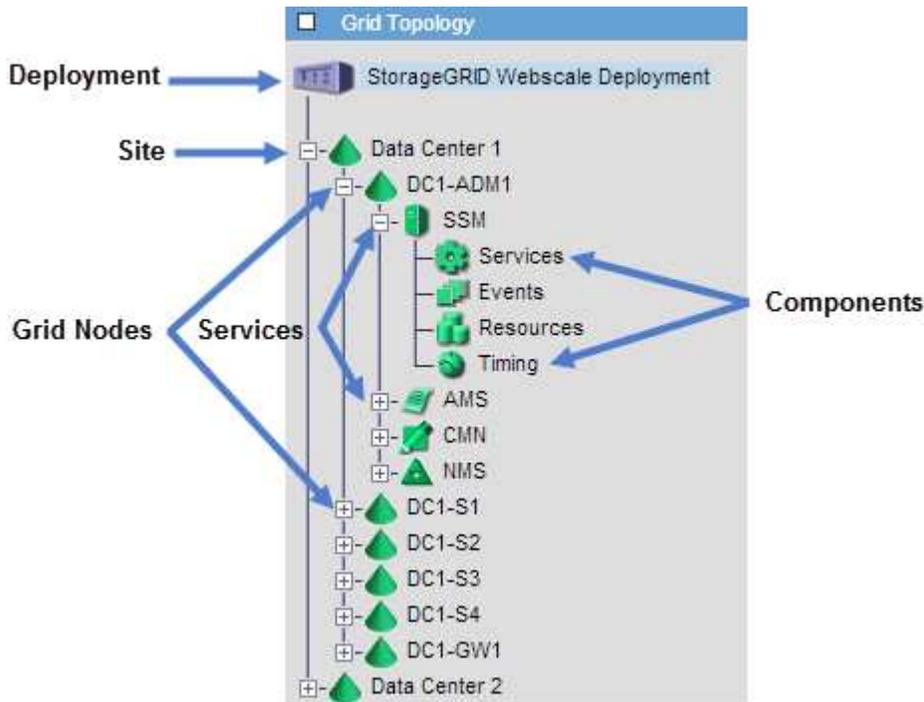


Nachdem Sie eine vom Benutzer ausgelöste AutoSupport-Nachricht gesendet haben, aktualisieren Sie die AutoSupport-Seite im Browser nach 1 Minute, um auf die neuesten Ergebnisse zuzugreifen.

Sehen Sie sich den Baum der Grid Topology an

Die Grid Topology-Struktur bietet Zugriff auf detaillierte Informationen zu StorageGRID Systemelementen, einschließlich Standorten, Grid-Nodes, Services und Komponenten. In den meisten Fällen müssen Sie nur auf die Grid Topology-Struktur zugreifen, wenn Sie in der Dokumentation oder bei der Arbeit mit technischem Support angewiesen sind.

Um auf den Baum der Grid Topology zuzugreifen, wählen Sie **UNTERSTÜTZUNG > Tools > Grid-Topologie**.



Klicken Sie auf, um die Struktur der Grid Topology zu erweitern oder zu reduzieren **+** Oder **-** Am Standort, auf dem Node oder auf dem Service Level. Um alle Elemente der gesamten Site oder in jedem Knoten zu erweitern oder auszublenden, halten Sie die **<Strg>**-Taste gedrückt, und klicken Sie auf.

StorageGRID Attribute

Attribute berichten Werte und Status für viele Funktionen des StorageGRID-Systems. Für jeden Grid-Node, jeden Standort und das gesamte Raster sind Attributwerte verfügbar.

StorageGRID-Attribute werden an mehreren Stellen im Grid-Manager verwendet:

- **Knoten Seite:** Viele der auf der Seite Knoten angezeigten Werte sind StorageGRID-Attribute. (Auf den Seiten Nodes werden auch die Kennzahlen Prometheus angezeigt.)
- **Alarmer:** Wenn Attribute definierte Schwellenwerte erreichen, werden StorageGRID-Alarmer (Altsystem) auf bestimmten Schweregraden ausgelöst.
- **Grid Topology Tree:** Attributwerte werden im Grid Topology Tree (**UNTERSTÜTZUNG > Tools > Grid Topology**) angezeigt.
- **Ereignisse:** Systemereignisse treten auf, wenn bestimmte Attribute einen Fehler oder Fehlerzustand für einen Knoten aufzeichnen, einschließlich Fehler wie Netzwerkfehler.

Attributwerte

Die Attribute werden nach bestem Aufwand gemeldet und sind ungefähr richtig. Unter bestimmten Umständen können Attributaktualisierungen verloren gehen, beispielsweise der Absturz eines Service oder der Ausfall und die Wiederherstellung eines Grid-Node.

Darüber hinaus kann es zu Verzögerungen bei der Ausbreitung kommen, dass die Meldung von Attributen beeinträchtigt wird. Aktualisierte Werte für die meisten Attribute werden in festen Intervallen an das StorageGRID-System gesendet. Es kann mehrere Minuten dauern, bis ein Update im System sichtbar ist, und zwei Attribute, die sich mehr oder weniger gleichzeitig ändern, können zu leicht unterschiedlichen Zeiten gemeldet werden.

Prüfen von Support-Kennzahlen

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support detaillierte Metriken und Diagramme für Ihr StorageGRID System prüfen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Auf der Seite Metriken können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist Open-Source-Software zum Sammeln von Kennzahlen. Grafana ist Open-Source-Software zur Visualisierung von Kennzahlen.



Die auf der Seite Metriken verfügbaren Tools sind für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe Liste von "[Häufig verwendete Prometheus-Kennzahlen](#)".

Schritte

1. Wählen Sie unter Anleitung des technischen Supports **SUPPORT > Tools > Metrics** aus.

Ein Beispiel für die Seite Metriken ist hier aufgeführt:

Metrics

Access charts and metrics to help troubleshoot issues.

i The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- <https://...>

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	EC Overview	Replicated Read Path Overview
Account Service Overview	Grid	S3 - Node
Alertmanager	ILM	S3 Overview
Audit Overview	Identity Service Overview	S3 Select
Cassandra Cluster Overview	Ingests	Site
Cassandra Network Overview	Node	Support
Cassandra Node Overview	Node (Internal Use)	Traces
Cross Grid Replication	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	

2. Um die aktuellen Werte der StorageGRID-Metriken abzufragen und Diagramme der Werte im Zeitverlauf anzuzeigen, klicken Sie im Abschnitt Prometheus auf den Link.

Das Prometheus-Interface wird angezeigt. Sie können über diese Schnittstelle Abfragen für die verfügbaren StorageGRID-Metriken ausführen und StorageGRID-Metriken im Laufe der Zeit grafisch darstellen.

Prometheus Alerts Graph Status ▾ Help

Enable query history

Expression (press Shift+Enter for newlines)

Execute - insert metric at cursor - ▾

Graph Console

Element	Value
no data	

Remove Graph

Add Graph



Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

- Um über einen längeren Zeitraum auf vorkonfigurierte Dashboards mit Diagrammen zu StorageGRID-Kennzahlen zuzugreifen, klicken Sie im Abschnitt „Grafana“ auf die Links.

Die Grafana-Schnittstelle für den ausgewählten Link wird angezeigt.



Führen Sie eine Diagnose aus

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support eine Diagnose auf Ihrem StorageGRID-System durchführen und die Ergebnisse überprüfen.

- ["Prüfen von Support-Kennzahlen"](#)
- ["Häufig verwendete Prometheus-Kennzahlen"](#)

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die Seite Diagnose führt eine Reihe von diagnostischen Prüfungen zum aktuellen Status des Rasters durch. Jede diagnostische Prüfung kann einen von drei Zuständen haben:

-  **Normal:** Alle Werte liegen im Normalbereich.
-  **Achtung:** Ein oder mehrere Werte liegen außerhalb des normalen Bereichs.
-  **Achtung:** Ein oder mehrere der Werte liegen deutlich außerhalb des normalen Bereichs.

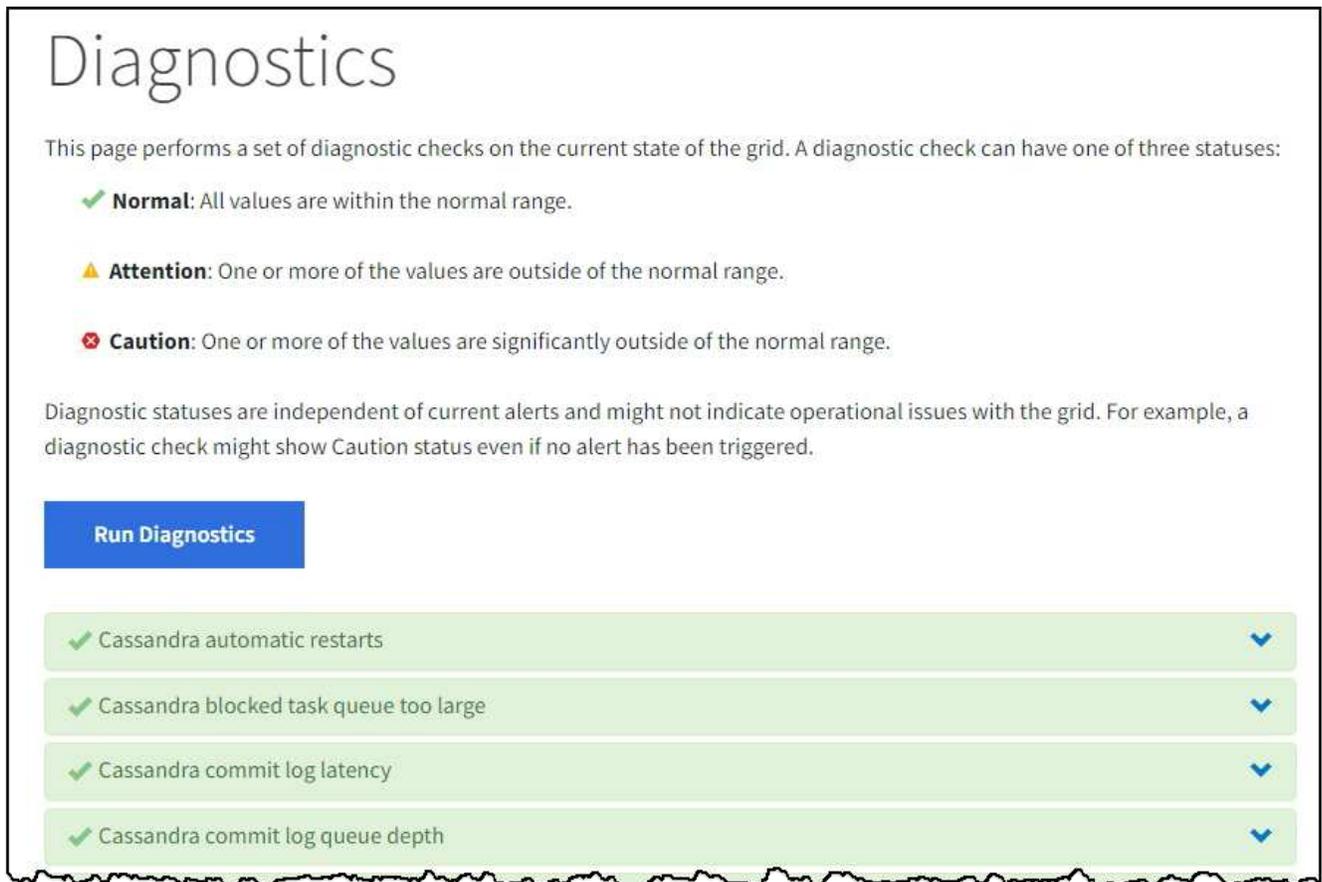
Diagnosestatus sind unabhängig von aktuellen Warnungen und zeigen möglicherweise keine betrieblichen Probleme mit dem Raster an. Beispielsweise wird bei einer Diagnose-Prüfung möglicherweise der Status „Achtung“ angezeigt, auch wenn keine Meldung ausgelöst wurde.

Schritte

1. Wählen Sie **SUPPORT > Tools > Diagnose**.

Die Seite Diagnose wird angezeigt und zeigt die Ergebnisse für jede Diagnostiktest an. Die Ergebnisse sind nach Schweregrad (Achtung, Achtung und dann normal) sortiert. Innerhalb jedes Schweregrads werden die Ergebnisse alphabetisch sortiert.

In diesem Beispiel haben alle Diagnosen einen normalen Status.



The screenshot shows a web interface titled "Diagnostics". It explains that diagnostic checks can have three statuses: Normal (green checkmark), Attention (yellow warning triangle), and Caution (red X). Below this, a blue button labeled "Run Diagnostics" is visible. Underneath, there is a list of four diagnostic checks, all of which are marked with a green checkmark, indicating a "Normal" status. Each check has a dropdown arrow on the right side.

Diagnostic Check	Status
Cassandra automatic restarts	Normal
Cassandra blocked task queue too large	Normal
Cassandra commit log latency	Normal
Cassandra commit log queue depth	Normal

2. Wenn Sie mehr über eine bestimmte Diagnose erfahren möchten, klicken Sie auf eine beliebige Stelle in der Zeile.

Details zur Diagnose und ihren aktuellen Ergebnissen werden angezeigt. Folgende Details sind aufgelistet:

- **Status:** Der aktuelle Status dieser Diagnose: Normal, Achtung oder Achtung.
- **Prometheus query:** Bei Verwendung für die Diagnose, der Prometheus Ausdruck, der verwendet

wurde, um die Statuswerte zu generieren. (Ein Prometheus-Ausdruck wird nicht für alle Diagnosen verwendet.)

- **Schwellenwerte:** Wenn für die Diagnose verfügbar, die systemdefinierten Schwellenwerte für jeden anormalen 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 Node in einem StorageGRID System angezeigt. Alle Node-Werte liegen unter den Warn- und Warnschwellenwerten, sodass der Gesamtstatus der Diagnose normal ist.

✓ **CPU utilization**

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status ✓ Normal

Prometheus query `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`
[View in Prometheus](#)

Thresholds
⚠ Attention >= 75%
✖ Caution >= 95%

Status	Instance	CPU Utilization
✓	DC1-ADM1	2.598%
✓	DC1-ARC1	0.937%
✓	DC1-G1	2.119%
✓	DC1-S1	8.708%
✓	DC1-S2	8.142%
✓	DC1-S3	9.669%
✓	DC2-ADM1	2.515%
✓	DC2-ARC1	1.152%
✓	DC2-S1	8.204%
✓	DC2-S2	5.000%
✓	DC2-S3	10.469%

3. **Optional:** Um Grafana-Diagramme zu 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 auf dem Node-Dashboard die CPU-Auslastung für diesen Node und andere Grafana-Diagramme für den Node angezeigt.



Sie können auch über den Abschnitt „Grafana“ auf der Seite * SUPPORT* > **Tools** > **Metriken** auf die vorkonfigurierten Dashboards von Grafana zugreifen.



4. **Optional:** Um ein Diagramm des Prometheus-Ausdrucks über die Zeit zu sehen, klicken Sie auf **Anzeigen in Prometheus**.

Es wird ein Prometheus-Diagramm des in der Diagnose verwendeten Ausdrucks angezeigt.

Enable query history

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

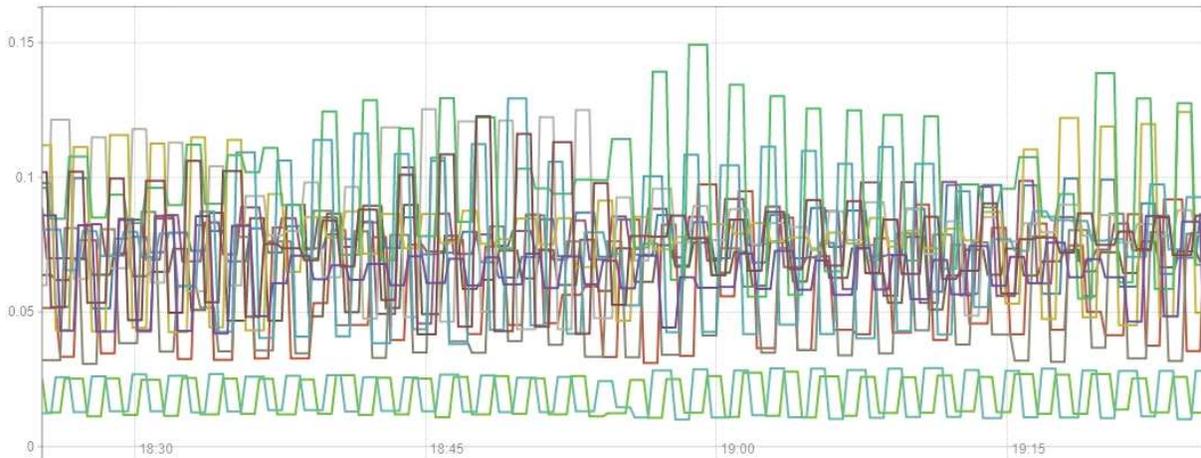
Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor -

Graph Console

1h + << Until >> Res. (s) stacked



- {instance="DC3-S3"}
- {instance="DC3-S2"}
- {instance="DC3-S1"}
- {instance="DC2-S3"}
- {instance="DC2-S2"}
- {instance="DC2-S1"}
- {instance="DC2-ADM1"}
- {instance="DC1-S3"}
- {instance="DC1-S2"}
- {instance="DC1-S1"}
- {instance="DC1-G1"}
- {instance="DC1-ARC1"}
- {instance="DC1-ADM1"}

Remove Graph

Add Graph

Erstellen benutzerdefinierter Überwachungsanwendungen

Mithilfe der StorageGRID-Kennzahlen der Grid-Management-API können Sie benutzerdefinierte Monitoring-Applikationen und Dashboards erstellen.

Wenn Sie Kennzahlen 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.

Über ein externes Monitoring-Tool wie Grafana können Sie auch direkt auf die Prometheus Metriken zugreifen. Zur Verwendung eines externen Tools müssen Sie ein Administrator-Clientzertifikat hochladen oder erstellen, damit StorageGRID das Tool für die Sicherheit authentifizieren kann. Siehe ["Anweisungen für die Administration von StorageGRID"](#).

Informationen zu den Kennzahlen-API-Vorgängen, einschließlich der vollständigen Liste der verfügbaren Metriken, finden Sie im Grid Manager. Wählen Sie oben auf der Seite das Hilfesymbol aus und wählen Sie **API-Dokumentation > metrics**.



GET	<code>/grid/metric-labels/{label}/values</code>	Lists the values for a metric label	
GET	<code>/grid/metric-names</code>	Lists all available metric names	
GET	<code>/grid/metric-query</code>	Performs an instant metric query at a single point in time	
GET	<code>/grid/metric-query-range</code>	Performs a metric query over a range of time	

Die Einzelheiten zur Implementierung einer benutzerdefinierten Überwachungsanwendung liegen über dem Umfang dieser Dokumentation hinaus.

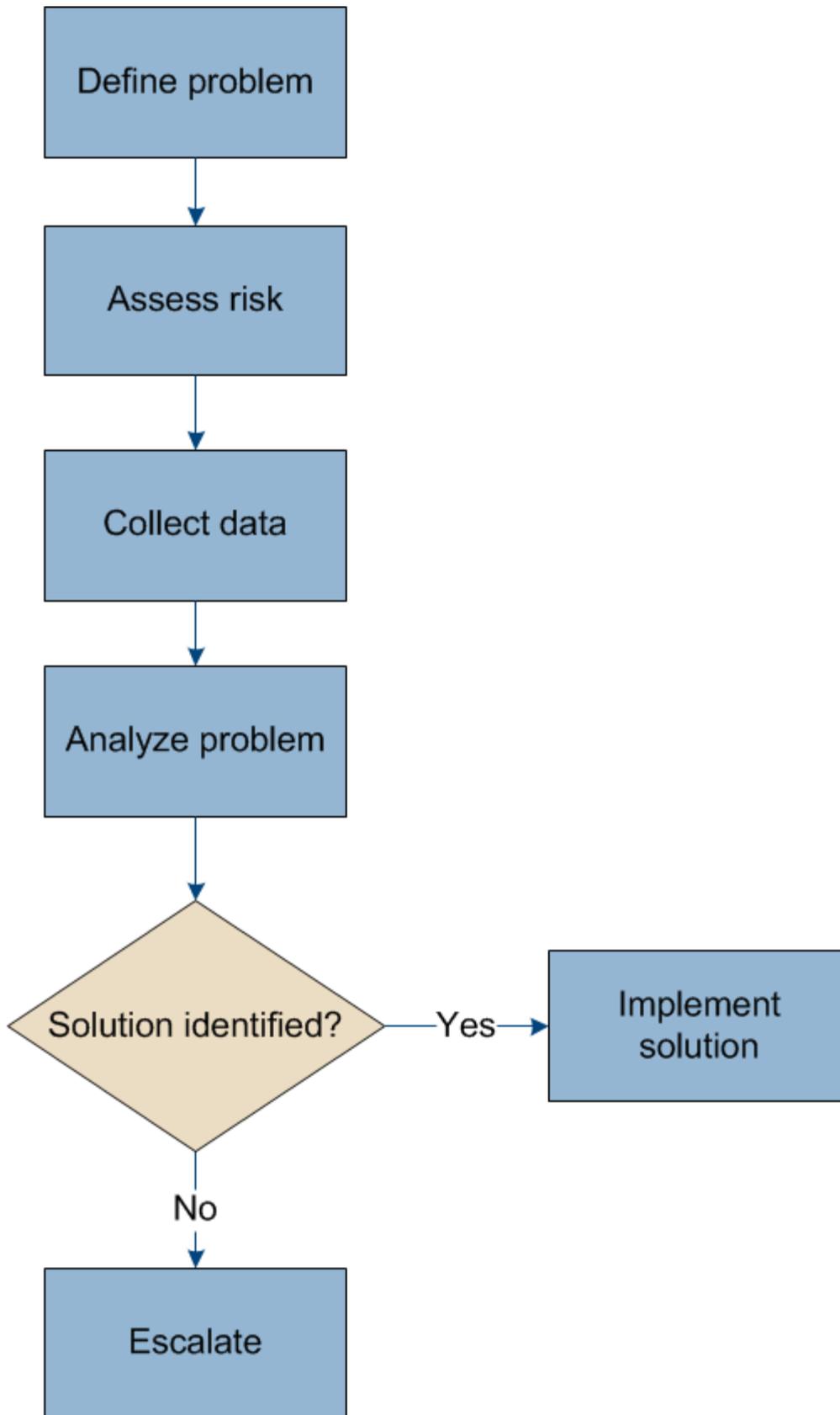
Fehlerbehebung für das StorageGRID-System

Fehlerbehebung bei einem StorageGRID-System: Übersicht

Wenn bei der Verwendung eines StorageGRID-Systems ein Problem auftritt, finden Sie in den Tipps und Richtlinien dieses Abschnitts Hilfe zum ermitteln und Beheben des Problems.

Überblick über die Problembestimmung

Wenn bei Ihnen ein Problem auftritt "[Verwalten eines StorageGRID-Systems](#)", Sie können den in dieser Abbildung beschriebenen Prozess verwenden, um das Problem zu identifizieren und zu analysieren. Häufig können Sie Probleme selbst lösen. Unter Umständen müssen Sie jedoch einige Probleme an den technischen Support eskalieren.



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 erfassen können, um ein Problem zu definieren:

Frage	Beispielantwort
Was macht das StorageGRID-System? Was sind die Symptome?	Client-Applikationen berichten, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann hat das Problem begonnen?	Die Objektaufnahme wurde am 8. Januar 2020 um 14:50 Uhr verweigert.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Durch Client-Anwendung benachrichtigt. Auch Benachrichtigung per E-Mail erhalten.
Tritt das Problem konsequent oder nur in manchen Fällen auf?	Das Problem ist noch nicht behoben.
Wenn das Problem regelmäßig auftritt, welche Schritte dazu führen, 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 Zeiten der einzelnen Vorfälle, die Sie kennen.	Das Problem ist nicht intermittierend.
Haben Sie dieses Problem schon einmal gesehen? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dies ist das erste Mal, dass ich dieses Thema gesehen habe.

Bewerten Sie das Risiko und die Auswirkungen auf das System

Bewerten Sie nach Definition des Problems sein Risiko und die Auswirkungen auf das StorageGRID System. Beispielsweise bedeutet das Vorhandensein kritischer Warnmeldungen nicht zwangsläufig, dass das System keine Kernservices liefert.

In dieser Tabelle sind die Auswirkungen eines Beispielproblems auf Systemvorgänge zusammengefasst:

Frage	Beispielantwort
Kann das StorageGRID System Inhalte aufnehmen?	Nein
Können Client-Anwendungen Inhalte abrufen?	Einige Objekte können abgerufen werden, andere nicht.
Sind Daten gefährdet?	Nein
Ist die Fähigkeit, Geschäfte zu führen, stark beeinträchtigt?	Ja, da Client-Applikationen keine Objekte im StorageGRID System speichern können und Daten nicht konsistent abgerufen werden können.

Datenerfassung

Nach dem Definition des Problems und der Bewertung der Risiken und Auswirkungen können Sie Daten zur Analyse sammeln. Die Art der Daten, die am nützlichsten zu erfassen sind, hängt von der Art des Problems ab.

Art der zu erfassenden Daten	Warum diesen Dat sammeln	Anweisungen
Zeitplan der neuesten Änderungen erstellen	Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	<ul style="list-style-type: none">• Erstellen Sie eine Zeitleiste der neuesten Änderungen
Prüfen von Warnungen und Alarmen	<p>Mithilfe von Warnfunktionen und Alarmen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme geben.</p> <p>Überprüfen Sie die Liste der aktuellen Warnungen und Alarme, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat.</p> <p>Prüfen Sie die in der Vergangenheit ausgelösten Warnmeldungen und Alarme, um zusätzliche Einblicke zu erhalten.</p>	<ul style="list-style-type: none">• "Anzeige aktueller und aufgelöster Warnmeldungen"• "Verwalten von Alarmen (Altsystem)"
Monitoring von Ereignissen	Ereignisse umfassen Systemfehler oder Fehlerereignisse für einen Node, einschließlich Fehler wie Netzwerkfehler. Überwachen Sie Ereignisse, um weitere Informationen zu Problemen zu erhalten oder um Hilfe bei der Fehlerbehebung zu erhalten.	<ul style="list-style-type: none">• "Monitoring von Ereignissen"
Identifizieren von Trends mithilfe von Diagrammen und Textberichten	Trends liefern wertvolle Hinweise darauf, wann Probleme zuerst auftraten, und können Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	<ul style="list-style-type: none">• "Verwenden Sie Diagramme und Diagramme"• "Verwenden Sie Textberichte"
Basispläne erstellen	Sammeln von Informationen über die normalen Stufen verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Grundlinien können wertvolle Hinweise liefern.	<ul style="list-style-type: none">• Basispläne erstellen
Durchführen von Einspeisung und Abruf von Tests	Zur Fehlerbehebung von Performance-Problemen bei Aufnahme und Abruf können Objekte auf einer Workstation gespeichert und abgerufen werden. Vergleichen Sie die Ergebnisse mit denen, die bei der Verwendung der Client-Anwendung angezeigt werden.	<ul style="list-style-type: none">• "PUT- und GET-Performance werden überwacht"

Art der zu erfassenden Daten	Warum diesen Dat sammeln	Anweisungen
Audit-Meldungen prüfen	Überprüfen Sie Audit-Meldungen, um StorageGRID Vorgänge im Detail zu befolgen. Die Details in Audit-Meldungen können bei der Behebung vieler Arten von Problemen, einschließlich von Performance-Problemen, nützlich sein.	<ul style="list-style-type: none"> • "Audit-Meldungen prüfen"
Überprüfen Sie Objektstandorte und Storage-Integrität	Wenn Sie Speicherprobleme haben, stellen Sie sicher, dass Objekte an der gewünschten Stelle platziert werden. Überprüfen Sie die Integrität von Objektdaten auf einem Storage-Node.	<ul style="list-style-type: none"> • "Überwachen von Objektverifizierungsvorgängen" • "Bestätigen Sie den Speicherort der Objektdaten" • "Überprüfen Sie die Objektintegrität"
Datenerfassung für technischen Support	Vom technischen Support werden Sie möglicherweise aufgefordert, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um Probleme zu beheben.	<ul style="list-style-type: none"> • "Erfassen von Protokolldateien und Systemdaten" • "Senden Sie manuell eine AutoSupport Meldung aus" • "Prüfen von Support-Kennzahlen"

Erstellen Sie eine Zeitleiste der neuesten 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.
- Durch eine Zeitleiste von Änderungen können Sie feststellen, welche Änderungen für ein Problem verantwortlich sein könnten und wie jede Änderung ihre Entwicklung beeinflusst haben könnte.

Erstellen Sie eine Tabelle mit den letzten Änderungen an Ihrem System, die Informationen darüber enthält, wann jede Änderung stattgefunden hat und welche relevanten Details über die Änderung angezeigt werden, und Informationen darüber, was während der Änderung noch passiert ist:

Zeit der Änderung	Art der Änderung	Details
Beispiel: <ul style="list-style-type: none"> • Wann haben Sie die Node-Wiederherstellung gestartet? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Prozess unterbrochen? 	Was ist los? Was haben Sie gemacht?	Dokumentieren Sie alle relevanten Details zu der Änderung. Beispiel: <ul style="list-style-type: none"> • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Änderungen bei Client-Workloads Achten Sie darauf, zu beachten, ob mehrere Änderungen gleichzeitig durchgeführt wurden. Wurde diese Änderung beispielsweise vorgenommen, während ein Upgrade durchgeführt wurde?

Beispiele für signifikante aktuelle Änderungen

Hier einige Beispiele für potenziell signifikante Änderungen:

- Wurde das StorageGRID System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde kürzlich ein Upgrade des Systems durchgeführt? Wurde ein Hotfix angewendet?
- Wurde irgendeine Hardware in letzter Zeit repariert oder geändert?
- Wurde die ILM-Richtlinie aktualisiert?
- Hat sich der Client-Workload geändert?
- Hat sich die Client-Applikation oder deren Verhalten geändert?
- Haben Sie den Lastausgleich geändert oder eine Hochverfügbarkeitsgruppe aus Admin-Nodes oder Gateway-Nodes hinzugefügt oder entfernt?
- Wurden Aufgaben gestartet, die ein sehr langer Zeitaufwand beanspruchen können? Beispiele:
 - Wiederherstellung eines fehlerhaften Speicherknotens
 - Ausmusterung von Storage-Nodes
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, beispielsweise beim Hinzufügen eines Mandanten oder bei der Änderung der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden Plattform-Services kürzlich aktiviert oder geändert?
- Wurde die Compliance in letzter Zeit aktiviert?
- Wurden Cloud-Storage-Pools hinzugefügt oder entfernt?
- Wurden Änderungen an der Storage-Komprimierung oder -Verschlüsselung vorgenommen?
- Wurden Änderungen an der Netzwerkinfrastruktur vorgenommen? Beispiel: VLANs, Router oder DNS.
- Wurden Änderungen an NTP-Quellen vorgenommen?
- Wurden Änderungen an den Grid-, Admin- oder Client-Netzwerkschnittstellen vorgenommen?
- Wurden Konfigurationsänderungen am Archiv-Node vorgenommen?
- Wurden weitere Änderungen am StorageGRID System bzw. an der zugehörigen Umgebung vorgenommen?

Basispläne erstellen

Sie können Basislinien für Ihr System einrichten, indem Sie die normalen Ebenen verschiedener Betriebswerte erfassen. In Zukunft können Sie aktuelle Werte mit diesen Basiswerten vergleichen, um ungewöhnliche Werte zu erkennen und zu beheben.

Eigenschaft	Wert	Wie zu erhalten
Durchschnittlicher Storage-Verbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	<p>Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher.</p> <p>Suchen Sie im Diagramm Speicher verwendet - Objektdaten einen Zeitraum, in dem die Linie ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Speicherplatz jeden Tag verbraucht wird</p> <p>Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.</p>
Durchschnittlicher Metadatenverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	<p>Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher.</p> <p>Suchen Sie im Diagramm „verwendete Speicher - Objektmetadaten“ einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Metadaten-Storage täglich belegt wird</p> <p>Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.</p>
Geschwindigkeit von S3/Swift Operationen	Vorgänge/Sekunde	<p>Wählen Sie im Dashboard von Grid Manager Performance > S3 Operations oder Performance > Swift Operations aus.</p> <p>Um die Aufnahme- und Abrufraten für einen bestimmten Standort oder Knoten anzuzeigen, wählen Sie NODES > Site oder Storage Node > Objects aus. Positionieren Sie den Cursor auf dem Diagramm „Aufnahme und Abruf“ für S3 oder Swift.</p>
S3/Swift-Vorgänge sind fehlgeschlagen	Betrieb	<p>Wählen Sie SUPPORT > Tools > Grid-Topologie aus. Zeigen Sie auf der Registerkarte Übersicht im Abschnitt API-Vorgänge den Wert für S3-Operationen an – Fehlgeschlagen oder Swift-Vorgänge – Fehlgeschlagen.</p>

Eigenschaft	Wert	Wie zu erhalten
ILM-Auswertungsrage	Objekte/Sekunde	Wählen Sie auf der Seite Knoten GRID > ILM aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basislinienwert für Bewertungsrate für Ihr System zu schätzen.
ILM-Scan-Rate	Objekte/Sekunde	Wählen Sie NODES > Grid > ILM aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basislinienwert für Scan-Rate für Ihr System abzuschätzen.
Objekte, die sich aus Client-Vorgängen in Warteschlange befinden	Objekte/Sekunde	Wählen Sie NODES > Grid > ILM aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basislinienwert für Objekte in der Warteschlange (von Client-Operationen) für Ihr System abzuschätzen.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie NODES > Storage Node > Objekte aus. Zeigen Sie in der Tabelle Abfragen den Wert für durchschnittliche Latenz an.

Analysieren von Daten

Verwenden Sie die gesammelten Informationen, um die Ursache des Problems und der potenziellen Lösungen zu ermitteln.

Die Analyse ist Problem-abhängig, aber im Allgemeinen:

- Erkennen von Fehlerpunkten und Engpässen mithilfe der Alarme.
- Rekonstruieren Sie den Problemverlauf mithilfe der Alarmhistorie und -Diagramme.
- Verwenden Sie Diagramme, um Anomalien zu finden und die Problemsituation mit dem normalen Betrieb zu vergleichen.

Checkliste für Eskalationsinformationen

Wenn Sie das Problem nicht alleine lösen können, wenden Sie sich an den technischen Support. Bevor Sie sich an den technischen Support wenden, müssen Sie die in der folgenden Tabelle aufgeführten Informationen zur Erleichterung der Problembeseitigung nutzen.

✓	Element	Hinweise
	Problemstellung	<p>Was sind die Problemsymptome? Wann hat das Problem begonnen? Passiert es konsequent oder intermittierend? Welche Zeiten hat es gelegentlich gegeben?</p> <p>Definieren Sie das Problem</p>
	Folgenabschätzung	<p>Wo liegt der Schweregrad des Problems? Welche Auswirkungen hat dies auf die Client-Applikation?</p> <ul style="list-style-type: none"> • Ist der Client bereits erfolgreich verbunden? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	<p>Wählen Sie WARTUNG > System > Lizenz. Die StorageGRID System-ID wird im Rahmen der aktuellen Lizenz angezeigt.</p>
	Softwareversion	<p>Wählen Sie oben im Grid Manager das Hilfesymbol aus, und wählen Sie über, um die StorageGRID-Version anzuzeigen.</p>
	Anpassbarkeit	<p>Fassen Sie zusammen, wie Ihr StorageGRID System konfiguriert ist. Nehmen Sie z. B. Folgendes auf:</p> <ul style="list-style-type: none"> • Verwendet das Grid Storage-Komprimierung, Storage-Verschlüsselung oder Compliance? • Erstellt ILM replizierte oder Erasure Coding Objekte? Stellt ILM Standortredundanz sicher? Nutzen ILM-Regeln das ausgewogene, strikte oder duale Commit-Aufnahmeverhalten?
	Log-Dateien und Systemdaten	<p>Erfassen von Protokolldateien und Systemdaten für Ihr System Wählen Sie SUPPORT > Extras > Protokolle.</p> <p>Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes sammeln.</p> <p>Wenn Sie Protokolle nur für ausgewählte Knoten erfassen, müssen Sie mindestens einen Speicherknoten mit dem ADC-Service einschließen. (Die ersten drei Storage-Nodes an einem Standort enthalten den ADC-Service.)</p> <p>"Erfassen von Protokolldateien und Systemdaten"</p>
	Basisinformationen	<p>Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch</p> <p>Basispläne erstellen</p>

✓	Element	Hinweise
	Zeitachse der letzten Änderungen	Erstellen Sie eine Zeitleiste, in der alle letzten Änderungen am System oder seiner Umgebung zusammengefasst sind. Erstellen Sie eine Zeitleiste der neuesten Änderungen
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie Schritte zur Diagnose oder Behebung des Problems selbst ergriffen haben, achten Sie darauf, die Schritte und das Ergebnis zu notieren.

Behebung von Objekt- und Storage-Problemen

Bestätigen Sie den Speicherort der Objektdaten

Je nach dem Problem sollten Sie dies möglicherweise tun "[Bestätigen Sie, wo Objektdaten gespeichert werden](#)". Beispielsweise möchten Sie überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und Objektdaten dort gespeichert werden, wo sie geplant sind.

Bevor Sie beginnen

- Sie müssen über eine Objektkennung verfügen, die einer der folgenden sein kann:
 - **UUID:** Der Universally Unique Identifier des Objekts. Geben Sie die UUID in allen Großbuchstaben ein.
 - **CBID:** Die eindeutige Kennung des Objekts in StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in allen Großbuchstaben ein.
 - **S3-Bucket und Objektschlüssel:** Wenn ein Objekt durch das aufgenommen wird "[S3 Schnittstelle](#)", Die Client-Anwendung verwendet eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
 - **Swift-Container und Objektname:** Wenn ein Objekt durch das aufgenommen wird "[Swift-Schnittstelle](#)", Die Client-Anwendung verwendet eine Kombination aus Container und Objektname, um das Objekt zu speichern und zu identifizieren.

Schritte

1. Wählen Sie **ILM > Object Metadata Lookup**.
2. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

Sie können eine UUID, CBID, S3 Bucket/Objektschlüssel oder Swift Container/Objektname eingeben.

3. Wenn Sie eine bestimmte Version des Objekts suchen möchten, geben Sie die Version-ID ein (optional).

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

Version ID (optional)

4. Wählen Sie **Look Up**.

Der "[Ergebnisse der Suche nach Objektmetadaten](#)" Angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

- Systemmetadaten, einschließlich Objekt-ID (UUID), Version-ID (optional), Objektname, Name des Containers, Mandantenkontoname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

Fehler beim Objektspeicher (Storage Volume)

Der zugrunde liegende Storage auf einem Storage-Node ist in Objektspeicher unterteilt. Objektspeicher werden auch als Storage Volumes bezeichnet.

Sie können die 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

Um mehr zu sehen "[Details zu jedem Storage-Node](#)", Folgen Sie folgenden Schritten:

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **site > Storage Node > LDR > Storage > Übersicht > Haupt**.



Overview: LDR (DC1-S1) - Storage

Updated: 2020-01-29 15:03:39 PST

Storage State - Desired:	Online	
Storage State - Current:	Online	
Storage Status:	No Errors	

Utilization

Total Space:	322 GB	
Total Usable Space:	311 GB	
Total Usable Space (Percent):	96.534 %	
Total Data:	994 KB	
Total Data (Percent):	0 %	

Replication

Block Reads:	0	
Block Writes:	0	
Objects Retrieved:	0	
Objects Committed:	0	
Objects Deleted:	0	
Delete Service State:	Enabled	

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health	
0000	107 GB	96.4 GB	994 KB	0 B	0.001 %	No Errors	
0001	107 GB	107 GB	0 B	0 B	0 %	No Errors	
0002	107 GB	107 GB	0 B	0 B	0 %	No Errors	

Je nach Art des Ausfalls können Fehler bei einem Storage-Volume in einem Alarm über den Storage-Status oder den Zustand eines Objektspeicher gespiegelt werden. Wenn ein Speichervolume ausfällt, sollten Sie das ausgefallene Speichervolume reparieren, um den Speicherknoten so bald wie möglich wieder voll zu machen. Bei Bedarf können Sie auf die Registerkarte **Konfiguration** und gehen "[Setzen Sie den Speicher-Node in einen schreibgeschützten Status](#)-" Damit das StorageGRID-System es für den Datenabruf nutzen kann, während Sie sich auf ein vollständiges Recovery des Servers vorbereiten.

Überprüfen Sie die Objektintegrität

Das StorageGRID System überprüft die Integrität der Objektdaten auf Storage-Nodes und überprüft sowohl beschädigte als auch fehlende Objekte.

Es gibt zwei Verifizierungsverfahren: Hintergrundüberprüfung und Objektexistenz-Prüfung (früher als Vordergrundüberprüfung bezeichnet). Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung wird automatisch ausgeführt und überprüft kontinuierlich die Korrektheit von Objektdaten. Die Überprüfung der ObjektExistenz kann von einem Benutzer ausgelöst werden, um die Existenz (obwohl nicht die Richtigkeit) von Objekten schneller zu überprüfen.

Was ist Hintergrundüberprüfung?

Die Hintergrundüberprüfung überprüft Storage Nodes automatisch und kontinuierlich auf beschädigte Kopien

von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

Bei der Hintergrundüberprüfung werden die Integrität replizierter Objekte und Objekte mit Erasure-Coding-Verfahren überprüft:

- **Replizierte Objekte:** Findet der Hintergrundverifizierungsvorgang ein beschädigtes Objekt, wird die beschädigte Kopie vom Speicherort entfernt und an anderer Stelle auf dem Speicherknoten isoliert. Anschließend wird eine neue, nicht beschädigte Kopie erstellt und gemäß der aktiven ILM-Richtlinie platziert. Die neue Kopie wird möglicherweise nicht auf dem Speicherknoten abgelegt, der für die ursprüngliche Kopie verwendet wurde.



Beschädigte Objektdaten werden nicht aus dem System gelöscht, sondern in Quarantäne verschoben, sodass weiterhin darauf zugegriffen werden kann. Weitere Informationen zum Zugriff auf gesperrte Objektdaten erhalten Sie vom technischen Support.

- **Erasure-codierte Objekte:** Erkennt der Hintergrund-Verifizierungsprozess, dass ein Fragment eines Löschungscodierten Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Daten- und Paritätsfragmente neu zu erstellen. Wenn das beschädigte Fragment nicht neu erstellt werden kann, wird versucht, eine weitere Kopie des Objekts abzurufen. Wenn der Abruf erfolgreich ist, wird eine ILM-Bewertung durchgeführt, um eine Ersatzkopie des Objekts, das mit der Fehlerkorrektur codiert wurde, zu erstellen.

Bei der Hintergrundüberprüfung werden nur Objekte auf Speicherknoten überprüft. Es überprüft keine Objekte auf Archiv-Nodes oder in einem Cloud-Speicherpool. Objekte müssen älter als vier Tage sein, um sich für die Hintergrundüberprüfung zu qualifizieren.

Die Hintergrundüberprüfung läuft mit einer kontinuierlichen Geschwindigkeit, die nicht auf normale Systemaktivitäten ausgerichtet ist. Die Hintergrundüberprüfung kann nicht angehalten werden. Sie können jedoch die Hintergrundverifizierungsrate erhöhen, um falls Sie vermuten, dass ein Problem vorliegt, den Inhalt eines Storage-Nodes schneller zu überprüfen.

Warnmeldungen und Alarme (alt) im Zusammenhang mit der Hintergrundüberprüfung

Wenn das System ein beschädigtes Objekt erkennt, das nicht automatisch korrigiert werden kann (weil die Beschädigung verhindert, dass das Objekt identifiziert wird), wird die Warnmeldung **Unidentified Corrupt Object Detected** ausgelöst.

Wenn eine Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, weil es keine weitere Kopie finden kann, wird die Warnmeldung **Objects lost** ausgelöst.

Ändern Sie die Hintergrundverifizierungsrate

Sie können die Rate ändern, mit der die Hintergrundüberprüfung replizierte Objektdaten auf einem Storage-Node überprüft, wenn Sie Bedenken hinsichtlich der Datenintegrität haben.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Sie können die Verifizierungsrate für die Hintergrundüberprüfung eines Speicherknoten ändern:

- Adaptiv: Standardeinstellung. Die Aufgabe wurde entwickelt, um maximal 4 MB/s oder 10 Objekte/s zu

überprüfen (je nachdem, welcher Wert zuerst überschritten wird).

- Hoch: Die Storage-Verifizierung verläuft schnell und kann zu einer Geschwindigkeit führen, die normale Systemaktivitäten verlangsamen kann.

Verwenden Sie die hohe Überprüfungsrate nur, wenn Sie vermuten, dass ein Hardware- oder Softwarefehler beschädigte Objektdaten aufweisen könnte. Nach Abschluss der Hintergrundüberprüfung mit hoher Priorität wird die Verifizierungsrate automatisch auf Adaptive zurückgesetzt.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Storage Node > LDR > Verifizierung** aus.
3. Wählen Sie **Konfiguration > Main**.
4. Gehen Sie zu **LDR > Verifizierung > Konfiguration > Main**.
5. Wählen Sie unter Hintergrundüberprüfung die Option **Verifizierungsrate > hoch** oder **Verifizierungsrate > adaptiv** aus.

Overview Alarms Reports Configuration

Main

Configuration: LDR (Storage Node) - Verification
Updated: 2021-11-11 07:13:00 MST

Reset Missing Objects Count

Background Verification

Verification Rate Adaptive

Reset Corrupt Objects Count

Quarantined Objects

Delete Quarantined Objects

Apply Changes



Wenn Sie die Verifizierungsrate auf hoch setzen, wird der alte Alarm VPRI (Verification Rate) auf der Melderebene ausgelöst.

6. Klicken Sie Auf **Änderungen Übernehmen**.
7. Überwachen der Ergebnisse der Hintergrundüberprüfung replizierter Objekte
 - a. Wechseln Sie zu **NODES > Storage Node > Objects**.
 - b. Überwachen Sie im Abschnitt Überprüfung die Werte für **beschädigte Objekte** und **beschädigte Objekte nicht identifiziert**.

Wenn bei der Hintergrundüberprüfung beschädigte replizierte Objektdaten gefunden werden, wird die Metrik **beschädigte Objekte** erhöht und StorageGRID versucht, die Objektkennung aus den Daten zu extrahieren, wie folgt:

- Wenn die Objekt-ID extrahiert werden kann, erstellt StorageGRID automatisch eine neue Kopie der Objektdaten. Die neue Kopie kann an jedem beliebigen Ort im StorageGRID System erstellt werden, der die aktive ILM-Richtlinie erfüllt.
 - Wenn der Objektbezeichner nicht extrahiert werden kann (weil er beschädigt wurde), wird die Metrik **korrupte Objekte nicht identifiziert** erhöht und die Warnung **nicht identifiziertes beschädigtes Objekt erkannt** ausgelöst.
- c. Wenn beschädigte replizierte Objektdaten gefunden werden, wenden Sie sich an den technischen Support, um die Ursache der Beschädigung zu ermitteln.
8. Überwachen Sie die Ergebnisse der Hintergrundüberprüfung von Objekten, die mit Erasure Coding codiert wurden.

Wenn bei der Hintergrundüberprüfung beschädigte Fragmente von Objektdaten gefunden werden, die mit dem Erasure-Coding-Verfahren codiert wurden, wird das Attribut „beschädigte Fragmente erkannt“ erhöht. StorageGRID stellt sich wieder her, indem das beschädigte Fragment auf demselben Speicherknoten wiederhergestellt wird.

- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Storage Node > LDR > Erasure Coding** aus.
 - c. Überwachen Sie in der Tabelle „Ergebnisse der Überprüfung“ das Attribut „beschädigte Fragmente erkannt“ (ECCD).
9. Nachdem das StorageGRID System beschädigte Objekte automatisch wiederhergestellt hat, setzen Sie die Anzahl beschädigter Objekte zurück.
- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Storage Node > LDR > Verifizierung > Konfiguration**.
 - c. Wählen Sie **Anzahl Der Beschädigten Objekte Zurücksetzen**.
 - d. Klicken Sie Auf **Änderungen Übernehmen**.
10. Wenn Sie sicher sind, dass isolierte Objekte nicht erforderlich sind, können Sie sie löschen.



Wenn der Alarm **Objects lost** oder der Legacy-Alarm LOST (Lost Objects) ausgelöst wurde, möchte der technische Support möglicherweise auf isolierte Objekte zugreifen, um das zugrunde liegende Problem zu beheben oder eine Datenwiederherstellung zu versuchen.

- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- b. Wählen Sie **Storage Node > LDR > Verifizierung > Konfiguration**.
- c. Wählen Sie **Gesperrte Objekte Löschen**.
- d. Wählen Sie **Änderungen Anwenden**.

Was ist Objektexistenz-Prüfung?

Die ObjektExistenz überprüft, ob alle erwarteten replizierten Kopien von Objekten und mit Erasure Coding verschlüsselten Fragmenten auf einem Storage Node vorhanden sind. Die Objektüberprüfung überprüft nicht die Objektdaten selbst (Hintergrundüberprüfung führt das durch); stattdessen bietet sie eine Möglichkeit, die Integrität von Speichergeräten zu überprüfen, insbesondere wenn ein kürzlich auftretende Hardwareproblem die Datenintegrität beeinträchtigen könnte.

Im Gegensatz zur automatischen Hintergrundüberprüfung müssen Sie einen Auftrag zur Überprüfung der Objektexistenz manuell starten.

Die Objektexistenz prüft die Metadaten für jedes in StorageGRID gespeicherte Objekt und überprüft, ob es sich um replizierte Objektkopien sowie um Erasure Coding verschlüsselte Objektfragmente handelt. Fehlende Daten werden wie folgt behandelt:

- **Replizierte Kopien:** Fehlt eine Kopie replizierter Objektdaten, versucht StorageGRID automatisch, die Kopie von einer an anderer Stelle im System gespeicherten Kopie zu ersetzen. Der Storage-Node führt eine vorhandene Kopie durch eine ILM-Evaluierung aus. Damit wird festgestellt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da eine weitere Kopie fehlt. Eine neue Kopie wird erstellt und platziert, um die aktive ILM-Richtlinie des Systems zu erfüllen. Diese neue Kopie kann nicht an derselben Stelle platziert werden, an der die fehlende Kopie gespeichert wurde.
- **Erasure-codierte Fragmente:** Fehlt ein Fragment eines Objekts mit Lösungscode, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten mithilfe der verbleibenden Fragmente neu zu erstellen. Wenn das fehlende Fragment nicht neu aufgebaut werden kann (weil zu viele Fragmente verloren gegangen sind), versucht ILM, eine andere Kopie des Objekts zu finden, mit der es ein neues, lösercodiertes Fragment generieren kann.

Überprüfung der ObjektExistenz ausführen

Sie erstellen und führen jeweils einen Job für die Überprüfung der Objektexistenz aus. Wenn Sie einen Job erstellen, wählen Sie die Speicherknoten und -Volumes aus, die Sie überprüfen möchten. Sie wählen auch das Consistency Control für den Job aus.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben sichergestellt, dass die zu prüfenden Speicherknoten online sind. Wählen Sie **NODES**, um die Tabelle der Knoten anzuzeigen. Stellen Sie sicher, dass neben dem Knotennamen für die Knoten, die Sie überprüfen möchten, keine Warnsymbole angezeigt werden.
- Sie haben sichergestellt, dass die folgenden Verfahren auf den Knoten, die Sie überprüfen möchten, **nicht** ausgeführt werden:
 - Grid-Erweiterung, um einen Storage-Node hinzuzufügen
 - Deaktivierung des Storage Node
 - Recovery eines ausgefallenen Storage-Volumes
 - Wiederherstellung eines Speicherknoten mit einem ausgefallenen Systemlaufwerk
 - EC-Ausgleich
 - Appliance-Node-Klon

Die Objektprüfung bietet keine nützlichen Informationen, während diese Verfahren ausgeführt werden.

Über diese Aufgabe

Die Fertigstellung eines Objektes kann je nach Anzahl der Objekte im Raster, der ausgewählten Storage-Nodes und Volumes und der ausgewählten Konsistenzgruppe Tage oder Wochen dauern. Sie können nur einen Job gleichzeitig ausführen, aber Sie können mehrere Speicherknoten und Volumes gleichzeitig auswählen.

Schritte

1. Wählen Sie **WARTUNG > Aufgaben > Objekt Existenzprüfung**.
2. Wählen Sie **Job erstellen**. Der Assistent Job-Prüfung für Objektexistenz erstellen wird angezeigt.

3. Wählen Sie die Nodes 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 Node-Namen 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 mithilfe der Storage-Volume-Nummer oder des Node-Namens 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 das Consistency Control für den Job aus.

Die Konsistenzkontrolle bestimmt, wie viele Kopien von Objektmetadaten für die Objektüberprüfung verwendet werden.

- **Strong-site**: Zwei Kopien von Metadaten an einem einzigen Standort.
- **Stark-global**: Zwei Kopien von Metadaten an jedem Standort.
- **Alle** (Standard): Alle drei Kopien von Metadaten an jedem Standort.

Weitere Informationen zur Consistency Control finden Sie in den Beschreibungen im Assistenten.

8. Wählen Sie **Weiter**.

9. Ihre Auswahl überprüfen und überprüfen. Sie können **Zurück** auswählen, um zu einem vorherigen Schritt im Assistenten zu wechseln, um Ihre Auswahl zu aktualisieren.

Ein Job zur Überprüfung der Objektexistenz wird erstellt und wird ausgeführt, bis einer der folgenden Aktionen ausgeführt wird:

- Der Job ist abgeschlossen.
- Sie unterbrechen oder abbrechen den Job. Sie können einen angehaltenen Job fortsetzen, aber einen abgebrochenen Job nicht wieder aufnehmen.
- Der Job wird abgestellt. Die Warnung * Objektexistenz ist blockiert* wird ausgelöst. Befolgen Sie die für die Meldung angegebenen Korrekturmaßnahmen.
- Der Job schlägt fehl. Die Warnung * Objektexistenz ist fehlgeschlagen* wird ausgelöst. Befolgen Sie die für die Meldung angegebenen Korrekturmaßnahmen.
- Es wird eine Meldung „Service nicht verfügbar“ oder „interner Serverfehler“ angezeigt. Aktualisieren Sie nach einer Minute die Seite, um mit der Überwachung des Jobs fortzufahren.



Sie können bei Bedarf von der Seite „Objektexistenz“ wegnavigieren und mit der Überwachung des Jobs fortfahren.

10. Zeigen Sie während der Ausführung des Jobs die Registerkarte **aktiver Job** an, und notieren Sie den Wert fehlender Objektkopien.

Dieser Wert stellt die Gesamtzahl der fehlenden Kopien replizierter Objekte und Objekte mit Erasure-

Coding-Code mit einem oder mehreren fehlenden Fragmenten dar.

Wenn die Anzahl der erkannten fehlenden Objektkopien größer als 100 ist, kann es zu einem Problem mit dem Speicher des Speicherknotens kommen.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job Job history

Status: **Accepted** Consistency control: **All**

Job ID: 2334602652907829302 Start time: 2021-11-10 14:43:02 MST

Missing object copies detected: **0** Elapsed time: —

Progress:  0% Estimated time to completion: —

Pause Cancel

Volumes Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Nehmen Sie nach Abschluss des Jobs alle weiteren erforderlichen Maßnahmen vor:

- Wenn fehlende Objektkopien gefunden wurden, ist Null, dann wurden keine Probleme gefunden. Es ist keine Aktion erforderlich.
- Wenn fehlende Objektkopien erkannt sind größer als Null und die Warnung **Objekte verloren** nicht ausgelöst wurde, wurden alle fehlenden Kopien vom System repariert. Überprüfen Sie, ob Hardwareprobleme behoben wurden, um zukünftige Schäden an Objektkopien zu vermeiden.
- Wenn fehlende Objektkopien erkannt sind größer als Null und die Warnung **Objekte verloren** ausgelöst wurde, könnte die Datenintegrität beeinträchtigt werden. Wenden Sie sich an den technischen Support.
- Sie können verlorene Objektkopien untersuchen, indem Sie die LLST-Audit-Meldungen mit grep extrahieren: `grep LLST audit_file_name`.

Dieses Verfahren ähnelt dem Verfahren für "[Untersuchung verlorener Objekte](#)", Obwohl für Objektkopien Sie suchen LLST Statt OLST.

12. Wenn Sie für den Job die Kontrolle der Konsistenz vor Ort oder stark-global ausgewählt haben, warten Sie ungefähr drei Wochen auf die Metadatenkonsistenz, und führen Sie den Job erneut auf denselben Volumes aus.

Wenn StorageGRID Zeit hatte, konsistente Metadaten für die im Job enthaltenen Nodes und Volumes zu erzielen, konnte eine erneute Ausführung des Jobs fälschlicherweise gemeldete fehlende Objektkopien löschen oder zusätzliche Objektkopien veranlassen, dass sie nicht verwendet wurden.

- a. Wählen Sie **WARTUNG > Objekt Existenzprüfung > Jobverlauf**.
- b. Legen Sie fest, welche Jobs für die erneute Ausführung bereit sind:
 - i. Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.
 - ii. Überprüfen Sie für diese Jobs die Spalte Consistency Control auf Strong-site oder strong-global.
- c. Aktivieren Sie das Kontrollkästchen für jeden Job, den Sie erneut ausführen möchten, und wählen Sie dann **erneut ausführen**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job | Job history

Delete | **Rerun** | Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

<input type="checkbox"/>	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
<input checked="" type="checkbox"/>	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
<input type="checkbox"/>	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. Überprüfen Sie im Assistenten für Rerun-Jobs die ausgewählten Knoten und Volumes und die Konsistenzsteuerung.
- e. Wenn Sie bereit sind, die Jobs erneut auszuführen, wählen Sie **Rerun**.

Die Registerkarte „aktiver Job“ wird angezeigt. Alle ausgewählten Jobs werden als ein Job bei einer Consistency Control von strong-site erneut ausgeführt. In einem Feld mit * Related Jobs* im Bereich Details werden die Job-IDs für die ursprünglichen Jobs angezeigt.

Nachdem Sie fertig sind

Wenn Sie noch Bedenken bezüglich der Datenintegrität haben, gehen Sie zu **SUPPORT > Tools > Grid-Topologie > Site > Storage-Node > LDR > Verifizierung > Konfiguration > Main** und erhöhen Sie die Hintergrundverifizierungsrate. Die Hintergrundüberprüfung überprüft die Richtigkeit aller gespeicherten Objektdaten und repariert sämtliche gefundenen Probleme. Das schnelle Auffinden und Reparieren potenzieller Probleme verringert das Risiko von Datenverlusten.

Fehlerbehebung bei S3 PUT Objektgröße zu groß Warnung

Die Warnmeldung S3 PUT Objektgröße zu groß wird ausgelöst, wenn ein Mandant einen nicht mehrteiligen PUT-Objekt-Vorgang versucht, der das S3-Größenlimit von 5 gib überschreitet.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".

Legen Sie fest, welche Mandanten Objekte verwenden, die größer als 5 gib sind, damit Sie sie benachrichtigen können.

Schritte

1. Gehen Sie zu **CONFIGURATION > Monitoring > Audit und Syslog-Server**.
2. Wenn die Schreibvorgänge des Clients normal sind, greifen Sie auf das Revisionsprotokoll zu:
 - a. Eingabe `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

- e. Eingabe `cd /var/local/audit/export`
- f. Ermitteln Sie, welche Mandanten Objekte mit einer Größe von mehr als 5 gib verwenden.
 - i. Eingabe `zgrep SPUT * | egrep "CSIZ\(UI64\) : [0-9]*[5-9][0-9]{9}"`
 - ii. Sehen Sie sich für jede Audit-Meldung in den Ergebnissen an `S3AI` Feld, um die Konto-ID des Mandanten zu bestimmen. Verwenden Sie die anderen Felder in der Meldung, um zu bestimmen, welche IP-Adresse vom Client, vom Bucket und vom Objekt verwendet wurde:

Codieren	Beschreibung
SAIP	Quell-IP
S3AI	Mandanten-ID
S3BK	Eimer
S3KY	Objekt
CSIZ	Größe (Byte)

Beispiel für Ergebnisse des Audit-Protokolls

```
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):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"060X85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][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 die Schreibvorgänge des Clients nicht normal sind, verwenden Sie die Mandanten-ID in der Warnmeldung, um den Mandanten zu identifizieren:

- a. Gehen Sie zu **SUPPORT > Tools > Logs**. Sammeln Sie Anwendungsprotokolle für den Speicher-Node in der Warnmeldung. Geben Sie 15 Minuten vor und nach der Warnmeldung 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. Durchsuchen Sie das Protokoll nach `method=PUT` Und identifizieren Sie den Client im `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 Mandanten, dass die maximale PUT-Objektgröße 5 gib beträgt, und verwenden Sie mehrteilige Uploads für Objekte, die mehr als 5 gib betragen.
5. Ignorieren Sie die Warnmeldung für eine Woche, wenn die Anwendung geändert wurde.

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Fehlerbehebung bei verlorenen und fehlenden Objektdaten: Übersicht

Objekte können aus verschiedenen Gründen abgerufen werden, darunter Leseanforderungen von einer Client-Applikation, Hintergrundverifizierungen replizierter Objektdaten, ILM-Neubewertungen und die Wiederherstellung von Objektdaten während der Recovery eines Storage Node.

Das StorageGRID System verwendet Positionsinformationen in den Metadaten eines Objekts, um von welchem Speicherort das Objekt abzurufen. Wenn eine Kopie des Objekts nicht am erwarteten Speicherort gefunden wird, versucht das System, eine andere Kopie des Objekts von einer anderen Stelle im System

abzurufen, vorausgesetzt, die ILM-Richtlinie enthält eine Regel zum Erstellen von zwei oder mehr Kopien des Objekts.

Wenn der Abruf erfolgreich ist, ersetzt das StorageGRID System die fehlende Kopie des Objekts. Andernfalls wird wie folgt die Warnung **Objekte verloren** ausgelöst:

- Wenn bei replizierten Kopien keine weitere Kopie abgerufen werden kann, gilt das Objekt als verloren, und die Warnmeldung wird ausgelöst.
- Wenn eine Kopie nicht vom erwarteten Speicherort abgerufen werden kann, wird das Attribut Corrupt Copies Detected (ECOR) für Kopien, die nach dem Löschen codiert wurden, um eins erhöht, bevor versucht wird, eine Kopie von einem anderen Speicherort abzurufen. Falls keine weitere Kopie gefunden wird, wird die Meldung ausgelöst.

Sie sollten alle **Objekte Lost**-Warnungen sofort untersuchen, um die Ursache des Verlusts zu ermitteln und zu ermitteln, ob das Objekt noch in einem Offline-oder anderweitig derzeit nicht verfügbar ist, Storage Node oder Archive Node. Siehe "[Untersuchen Sie verlorene Objekte](#)".

Wenn Objekt-Daten ohne Kopien verloren gehen, gibt es keine Recovery-Lösung. Sie müssen jedoch den Zähler „Lost Objects“ zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren. Siehe "[Verlorene und fehlende Objektanzahl zurücksetzen](#)".

Untersuchen Sie verlorene Objekte

Wenn der Alarm **Objekte verloren** ausgelöst wird, müssen Sie sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

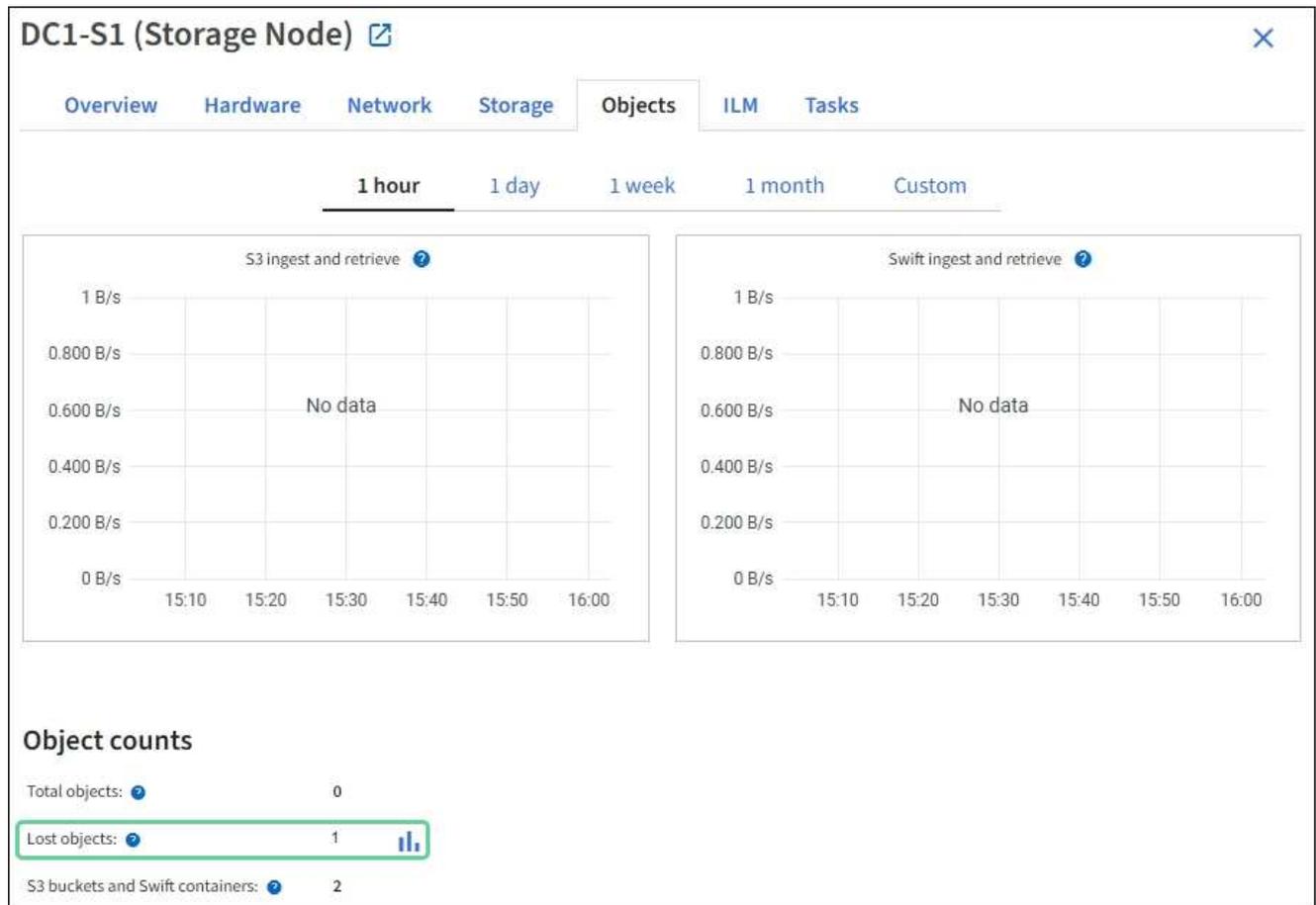
Die Warnung **Objects lost** zeigt an, dass StorageGRID glaubt, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

Untersuchen Sie verlorene Objektwarnungen sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. In einigen Fällen können Sie ein verlorenes Objekt wiederherstellen, wenn Sie eine sofortige Aktion ausführen.

Schritte

1. Wählen Sie **KNOTEN**.
2. Wählen Sie **Speicherknoten > Objekte** Aus.
3. Überprüfen Sie die Anzahl der verlorenen Objekte, die in der Tabelle Objektanzahl angezeigt werden.

Diese Nummer gibt die Gesamtzahl der Objekte an, die dieser Grid-Node im gesamten StorageGRID-System als fehlend erkennt. Der Wert ist die Summe der Zähler Lost Objects der Data Store Komponente innerhalb der LDR- und DDS-Dienste.



4. Von einem Admin-Node, "Rufen Sie das Überwachungsprotokoll auf" So bestimmen Sie die eindeutige Kennung (UUID) des Objekts, das die Warnmeldung **Objects lost** ausgelöst hat:
 - a. Melden Sie sich beim Grid-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
 - b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden. Geben Sie Ein: `cd /var/local/audit/export/`
 - c. Verwenden Sie `grep`, um die Audit-Meldungen zu „Objekt verloren“ (OLST) zu extrahieren. Geben Sie Ein: `grep OLST audit_file_name`
 - d. Beachten Sie den in der Meldung enthaltenen UUID-Wert.

```

>Admin: # grep OLSM 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):OLSM][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]

```

5. Verwenden Sie die `ObjectByUUID` Befehl zum Suchen des Objekts anhand seiner ID (UUID) und bestimmen Sie, ob die Daten gefährdet sind.

a. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole.

b. Geben Sie Ein: `/proc/OBRP/ObjectByUUID UUID_value`

In diesem ersten Beispiel, das Objekt mit UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 Hat zwei Standorte aufgelistet.

```

ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",

```

```

        "ITME": "1581534970983000"
    },
    "CMSM": {
        "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
        "LOCC": "us-east-1"
    }
},
"CLCO\ (Locations\)": \[
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID\)": "12448208",
        "VOLI\ (Volume ID\)": "3222345473",
        "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
        "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.880569"
    },
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID\)": "12288733",
        "VOLI\ (Volume ID\)": "3222345984",
        "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
        "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.934425"
    }
]
}

```

Im zweiten Beispiel das Objekt mit UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 Hat keine Standorte aufgelistet.

```

ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
      "ITME": "1581534970983000"
    },
    "CMSM": {
      "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
      "LOCC": "us-east-1"
    }
  }
}

```

- a. Überprüfen Sie die Ausgabe von `/proc/OBRP/ObjectByUUID`, und ergreifen Sie die entsprechenden Maßnahmen:

Metadaten	Schlussfolgerung
Kein Objekt gefunden („FEHLER“:“)	<p>Wenn das Objekt nicht gefunden wird, wird die Meldung „FEHLER“:“ zurückgegeben.</p> <p>Wenn das Objekt nicht gefunden wird, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um die Warnung zu löschen. Das Fehlen eines Objekts bedeutet, dass das Objekt absichtlich gelöscht wurde.</p>
Standorte > 0	<p>Wenn in der Ausgabe Standorte aufgeführt sind, kann die Warnung Objects Lost falsch positiv sein.</p> <p>Vergewissern Sie sich, dass die Objekte vorhanden sind. Verwenden Sie die Knoten-ID und den Dateipfad, der in der Ausgabe aufgeführt ist, um zu bestätigen, dass sich die Objektdatei am aufgelisteten Speicherort befindet.</p> <p>(Verfahren für "Suche nach möglicherweise verlorenen Objekten" Erläutert, wie Sie die Knoten-ID verwenden, um den richtigen Speicherknoten zu finden.)</p> <p>Wenn die Objekte vorhanden sind, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um die Warnung zu löschen.</p>
Standorte = 0	<p>Wenn in der Ausgabe keine Positionen aufgeführt sind, fehlt das Objekt möglicherweise. Versuchen Sie es "Suchen Sie das Objekt und stellen Sie es wieder her" Selbst oder Sie können sich an den technischen Support wenden.</p> <p>Vom technischen Support bitten Sie möglicherweise, zu bestimmen, ob ein Verfahren zur Storage-Recovery durchgeführt wird. Weitere Informationen finden Sie unter "Wiederherstellen von Objektdateien mit Grid Manager" Und "Wiederherstellung von Objektdateien auf einem Storage-Volume".</p>

Suche nach potenziell verlorenen Objekten und Wiederherstellung

Möglicherweise können Objekte gefunden und wiederhergestellt werden, die einen Alarm „Lost Objects“ (LOST Objects – LOST) und einen „Object Lost“-Alarm ausgelöst haben und die Sie als „potenziell verloren“ identifiziert haben.

Bevor Sie beginnen

- Sie haben die UUID eines verlorenen Objekts, wie in angegeben ["Untersuchen Sie verlorene Objekte"](#).
- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Im Anschluss an dieses Verfahren können Sie sich nach replizierten Kopien des verlorenen Objekts an einer anderen Stelle im Grid suchen. In den meisten Fällen wird das verlorene Objekt nicht gefunden. In einigen Fällen können Sie jedoch ein verlorenes repliziertes Objekt finden und wiederherstellen, wenn Sie umgehend Maßnahmen ergreifen.



Wenden Sie sich an den technischen Support, wenn Sie Hilfe bei diesem Verfahren benötigen.

Schritte

1. Suchen Sie in einem Admin-Knoten die Prüfprotokolle nach möglichen Objektspeichern:
 - a. Melden Sie sich beim Grid-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
 - b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`
 - c. Verwenden Sie `grep`, um den zu extrahieren **"Überwachungsmeldungen, die mit dem potenziell verlorenen Objekt verknüpft sind"** Und senden Sie sie an eine Ausgabedatei. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_lost_object.txt
```

- d. Verwenden Sie `grep`, um die Meldungen zum Lost Location (LLST) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep LLST output_file_name`

Beispiel:

```
Admin: # grep LLST messages_about_lost_objects.txt
```

Eine LLST-Überwachungsmeldung sieht wie diese Beispielmeldung 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) :
1581535134379225] [ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CL
SM]
[ATID (UI64) :7086871083190743409]]
```

- e. Suchen Sie in der LLST-Meldung das Feld PCLD und das Feld NOID.

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, wo eine Kopie des Objekts

gefunden werden kann.

Wenn Sie einen Speicherort für ein Objekt finden, kann das Objekt möglicherweise wiederhergestellt werden.

- a. Suchen Sie den Storage Node, der dieser LDR-Node-ID zugeordnet ist. Wählen Sie im Grid Manager **SUPPORT > Tools > Grid-Topologie** aus. Wählen Sie dann **Data Center > Storage Node > LDR** aus.

Die Knoten-ID für den LDR-Dienst befindet sich in der Tabelle Node Information. Überprüfen Sie die Informationen für jeden Speicherknoten, bis Sie den gefunden haben, der dieses LDR hostet.

2. Stellen Sie fest, ob das Objekt auf dem in der Meldung „Audit“ angegebenen Speicherknoten vorhanden ist:

- a. Melden Sie sich beim Grid-Node an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

- b. Stellen Sie fest, ob der Dateipfad für das Objekt vorhanden ist.

Verwenden Sie für den Dateipfad des Objekts den Wert von PCLD aus der LLST-Überwachungsmeldung.

Geben Sie beispielsweise Folgendes ein:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```



Schließen Sie den Pfad der Objektdatei immer in einzelne Anführungszeichen ein, um Sonderzeichen zu umgehen.

- Wenn der Objektpfad nicht gefunden wird, geht das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wird, 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 gleichen Speicherknoten aus die Eigentumsrechte an der Objektdatei, so dass sie von StorageGRID gemanagt werden kann. Geben Sie Ein: `chown ldr-user:bycast 'file_path_of_object'`
- b. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole. Geben Sie Ein: `telnet 0 1402`
- c. Geben Sie Ein: `cd /proc/STOR`
- d. Geben Sie Ein: `Object_Found 'file_path_of_object'`

Geben Sie beispielsweise Folgendes ein:

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Ausstellen der `Object_Found` Durch den Befehl wird das Raster des Speicherorts des Objekts benachrichtigt. Zudem wird die aktive ILM-Richtlinie ausgelöst, die zusätzliche Kopien gemäß den Angaben in der Richtlinie erstellt.



Wenn der Speicher-Node, auf dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf jeden Online-Speicher-Node kopieren. Platzieren Sie das Objekt in einem beliebigen `/var/local/rangedb`-Verzeichnis des Online-Storage-Node. Geben Sie dann den aus `Object_Found` Befehl mit diesem Dateipfad zum Objekt.

- Wenn das Objekt nicht wiederhergestellt werden kann, wird der `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, vergewissern Sie sich, dass neue Speicherorte erstellt wurden.

- Geben Sie Ein: `cd /proc/OBRP`
- Geben Sie Ein: `ObjectByUUID UUID_value`

Das folgende Beispiel zeigt, dass es zwei Standorte für das Objekt mit UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 gibt.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
```

```

"PPTH(Parent path)": "source",
"META": {
  "BASE(Protocol metadata)": {
    "PAWS(S3 protocol version)": "2",
    "ACCT(S3 account ID)": "44084621669730638018",
    "*ctp(HTTP content MIME type)": "binary/octet-stream"
  },
  "BYCB(System metadata)": {
    "CSIZ(Plaintext object size)": "5242880",
    "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
    "BSIZ(Content block size)": "5252084",
    "CVER(Content block version)": "196612",
    "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
    "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
    "ITME": "1581534970983000"
  },
  "CMSM": {
    "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
  },
  "AWS3": {
    "LOCC": "us-east-1"
  }
},
"CLCO\(Locations\)": \[
  \{
    "Location Type": "CLDI\(Location online\)\"",
    "NOID\(Node ID\)": "12448208",
    "VOLI\(Volume ID\)": "3222345473",
    "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
    "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
  },
  \{
    "Location Type": "CLDI\(Location online\)\"",
    "NOID\(Node ID\)": "12288733",
    "VOLI\(Volume ID\)": "3222345984",
    "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
    "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
  }
]
}

```

a. Melden Sie sich von der LDR-Konsole ab. Geben Sie Ein: `exit`

5. Durchsuchen Sie von einem Admin-Node aus die Prüfprotokolle für die ORLM-Überwachungsmeldung für dieses Objekt, um zu bestätigen, dass Information Lifecycle Management (ILM) Kopien nach Bedarf platziert hat.

a. Melden Sie sich beim Grid-Node an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`

c. Verwenden Sie `grep`, um die mit dem Objekt verknüpften Überwachungsmeldungen in eine Ausgabedatei zu extrahieren. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

d. Verwenden Sie `grep`, um die ORLM-Audit-Meldungen (Object Rules met) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep ORLM output_file_name`

Beispiel:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

Eine ORLM-Überwachungsmeldung sieht wie diese Beispielmeldung 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 FELD LOKS in der Überwachungsmeldung.

Wenn vorhanden, ist der Wert von CLDI in LOCS die Node-ID und die Volume-ID, in der eine Objektkopie erstellt wurde. Diese Meldung zeigt, dass das ILM angewendet wurde und dass an zwei Standorten im Grid zwei Objektkopien erstellt wurden.

6. "Setzt die Anzahl der verlorenen und fehlenden Objekte zurück" Im Grid-Manager.

Verlorene und fehlende Objektanzahl zurücksetzen

Nachdem Sie das StorageGRID-System untersucht und überprüft haben, ob alle aufgezeichneten verlorenen Objekte dauerhaft verloren gehen oder dass es sich um einen falschen Alarm handelt, können Sie den Wert des Attributs Lost Objects auf Null zurücksetzen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

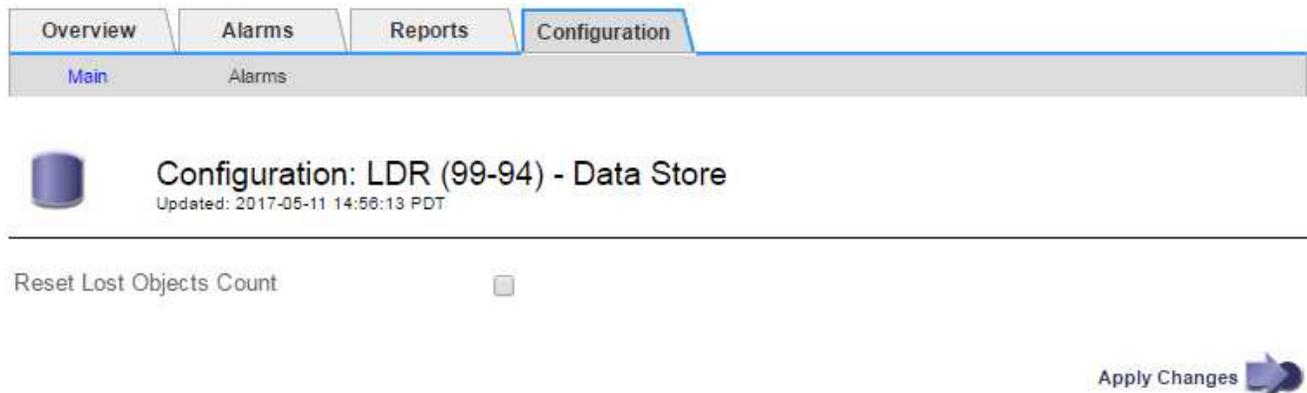
Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

- **UNTERSTÜTZUNG > Tools > Grid-Topologie > Site > Storage-Node > LDR > Data Store > Übersicht > Main**
- **UNTERSTÜTZUNG > Tools > Grid-Topologie > Site > Storage-Node > DDS > Data Store > Übersicht > Main**

Diese Anleitung zeigt das Zurücksetzen des Zählers von der Seite **LDR > Data Store**.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Site > Storage Node > LDR > Data Store > Konfiguration** für den Speicherknoten, der die Meldung **Objekte verloren** oder DEN VERLORENEN Alarm hat.
3. Wählen Sie **Anzahl Der Verlorenen Objekte Zurücksetzen**.



4. Klicken Sie Auf **Änderungen Übernehmen**.

Das Attribut Lost Objects wird auf 0 zurückgesetzt und die Warnung **Objects lost** und DIE VERLORENE Alarmfunktion werden gelöscht, was einige Minuten dauern kann.

5. Setzen Sie optional andere zugehörige Attributwerte zurück, die beim Identifizieren des verlorenen Objekts möglicherweise erhöht wurden.
 - a. Wählen Sie **Site > Storage Node > LDR > Erasure Coding > Konfiguration** aus.

- b. Wählen Sie **Reset reads Failure Count** und **Reset corrupte Kopien Detected Count** aus.
- c. Klicken Sie Auf **Änderungen Übernehmen**.
- d. Wählen Sie **Site > Storage Node > LDR > Verifizierung > Konfiguration** aus.
- e. Wählen Sie **Anzahl der fehlenden Objekte zurücksetzen** und **Anzahl der beschädigten Objekte zurücksetzen**.
- f. Wenn Sie sicher sind, dass isolierte Objekte nicht benötigt werden, können Sie **gesperrte Objekte löschen** auswählen.

Isolierte Objekte werden erstellt, wenn die Hintergrundüberprüfung eine beschädigte replizierte Objektkopie identifiziert. In den meisten Fällen ersetzt StorageGRID das beschädigte Objekt automatisch, und es ist sicher, die isolierten Objekte zu löschen. Wenn jedoch die Meldung **Objects lost** oder DER VERLORENE Alarm ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen.

- g. Klicken Sie Auf **Änderungen Übernehmen**.

Es kann einige Momente dauern, bis die Attribute zurückgesetzt werden, nachdem Sie auf **Änderungen anwenden** klicken.

Beheben Sie die Warnung „Niedrig Object Data Storage“

Der Alarm * Low Object Data Storage* überwacht, wie viel Speicherplatz zum Speichern von Objektdaten auf jedem Storage Node verfügbar ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".

Über diese Aufgabe

Die Warnung * Low Object Data Storage* wird ausgelöst, wenn die Gesamtzahl der replizierten und Erasure codierten Objektdaten auf einem Storage Node einer der Bedingungen entspricht, die in der Warnungsregel konfiguriert sind.

Standardmäßig wird eine wichtige Warnmeldung ausgelöst, wenn diese Bedingung als „true“ bewertet 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` Schätzung der Gesamtgröße der replizierten und Erasure-codierten Objektdaten für einen Storage-Node
- `storagegrid_storage_utilization_usable_space_bytes` Ist die Gesamtmenge an verbleibendem Objekt-Speicherplatz für einen Storage-Node.

Wenn ein Major oder Minor **Low Object Data Storage**-Alarm ausgelöst wird, sollten Sie so schnell wie möglich eine Erweiterung durchführen.

Schritte

1. Wählen Sie **ALERTS > Current**.

Die Seite „Meldungen“ wird angezeigt.

2. Erweitern Sie bei Bedarf aus der Warnmeldungstabelle die Warnungsgruppe **Low Object Data Storage** und wählen Sie die Warnung aus, die angezeigt werden soll.



Wählen Sie die Meldung und nicht die Überschrift einer Gruppe von Warnungen aus.

3. Überprüfen Sie die Details im Dialogfeld, und beachten Sie Folgendes:

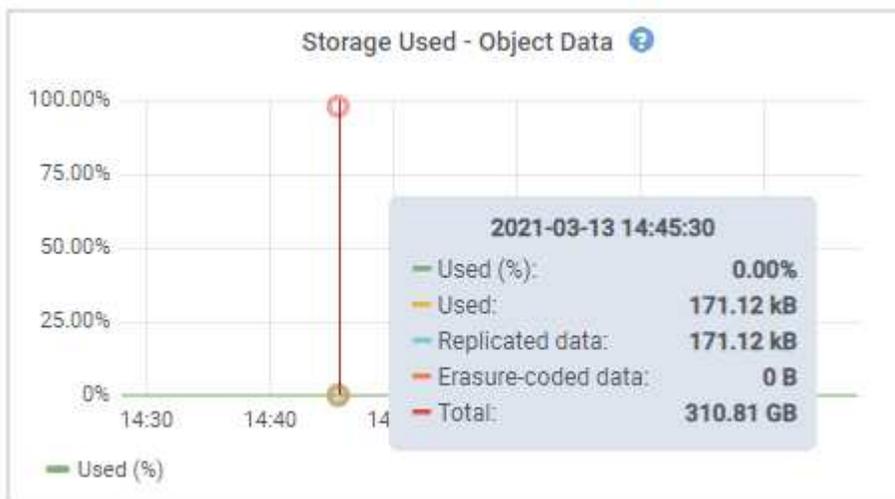
- Auslösezeit
- Der Name des Standorts und des Nodes
- Die aktuellen Werte der Metriken für diese Meldung

4. Wählen Sie **NODES > Storage Node oder Standort > Storage** aus.

5. Bewegen Sie den Cursor über die Grafik „verwendeter Speicher – Objektdaten“.

Die folgenden Werte werden angezeigt:

- **Used (%)**: 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, Standort oder Grid.
- **Erasur-codierte Daten**: Eine Schätzung der Menge der mit der Löschung codierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Gesamt**: Die Gesamtmenge an nutzbarem Speicherplatz auf diesem Knoten, Standort oder Grid. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` Metrisch.



6. Wählen Sie die Zeitsteuerelemente über dem Diagramm aus, um die Speichernutzung über verschiedene Zeiträume anzuzeigen.

Mit einem Blick auf die Storage-Nutzung im Laufe der Zeit können Sie nachvollziehen, wie viel Storage vor

und nach der Warnmeldung genutzt wurde, und Sie können schätzen, wie lange es dauern könnte, bis der verbleibende Speicherplatz des Node voll ist.

7. So bald wie möglich, "[Ergänzen Sie die Speicherkapazität](#)" Zu Ihrem Raster.

Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen.



Weitere Informationen finden Sie unter "[Management vollständiger Storage-Nodes](#)".

Verwandte Informationen

["Fehlerbehebung des Storage Status \(SSTS\)-Alarms \(Legacy\)"](#)

Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, müssen Sie möglicherweise die Warnung **Low read-only Watermark override** auflösen. Wenn möglich, sollten Sie Ihr System aktualisieren, um mit den optimierten Werten zu beginnen.

In vorherigen Versionen, die drei "[Wasserzeichen für Storage-Volumes](#)" Wurden globale Einstellungen — dieselben Werte wurden auf jedes Storage Volume auf jedem Storage Node angewendet. Ab StorageGRID 11.6 kann die Software diese Wasserzeichen für jedes Storage Volume optimieren, basierend auf der Größe des Storage-Nodes und der relativen Kapazität des Volumes.

Wenn Sie ein Upgrade auf StorageGRID 11.6 oder höher durchführen, werden die optimierten Wasserzeichen für Lese- und Schreibzugriff automatisch auf alle Speicher-Volumes angewendet, es sei denn, eine der folgenden Aussagen trifft zu:

- Ihr System ist in der Nähe der Kapazität und kann keine neuen Daten akzeptieren, wenn optimierte Wasserzeichen angewendet wurden. StorageGRID ändert in diesem Fall keine Wasserzeichen-Einstellungen.
- Sie haben zuvor eine der Storage-Volume-Wasserzeichen auf einen benutzerdefinierten Wert gesetzt. StorageGRID überschreibt keine benutzerdefinierten Wasserzeichen-Einstellungen mit optimierten Werten. Allerdings kann StorageGRID die Warnung **Low read-only Watermark override** auslösen, wenn Ihr benutzerdefinierter Wert für das Speichervolumen Soft Read-Only Watermark zu klein ist.

Analysieren Sie die Meldung

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, wird möglicherweise für einen oder mehrere Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

Jede Instanz des Alarms weist darauf hin, dass der benutzerdefinierte Wert des **Storage Volume Soft Read-Only Watermark** kleiner als der für diesen Speicherknoten optimierte Mindestwert ist. Wenn Sie die benutzerdefinierte Einstellung weiterhin verwenden, wird der Speicherknoten möglicherweise kritisch wenig Speicherplatz ausgeführt, bevor er sicher in den schreibgeschützten Zustand übergehen kann. Einige Speicher-Volumes sind möglicherweise nicht mehr zugänglich (automatisch abgehängt), wenn der Node die Kapazität erreicht.

Angenommen, Sie haben zuvor den **Speichervolumen Soft Read-Only-Wasserzeichen** auf 5 GB gesetzt. Nehmen Sie nun an, dass StorageGRID die folgenden optimierten Werte für die vier Storage-Volumes in Storage Node A berechnet hat:

Lautstärke 0	12 GB
Band 1	12 GB
Lautstärke 2	11 GB
Lautstärke 3	15 GB

Die Warnung **Low read-only Watermark override** wird für Storage Node A ausgelöst, da Ihr benutzerdefinierter Wasserzeichen (5 GB) kleiner als der für alle Volumes in diesem Knoten optimierte Mindestwert ist (11 GB). Wenn Sie die benutzerdefinierte Einstellung weiterhin verwenden, wird der Node möglicherweise schwer mit wenig Speicherplatz ausgeführt, bevor er sicher in den schreibgeschützten Zustand übergeht.

Beheben Sie die Meldung

Befolgen Sie diese Schritte, wenn eine oder mehrere **Low Read-Only-Wasserzeichen überschreiben** -Warnungen ausgelöst wurden. Sie können diese Anweisungen auch verwenden, wenn Sie derzeit benutzerdefinierte Wasserzeichen-Einstellungen verwenden und optimierte Einstellungen auch dann verwenden möchten, wenn keine Warnungen ausgelöst wurden.

Bevor Sie beginnen

- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Sie können die Warnung **Low read-only Watermark override** lösen, indem Sie benutzerdefinierte Wasserzeichen-Einstellungen auf die neuen Wasserzeichen-Überschreibungen aktualisieren. Wenn jedoch ein oder mehrere Speicherknoten nahe voll sind oder Sie spezielle ILM-Anforderungen haben, sollten Sie zunächst die optimierten Speicherabdrücke anzeigen und feststellen, ob sie sicher verwendet werden können.

Bewertung der Nutzung von Objektdaten für das gesamte Grid

Schritte

1. Wählen Sie **KNOTEN**.
2. Erweitern Sie für jeden Standort im Raster die Liste der Nodes.
3. Überprüfen Sie die Prozentwerte, die in der Spalte **Objektdaten verwendet** für jeden Speicherknoten an jedem Standort angezeigt werden.
4. Wenn keiner der Speicherknoten fast voll ist (zum Beispiel sind alle **Objektdaten verwendet** Werte kleiner als 80%), können Sie die Überschreibeinstellungen verwenden. Gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#).



Es gibt einige Ausnahmen von dieser allgemeinen Regel. Wenn ILM-Regeln beispielsweise ein strenges Aufnahmeverhalten verwenden oder bestimmte Storage-Pools nahezu vollständig sind, sollten Sie zuerst die Schritte in durchführen [Anzeigen optimierter Speicherabdrücke](#) Und [ob Sie optimierte Wasserzeichen verwenden können](#).

5. Wenn mehrere Speicherknoten nahezu voll sind, führen Sie die Schritte unter aus [Anzeigen optimierter Speicherabdrücke](#) Und [ob Sie optimierte Wasserzeichen verwenden können](#).

Anzeigen optimierter Speicherabdrücke

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das **Speichervolumen Soft Read-Only Watermark** berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Metriken**.
2. Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
3. Um das empfohlene Mindestwasserzeichen für weichen, schreibgeschützten Wert anzuzeigen, geben Sie die folgende Prometheus-Metrik ein, und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der mindestens optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das **Speichervolumen-Soft-Read-Only-Wasserzeichen**, wird für den Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

4. Um das empfohlene maximale Softread-only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der maximal optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt.

5. Beachten Sie den maximal optimierten Wert für jeden Speicherknoten.

Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können

Schritte

1. Wählen Sie **KNOTEN**.
2. Wiederholen Sie diese Schritte für jeden Online-Speicherknoten:
 - a. Wählen Sie **Storage-Node > Storage** Aus.
 - b. Scrollen Sie nach unten zur Tabelle „Objektspeichern“.
 - c. Vergleichen Sie den **verfügbaren**-Wert für jeden Objektspeicher (Volumen) mit dem für diesen Speicherknoten angegebenen maximalen optimierten Wasserzeichen.
3. Wenn mindestens ein Volume auf jedem Online-Speicherknoten mehr Speicherplatz als das maximal optimierte Wasserzeichen für diesen Knoten hat, gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#) Um die optimierten Wasserzeichen zu verwenden.

Andernfalls erweitern Sie Ihr Raster so schnell wie möglich. Entweder "[Storage-Volumes hinzufügen](#)" Zu einem vorhandenen Node oder "[Neue Storage-Nodes hinzufügen](#)". Fahren Sie dann mit fort [Verwenden Sie optimierte Wasserzeichen](#) Zum Aktualisieren der Einstellungen für Wasserzeichen.

4. Wenn Sie mit der Verwendung benutzerdefinierter Werte für die Speichervolumen-Wasserzeichen

fortfahren müssen, "Stille" Oder "Deaktivieren" Die Warnung * Low read-only Watermark override*.



Auf jedes Storage Volume auf jedem Storage Node werden dieselben benutzerdefinierten Werte angewendet. Die Verwendung kleinerer Werte als empfohlen für Speichervolumen-Wasserzeichen kann dazu führen, dass einige Speicher-Volumes nicht mehr zugänglich sind (automatisch abgehängt), wenn der Node die Kapazität erreicht.

Verwenden Sie optimierte Wasserzeichen

Schritte

1. Gehen Sie zu **KONFIGURATION** > **System** > **Speicheroptionen**.
2. Wählen Sie im Menü Speicheroptionen die Option **Konfiguration** aus.
3. Ändern Sie alle drei Wasserzeichen-Überschreibungen auf 0.
4. Wählen Sie **Änderungen Anwenden**.

Für jedes Storage Volume gelten nun optimierte Wasserzeichen, basierend auf der Größe des Storage Nodes und der relativen Kapazität des Volumes.

Storage Options Overview
Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

Fehlersuche im SSTS-Alarm (Storage Status) durchführen

Der SSTS-Alarm (Storage Status) wird ausgelöst, wenn ein Speicherknoten über nicht genügend freien Speicherplatz für den Objektspeicher verfügt.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Der SSTS-Alarm (Speicherstatus) wird auf Notice-Ebene ausgelöst, wenn die Menge an freiem Speicherplatz auf jedem Volume in einem Speicherknoten unter den Wert des Speichervolumen-Soft-Read-Only-Wasserzeichens (**KONFIGURATION > System > Speicheroptionen**) fällt.



Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

Angenommen, das Speichervolumen-Soft-Read-Only-Wasserzeichen ist auf 10 GB gesetzt, das ist der Standardwert. Der SSTS-Alarm wird ausgelöst, wenn auf jedem Speicher-Volume im Storage-Node weniger als 10 GB nutzbarer Speicherplatz verbleibt. Wenn eines der Volumes über 10 GB oder mehr verfügbaren Speicherplatz verfügt, wird der Alarm nicht ausgelöst.

Wenn ein SSTS-Alarm ausgelöst wurde, können Sie diese Schritte ausführen, um das Problem besser zu verstehen.

Schritte

1. Wählen Sie **SUPPORT > Alarme (alt) > Aktueller Alarm** aus.
2. Wählen Sie in der Spalte Service das Rechenzentrum, den Node und den Service aus, die dem SSTS-Alarm zugeordnet sind.

Die Seite Grid Topology wird angezeigt. Auf der Registerkarte „Alarme“ werden die aktiven Alarme für den ausgewählten Knoten und Dienst angezeigt.



Alarms: LDR (DC1-S3-101-195) - Storage

Updated: 2019-10-09 12:52:43 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
Normal	SHLH (Health)						<input type="checkbox"/>

Apply Changes

In diesem Beispiel wurden sowohl die SSTS-Alarme (Speicherstatus) als auch die SAVP (Total Usable Space (Prozent)) auf der Notice-Ebene ausgelöst.



Typischerweise werden sowohl der SSTS-Alarm als auch der SAVP-Alarm etwa gleichzeitig ausgelöst. Ob jedoch beide Alarme ausgelöst werden, hängt von der Wasserzeichen-Einstellung in GB und der SAVP-Alarmeinstellung in Prozent ab.

- Um festzustellen, wie viel nutzbarer Speicherplatz tatsächlich verfügbar ist, wählen Sie **LDR > Storage > Übersicht** und suchen Sie das Attribut Total Usable Space (STAS).

Overview Alarms Reports Configuration

Main

 Overview: LDR (:DC1-S1-101-193) - Storage
Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:	Online	
Storage State - Current:	Read-only	
Storage Status:	Insufficient Free Space	 

Utilization

Total Space:	164 GB	
Total Usable Space:	19.6 GB	
Total Usable Space (Percent):	11.937 %	 
Total Data:	139 GB	
Total Data (Percent):	84.567 %	

Replication

Block Reads:	0	
Block Writes:	2,279,881	
Objects Retrieved:	0	
Objects Committed:	88,882	
Objects Deleted:	16	
Delete Service State:	Enabled	

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	54.7 GB	2.93 GB	 46.2 GB	 0 B	 84.486 %	No Errors  
0001	54.7 GB	8.32 GB	 46.3 GB	 0 B	 84.644 %	No Errors  
0002	54.7 GB	8.36 GB	 46.3 GB	 0 B	 84.57 %	No Errors  

In diesem Beispiel bleiben nur 19.6 GB des 164 GB Speicherplatzes auf diesem Speicherknoten verfügbar. Beachten Sie, dass der Gesamtwert die Summe der **verfügbaren**-Werte für die drei Objektspeicher-Volumes ist. Der SSTS-Alarm wurde ausgelöst, weil jedes der drei Speicher-Volumes weniger als 10 GB verfügbaren Speicherplatz hatte.

- Um zu verstehen, wie Speicher im Laufe der Zeit genutzt wurde, wählen Sie die Registerkarte **Berichte** und zeichnen den gesamten nutzbaren Speicherplatz in den letzten Stunden.

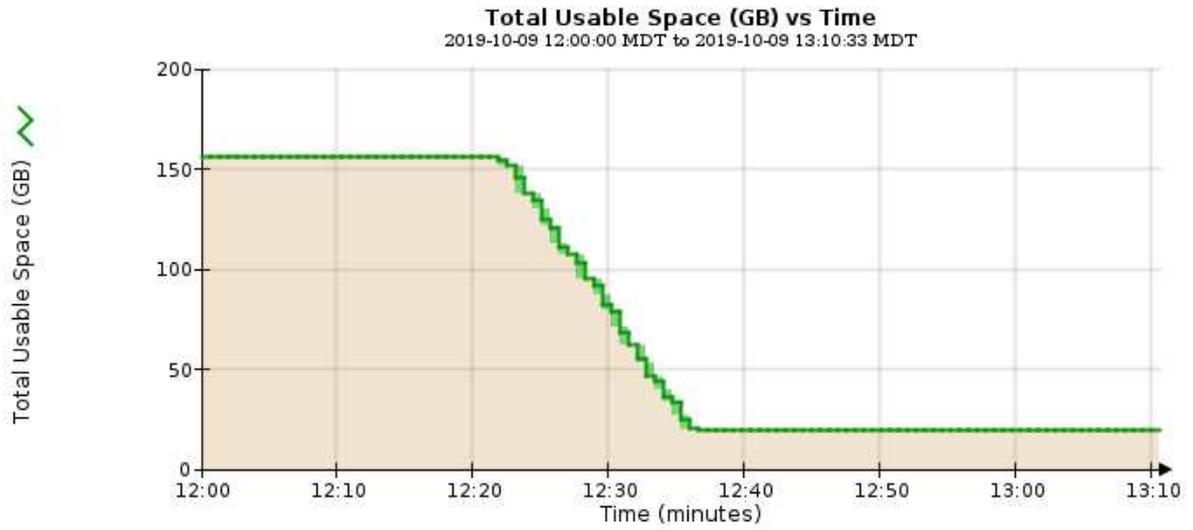
In diesem Beispiel sank der gesamte nutzbare Speicherplatz von etwa 155 GB bei 12:00 auf 20 GB bei 12:35, was der Zeit entspricht, zu der der SSTS-Alarm ausgelöst wurde.



Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	2019/10/09 12:00:00
Quick Query:	Custom Query	Raw Data:	<input type="checkbox"/>	End Date:	2019/10/09 13:10:33

Update



5. Um zu verstehen, wie Speicher als Prozentsatz der Gesamtmenge genutzt wird, geben Sie den gesamten nutzbaren Speicherplatz (Prozent) in den letzten Stunden an.

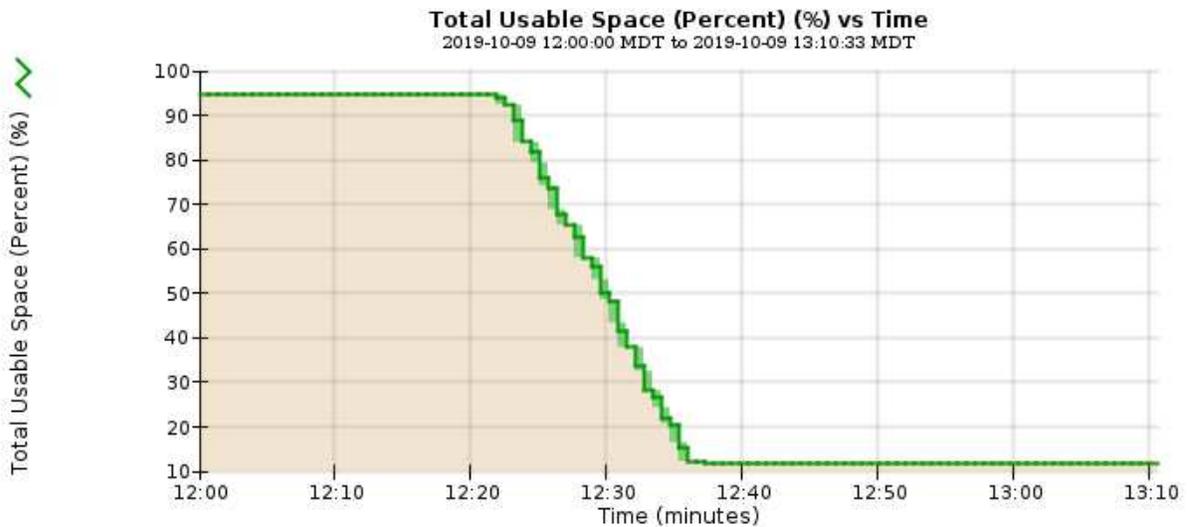
In diesem Beispiel sank der nutzbare Gesamtspeicherplatz von 95 % auf etwa 10 % zur selben Zeit.



Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space (Percent)	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	2019/10/09 12:00:00
Quick Query:	Custom Query	Raw Data:	<input type="checkbox"/>	End Date:	2019/10/09 13:10:33

Update



6. Nach Bedarf ["Ergänzen Sie die Speicherkapazität"](#).

Siehe auch ["Management vollständiger Storage-Nodes"](#).

Fehlerbehebung bei der Bereitstellung von Plattform-Services-Meldungen (SMTT-Alarm)

Der SMTT-Alarm (Total Events) wird im Grid Manager ausgelöst, wenn eine Plattfordienstmeldung an ein Ziel gesendet wird, das die Daten nicht akzeptieren kann.

Über diese Aufgabe

Beispielsweise kann ein mehrteiliger S3-Upload erfolgreich sein, auch wenn die zugehörige Replizierungs- oder Benachrichtigung nicht an den konfigurierten Endpunkt geliefert werden kann. Alternativ kann eine Nachricht für die CloudMirror Replizierung nicht bereitgestellt werden, wenn die Metadaten zu lang sind.

Der SMTT-Alarm enthält eine Meldung „Letztes Ereignis“, die lautet: Failed to publish notifications for *bucket-name object key* Für das letzte Objekt, dessen Benachrichtigung fehlgeschlagen ist.

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log` Protokolldatei. Siehe ["Referenz für Protokolldateien"](#).

Weitere Informationen finden Sie im ["Fehlerbehebung bei Plattform-Services"](#). Möglicherweise müssen Sie es ["Greifen Sie über den Tenant Manager auf den Mandanten zu"](#) So beheben Sie einen Plattfordienstfehler.

Schritte

1. Um den Alarm anzuzeigen, wählen Sie **NODES > site > Grid Node > Events** aus.
2. Letztes Ereignis oben in der Tabelle anzeigen.

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

3. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
4. Wählen Sie **Anzahl der Ereignisse zurücksetzen**.
5. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.
6. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts auszulösen.

Behebung von Metadatenproblemen

Sie können mehrere Aufgaben durchführen, um die Ursache von Metadatenproblemen zu ermitteln.

Warnmeldung für Storage mit niedrigen Metadaten

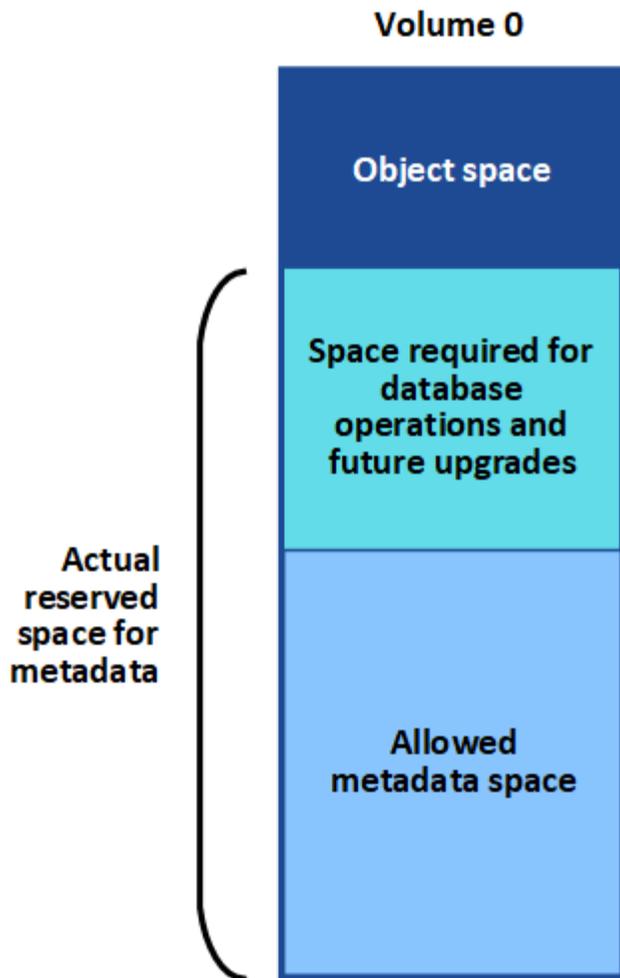
Wenn die Warnung * Storage* mit niedrigen Metadaten ausgelöst wird, müssen Sie neue Storage-Nodes hinzufügen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

StorageGRID reserviert eine bestimmte Menge an Speicherplatz auf Volume 0 jedes Storage-Nodes für Objekt-Metadaten. Dieser Speicherplatz wird als tatsächlicher reservierter Speicherplatz bezeichnet und in den Speicherplatz für Objekt-Metadaten (zulässiger Metadatenspeicherplatz) und den für wichtige Datenbankvorgänge wie Data-Compaction und Reparatur erforderlichen Speicherplatz unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.



Wenn Objektmetadaten mehr als 100 % des für Metadaten zulässigen Speicherplatzes verbrauchen, können Datenbankvorgänge nicht effizient ausgeführt werden und es treten Fehler auf.

Das können Sie "[Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node](#)" Um Ihnen zu helfen, Fehler frühzeitig zu erkennen und zu beheben, bevor sie auftreten.

StorageGRID verwendet die folgende Prometheus Kennzahl, um den vollen Umfang des zulässigen Metadaten-Speicherplatzes zu messen:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Wenn dieser Prometheus-Ausdruck bestimmte Schwellenwerte erreicht, wird die Warnung **Low Metadaten Storage** ausgelöst.

- **Minor:** Objektmetadaten verwenden 70% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie sollten so bald wie möglich neue Storage-Nodes hinzufügen.
- **Major:** Objektmetadaten verwenden 90% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie müssen sofort neue Storage-Nodes hinzufügen.



Wenn Objektmetadaten 90 % oder mehr des zulässigen MetadatenSpeichers verwenden, wird eine Warnung im Dashboard angezeigt. Wenn diese Warnung angezeigt wird, müssen Sie sofort neue Speicherknoten hinzufügen. Es ist nicht zulässig, dass Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes nutzen.

- **Kritisch:** Objektmetadaten verbrauchen 100% oder mehr des zulässigen Metadaten-Speicherplatzes und verbrauchen den für wichtige Datenbankvorgänge erforderlichen Speicherplatz. Sie müssen die Aufnahme neuer Objekte beenden und sofort neue Speicherknoten hinzufügen.

In dem folgenden Beispiel belegen die Objektmetadaten mehr als 100 % des zulässigen Metadaten-Speicherplatzes. Hierbei handelt es sich um eine kritische Situation, die zu einem ineffizienten und ineffizienten Datenbankbetrieb und zu Fehlern führt.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.



Wenn die Größe von Volume 0 kleiner ist als die Option „Metadatenreservierter Speicherplatz“ (z. B. in einer nicht-Produktionsumgebung), kann die Berechnung für die Warnmeldung * Low Metadaten Storage* fehlerhaft sein.

Schritte

1. Wählen Sie **ALERTS > Current**.
2. Erweitern Sie, falls erforderlich, aus der Warnmeldungstabelle die Warnungsgruppe **Low-Metadaten-Speicher** und wählen Sie die spezifische Warnung aus, die Sie anzeigen möchten.
3. Überprüfen Sie die Details im Dialogfeld „Warnung“.
4. Wenn eine wichtige oder kritische Warnung für * Storage-Systeme mit niedrigen Metadaten* ausgelöst wurde, führen Sie eine Erweiterung durch, um Storage-Nodes sofort hinzuzufügen.



Da StorageGRID komplette Kopien aller Objektmetadaten an jedem Standort speichert, wird die Metadaten-Kapazität des gesamten Grid durch die Metadaten-Kapazität des kleinsten Standorts begrenzt. Wenn Sie Metadaten an einem Standort hinzufügen müssen, sollten Sie auch "[Erweitern Sie alle anderen Standorte](#)" An die gleiche Anzahl von Storage-Nodes.

Nach der Erweiterung verteilt StorageGRID die vorhandenen Objekt-Metadaten neu auf die neuen Nodes, wodurch die allgemeine Metadaten des Grid erhöht werden. Es ist keine Benutzeraktion erforderlich. Die Warnung * Speicherung von niedrigen Metadaten* wird gelöscht.

Leistungen: Status - Cassandra (SVST) Alarm

Der Alarm Services: Status – Cassandra (SVST) gibt an, dass Sie die Cassandra-Datenbank für einen Storage-Node möglicherweise neu aufbauen müssen. Cassandra dient als MetadatenSpeicher für StorageGRID.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Wenn Cassandra länger als 15 Tage angehalten wird (z. B. ausgeschaltet), startet Cassandra nicht, wenn der Node wieder online geschaltet wird. Sie müssen die Cassandra-Datenbank für den betroffenen DDS-Dienst neu erstellen.

Das können Sie "[Führen Sie eine Diagnose aus](#)" Um zusätzliche Informationen über den aktuellen Zustand des Rasters zu erhalten.



Wenn zwei oder mehr der Cassandra-Datenbankdienste länger als 15 Tage ausgefallen sind, wenden Sie sich an den technischen Support und fahren Sie nicht mit den unten aufgeführten Schritten fort.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Site > Storage Node > SSM > Services > Alarme > Main**, um Alarme anzuzeigen.

Dieses Beispiel zeigt, dass der SVST-Alarm ausgelöst wurde.

The screenshot shows a web interface with tabs for Overview, Alarms, Reports, and Configuration. Under the Alarms tab, there are sub-tabs for Main and History. The main content area is titled "Alarms: SSM (DC1-S3) - Services" and includes a gear icon and an update timestamp of "Updated: 2014-08-14 16:29:36 PDT". Below this is a table with the following data:

Severity Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Minor SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:28 PDT	Not Running	Not Running		<input type="checkbox"/>

Auf der SSM Services-Hauptseite wird auch angezeigt, dass Cassandra nicht ausgeführt wird.

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC2-S1) - Services

Updated: 2017-03-30 09:53:53 MDT

Operating System: Linux
3.16.0-4-amd64

Services

Service	Version	Status	Threads	Load	Memory
Account Service	10.4.0-20161224.0333.803cd91	Running	7	0.002 %	12 MB
Administrative Domain Controller (ADC)	10.4.0-20170329.0039.8800cae	Running	52	0.14 %	63.1 MB
Cassandra	4.6.12-1.byc.0-20170308.0109.ba3598a	Not Running	0	0 %	0 B
Content Management System (CMS)	10.4.0-20170220.1846.1a76aed	Running	18	0.055 %	20.6 MB
Distributed Data Store (DDS)	10.4.0-20170329.0039.8800cae	Running	104	1.301 %	76 MB
Identity Service	10.4.0-20170203.2038.a457d45	Running	6	0 %	8.75 MB
Keystone Service	10.4.0-20170104.1815.6e52138	Running	5	0 %	7.77 MB
Local Distribution Router (LDR)	10.4.0-20170329.0039.8800cae	Running	109	0.218 %	96.6 MB
Server Manager	10.4.0-20170306.2303.9649faf	Running	4	3.58 %	19.1 MB

3. Versuchen Sie, Cassandra vom Speicher-Node neu zu starten:
 - a. Melden Sie sich beim Grid-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
 - b. Geben Sie Ein: `/etc/init.d/cassandra status`
 - c. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: `/etc/init.d/cassandra restart`
4. Falls Cassandra nicht neu startet, bestimmen Sie, wie lange Cassandra ausgefallen ist. Wenn Cassandra länger als 15 Tage ausfällt, müssen Sie die Cassandra-Datenbank neu aufbauen.



Wenn zwei oder mehr der Cassandra-Datenbankdienste ausgefallen sind, wenden Sie sich an den technischen Support, und fahren Sie nicht mit den folgenden Schritten fort.

Sie können feststellen, wie lange Cassandra ausgefallen ist, indem Sie sie aufschreiben oder die Datei `servermanager.log` lesen.

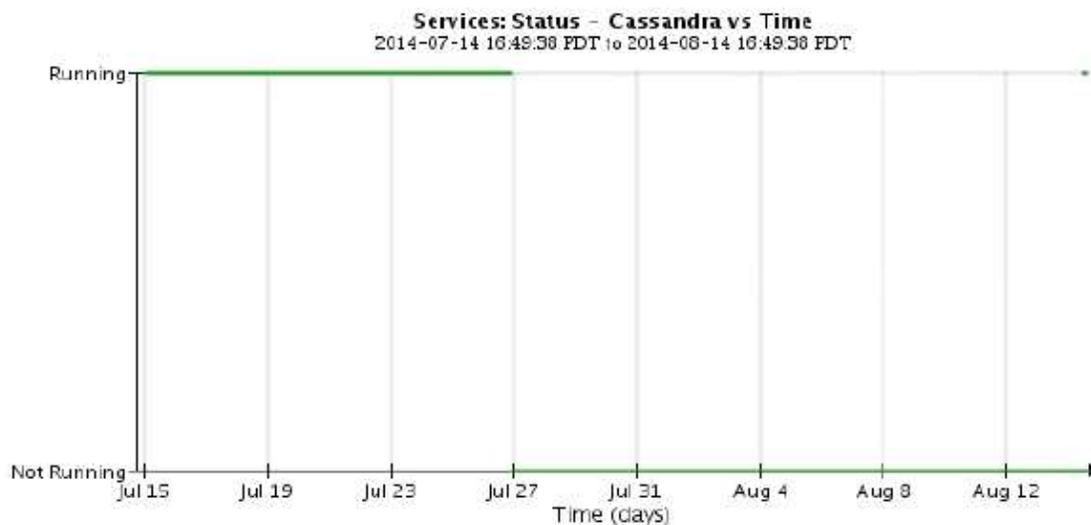
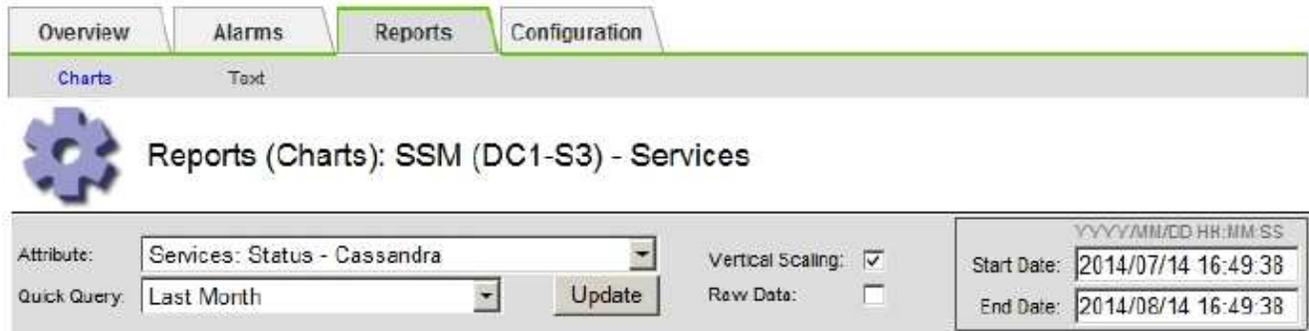
5. Cassandra Diagramm:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus. Wählen Sie dann **Site > Storage Node > SSM > Services > Berichte > Diagramme** aus.
 - b. Wählen Sie **Attribut > Service: Status - Cassandra**.
 - c. Geben Sie für **Startdatum** ein Datum ein, das mindestens 16 Tage vor dem aktuellen Datum liegt.

Geben Sie für **Enddatum** das aktuelle Datum ein.

d. Klicken Sie Auf **Aktualisieren**.

e. Wenn Cassandra für mehr als 15 Tage nicht verfügbar ist, bauen Sie die Cassandra-Datenbank erneut aus.

Das folgende Diagramm zeigt, dass Cassandra seit mindestens 17 Tagen ausgefallen ist.



6. So prüfen Sie die Datei `servermanager.log` auf dem Speicherknoten:

a. Melden Sie sich beim Grid-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

b. Geben Sie Ein: `cat /var/local/log/servermanager.log`

Der Inhalt der Datei `servermanager.log` wird angezeigt.

Wenn Cassandra länger als 15 Tage ausfällt, wird die folgende Meldung in der Datei `servermanager.log` angezeigt:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

- a. Stellen Sie sicher, dass der Zeitstempel dieser Nachricht der Zeitpunkt ist, zu dem Sie versucht haben, Cassandra wie in Schritt angegeben neu zu starten [Starten Sie Cassandra vom Storage-Node aus neu](#).

Für Cassandra gibt es mehrere Einträge; Sie müssen den letzten Eintrag finden.

- b. Wenn Cassandra länger als 15 Tage ausfällt, müssen Sie die Cassandra-Datenbank neu aufbauen.

Anweisungen hierzu finden Sie unter ["Stellen Sie Storage Node länger als 15 Tage wieder her"](#).

- c. Wenden Sie sich an den technischen Support, wenn die Alarme nach der Neuerstellung von Cassandra nicht gelöscht werden.

Cassandra-Fehler bei nicht genügend Speicher (SMTT-Alarm)

Ein Alarm für Total Events (SMTT) wird ausgelöst, wenn die Cassandra-Datenbank einen Fehler außerhalb des Arbeitsspeichers hat. Wenn dieser Fehler auftritt, wenden Sie sich an den technischen Support, um das Problem zu bearbeiten.

Über diese Aufgabe

Wenn für die Cassandra-Datenbank ein Fehler außerhalb des Arbeitsspeichers auftritt, wird ein Heap Dump erstellt, ein SMTT-Alarm (Total Events) ausgelöst und die Anzahl der Cassandra Heap Out of Memory-Fehler wird um eins erhöht.

Schritte

1. Um das Ereignis anzuzeigen, wählen Sie **SUPPORT > Tools > Grid-Topologie > Konfiguration**.
2. Stellen Sie sicher, dass die Anzahl der Cassandra Heap-Fehler bei einem Speicherfehler mindestens 1 beträgt.

Das können Sie ["Führen Sie eine Diagnose aus"](#) Um zusätzliche Informationen über den aktuellen Zustand des Rasters zu erhalten.

3. Gehen Sie zu `/var/local/core/`, Komprimieren Sie die `Cassandra.hprof` Datei erstellen und an den technischen Support senden.
4. Erstellen Sie ein Backup der `Cassandra.hprof` Datei und löschen Sie sie aus dem `/var/local/core/directory`.

Diese Datei kann bis zu 24 GB groß sein, so sollten Sie sie entfernen, um Speicherplatz freizugeben.

5. Nachdem das Problem behoben wurde, aktivieren Sie das Kontrollkästchen **Reset** für die Anzahl der Cassandra Heap Out of Memory-Fehler. Wählen Sie dann **Änderungen anwenden**.



Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung zur Konfiguration der Grid-Topologie-Seite verfügen.

Fehlerbehebung bei Zertifikatfehlern

Wenn beim Versuch, eine Verbindung mit StorageGRID über einen Webbrowser, einen S3- oder Swift-Client oder ein externes Monitoring-Tool herzustellen, ein Problem mit der Sicherheit oder dem Zertifikat auftritt, sollten Sie das Zertifikat überprüfen.

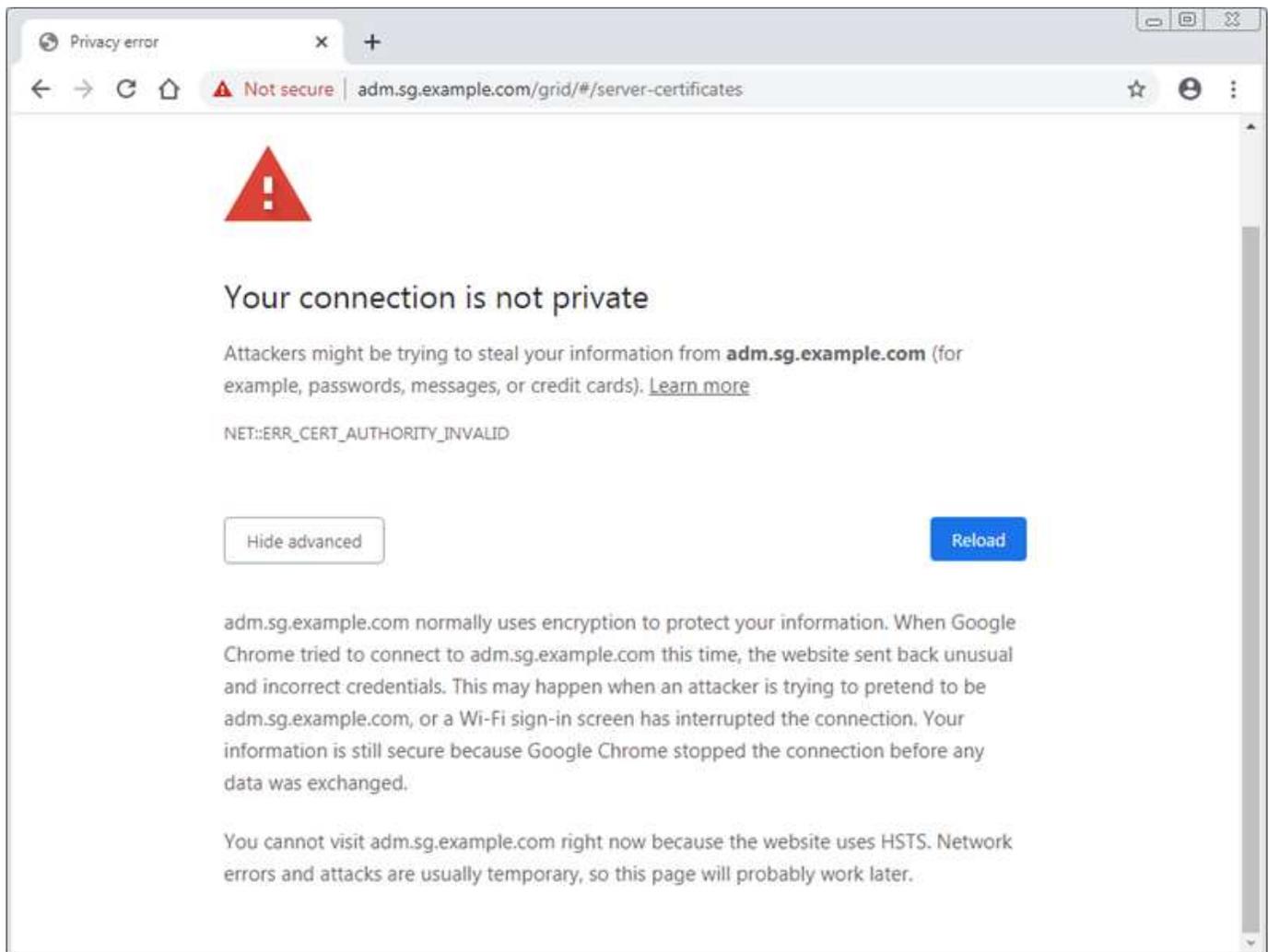
Über diese Aufgabe

Zertifikatfehler können Probleme verursachen, wenn Sie versuchen, eine Verbindung mit StorageGRID mithilfe des Grid Managers, der Grid Management API, des Mandantenmanagers oder der Mandantenmanagement-API herzustellen. Zertifikatfehler können auch auftreten, wenn Sie eine Verbindung mit einem S3- oder Swift-Client oder einem externen Monitoring-Tool herstellen.

Wenn Sie mit einem Domännennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für die benutzerdefinierte Managementoberfläche läuft ab.
- Sie werden von einem Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

Im folgenden Beispiel ist ein Zertifikatfehler angezeigt, wenn das Zertifikat der benutzerdefinierten Managementoberfläche abgelaufen ist:



Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnmeldung **Ablauf des Serverzertifikats für die Managementoberfläche** ausgelöst, wenn das Serverzertifikat abläuft.

Wenn Sie Clientzertifikate für die externe Prometheus-Integration verwenden, können Zertifikatfehler durch das Zertifikat der StorageGRID-Verwaltungsschnittstelle oder durch Clientzertifikate verursacht werden. Die auf der Seite [Zertifikate](#)* konfigurierte Warnung *Ablauf von Clientzertifikaten wird ausgelöst, wenn ein Clientzertifikat abläuft.

Schritte

Wenn Sie eine Benachrichtigung über ein abgelaufenes Zertifikat erhalten haben, rufen Sie die Zertifikatsdetails auf: . Wählen Sie **KONFIGURATION > Sicherheit > Zertifikate** und dann ["Wählen Sie die entsprechende Registerkarte Zertifikat aus"](#).

1. Überprüfen Sie die Gültigkeitsdauer des Zertifikats. + einige Webbrowser und S3- oder Swift-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.
2. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein oder generieren Sie ein neues Zertifikat.
 - Ein Serverzertifikat finden Sie in den Schritten für ["Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"](#).
 - Ein Client-Zertifikat finden Sie in den Schritten für ["Konfigurieren eines Client-Zertifikats"](#).
3. Versuchen Sie bei Serverzertifikatfehlern oder beiden der folgenden Optionen:
 - Stellen Sie sicher, dass der Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass das SAN mit der IP-Adresse oder dem Hostnamen des Node übereinstimmt, mit dem Sie eine Verbindung herstellen.
 - Wenn Sie versuchen, eine Verbindung zu StorageGRID mit einem Domain-Namen herzustellen:
 - i. Geben Sie die IP-Adresse des Admin-Knotens anstelle des Domain-Namens ein, um den Verbindungsfehler zu umgehen und auf den Grid-Manager zuzugreifen.
 - ii. Wählen Sie im Grid Manager die Option **KONFIGURATION > Sicherheit > Zertifikate** und dann ["Wählen Sie die entsprechende Registerkarte Zertifikat aus"](#) So installieren Sie ein neues benutzerdefiniertes Zertifikat oder fahren mit dem Standardzertifikat fort.
 - iii. Lesen Sie in der Anleitung zum Verwalten von StorageGRID die Schritte für ["Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"](#).

Fehlerbehebung bei Problemen mit Admin-Node und Benutzeroberfläche

Es gibt verschiedene Aufgaben, die Sie durchführen können, um die Ursache von Problemen im Zusammenhang mit Admin-Knoten und der StorageGRID-Benutzeroberfläche zu ermitteln.

Anmeldefehler

Wenn bei der Anmeldung bei einem StorageGRID-Administratorknoten ein Fehler auftritt, liegt möglicherweise ein Problem mit dem vor ["Konfiguration der Identitätsföderation"](#) A ["Netzwerk"](#) Oder ["Trennt"](#) Ein Problem mit ["Admin Node Services"](#), Oder ein ["Problem mit der Cassandra-Datenbank"](#) Auf verbundenen Storage-Nodes.

Bevor Sie beginnen

- Sie haben die `passwords.txt` Datei:
- Das ist schon ["Bestimmte Zugriffsberechtigungen"](#).

Über diese Aufgabe

Verwenden Sie diese Hinweise zur Fehlerbehebung, wenn eine der folgenden Fehlermeldungen angezeigt wird, wenn Sie versuchen, sich bei einem Admin-Knoten anzumelden:

- 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 melden Sie sich erneut an.

Wenn der Fehler nicht automatisch behoben wird, fahren Sie mit dem nächsten Schritt fort.

2. Wenn Ihr StorageGRID-System mehr als einen Admin-Knoten hat, melden Sie sich von einem anderen Admin-Knoten beim Grid-Manager an.
 - Wenn Sie sich anmelden können, können Sie die Optionen **Dashboard**, **NODES**, **Alerts** und **SUPPORT** verwenden, um die Ursache des Fehlers zu ermitteln.
 - Wenn Sie nur einen Admin-Knoten haben oder sich immer noch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.
3. Ermitteln, ob die Hardware des Node offline ist
4. Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, lesen Sie die Schritte für "[Konfigurieren der Single Sign-On-Funktion](#)".

Unter Umständen müssen Sie SSO für einen einzelnen Admin-Node vorübergehend deaktivieren und erneut aktivieren, um Probleme zu beheben.



Wenn SSO aktiviert ist, können Sie sich nicht über einen eingeschränkten Port anmelden. Sie müssen Port 443 verwenden.

5. Ermitteln Sie, ob das verwendete Konto einem föderierten Benutzer angehört.

Wenn das verbundene Benutzerkonto nicht funktioniert, melden Sie sich beim Grid Manager als lokaler Benutzer, z. B. als Root, an.

- Wenn sich der lokale Benutzer anmelden kann:
 - i. Überprüfen Sie alle angezeigten Alarmer.
 - ii. Wählen Sie **KONFIGURATION > Zugangskontrolle > Identitätsverbund** aus.
 - iii. Klicken Sie auf **Verbindung testen**, um die Verbindungseinstellungen für den LDAP-Server zu validieren.
 - iv. Wenn der Test fehlschlägt, beheben Sie alle Konfigurationsfehler.
 - Wenn der lokale Benutzer sich 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

7. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

Stellen Sie sicher, dass die nms-, mi-, nginx- und Management-API-Services 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. Vergewissern Sie sich, dass der nginx-gw-Dienst ausgeführt wird # `service nginx-gw status`

9. Lumberjack zum Sammeln von Protokollen verwenden: `# /usr/local/sbin/lumberjack.rb`

Wenn die fehlgeschlagene Authentifizierung in der Vergangenheit stattgefunden hat, können Sie die Skriptoptionen `--start` und `--end` Lumberjack verwenden, um den entsprechenden Zeitbereich festzulegen. Verwenden Sie die `lumberjack -h` für Details zu diesen Optionen.

Die Ausgabe an das Terminal gibt an, wo das Protokollarchiv kopiert wurde.

10. folgende Protokolle prüfen:

- `/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, die den ADC-Dienst an Ihrem Standort ausführen. In der Regel handelt es sich dabei um die ersten drei Storage-Nodes, die am Standort installiert wurden.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

Admin-Knoten verwenden den ADC-Dienst während des Authentifizierungsprozesses.

12. Melden Sie sich über den Admin-Node bei jedem der ADC-Speicherknoten an. Verwenden Sie dazu die IP-Adressen, die Sie identifiziert haben.
- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

13. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

Stellen Sie sicher, dass die Services `idnt`, `acct`, `nginx` und `cassandra` ausgeführt werden.

14. Wiederholen Sie die Schritte [Verwenden Sie Lumberjack, um Protokolle zu sammeln](#) Und [Protokolle prüfen](#) So prüfen Sie die Protokolle auf den Speicherknoten.

15. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Stellen Sie die Protokolle bereit, die Sie für den technischen Support gesammelt haben. Siehe auch ["Referenz für Protokolldateien"](#).

Probleme bei der Benutzeroberfläche

Die Benutzeroberfläche des Grid-Managers oder des Mandantenmanagers reagiert nach der Aktualisierung der StorageGRID-Software möglicherweise nicht wie erwartet.

Schritte

1. Stellen Sie sicher, dass Sie ein verwenden "[Unterstützter Webbrowser](#)".



Die Browser-Unterstützung kann sich mit jeder StorageGRID-Version ändern. Vergewissern Sie sich, dass Sie einen Browser verwenden, der von Ihrer StorageGRID-Version unterstützt wird.

2. Löschen Sie den Cache Ihres Webbrowsers.

Beim Löschen des Caches werden veraltete Ressourcen entfernt, die von der vorherigen Version der StorageGRID-Software verwendet werden, und die Benutzeroberfläche kann wieder ordnungsgemäß ausgeführt werden. Anweisungen hierzu finden Sie in der Dokumentation Ihres Webbrowsers.

Nicht Verfügbarer Admin-Node

Wenn das StorageGRID-System mehrere Administratorknoten enthält, können Sie den Status eines nicht verfügbaren Admin-Knotens mit einem anderen Admin-Knoten überprüfen.

Bevor Sie beginnen

Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Melden Sie sich bei einem verfügbaren Admin-Node mit einem bei Grid Manager an "[Unterstützter Webbrowser](#)".
2. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
3. Wählen Sie **Site > nicht verfügbarer Admin-Node > SSM > Services > Übersicht > Main**.
4. Suchen Sie nach Diensten, die den Status nicht aktiv haben und die möglicherweise auch blau angezeigt werden.
5. Bestimmen Sie, ob Alarme ausgelöst wurden.
6. Ergreifen Sie die entsprechenden Maßnahmen, um das Problem zu lösen.

Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen

Sie können verschiedene Aufgaben durchführen, um die Ursache von Problemen im Zusammenhang mit dem StorageGRID Netzwerk-, Hardware- und Plattformproblemen zu ermitteln.

„422: Nicht verarbeitbare Entität“ Fehler

Der Fehler 422: Nicht verarbeitbare Entität kann aus verschiedenen Gründen auftreten. Überprüfen Sie die Fehlermeldung, um festzustellen, welche Ursache Ihr Problem verursacht hat.

Wenn eine der aufgeführten Fehlermeldungen angezeigt wird, führen Sie die empfohlene Aktion durch.

Fehlermeldung	Ursache und Korrekturmaßnahme
<pre>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</pre>	<p>Diese Meldung kann auftreten, wenn Sie bei der Konfiguration der Identitätsföderation mit Windows Active Directory (AD) die Option TLS nicht verwenden für Transport Layer Security (TLS) auswählen.</p> <p>Die Verwendung der Option keine Verwendung von TLS wird nicht für die Verwendung mit AD-Servern unterstützt, die LDAP-Signatur erzwingen. Sie müssen entweder die Option STARTTLS verwenden oder die Option LDAPS verwenden für TLS auswählen.</p>
<pre>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)</pre>	<p>Diese Meldung wird angezeigt, wenn Sie versuchen, eine nicht unterstützte Chiffre zu verwenden, um eine TLS-Verbindung (Transport Layer Security) von StorageGRID zu einem externen System herzustellen, das für Identify Federation oder Cloud Storage Pools verwendet wird.</p> <p>Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss einen der verwenden "Von StorageGRID unterstützte Chiffren" Für ausgehende TLS-Verbindungen, wie in der Anleitung zur Verwaltung von StorageGRID gezeigt.</p>

Alarm bei MTU-Nichtübereinstimmung im Grid-Netzwerk

Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellung (Maximum Transmission Unit) für die Grid Network Interface (eth0) über Knoten im Grid deutlich unterscheidet.

Über diese Aufgabe

Die Unterschiede in den MTU-Einstellungen könnten darauf hinweisen, dass einige, aber nicht alle, eth0-Netzwerke für Jumbo Frames konfiguriert sind. Eine MTU-Größe von mehr als 1000 kann zu Problemen mit der Netzwerkleistung führen.

Schritte

1. Führen Sie die MTU-Einstellungen für eth0 auf allen Knoten auf.
 - Verwenden Sie die im Grid Manager angegebene Abfrage.
 - Navigieren Sie zu *primary Admin Node IP address/metrics/graph* Und geben Sie die folgende Abfrage ein: `node_network_mtu_bytes{interface='eth0'}`
2. "Ändern Sie die MTU-Einstellungen" Falls erforderlich, um sicherzustellen, dass sie für die Grid Network Interface (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 den verwenden `change-ip.py` Skript zum Ändern des MTU-Werts des Netzwerks im Container.

Verwenden Sie die folgenden Argumente, um die MTU auf Linux- oder VMware-basierten Knoten zu ändern.

Positionsargumente	Beschreibung
<code>mtu</code>	Die MTU, die eingestellt werden soll. Muss zwischen 1280 und 9216 liegen.
<code>network</code>	Die Netzwerke, auf die die MTU angewendet werden soll. Geben Sie einen oder mehrere der folgenden Netzwerktypen an: <ul style="list-style-type: none">• Raster• Admin• Client

+

Optionale Argumente	Beschreibung
<code>-h, - help</code>	Hilfemeldung anzeigen und beenden.
<code>-n node, --node node</code>	Der Node. Die Standardeinstellung ist der lokale Knoten.

NRER-Alarm (Network Receive Error)

NRER-Alarmer (Network Receive Error) können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerk-Hardware verursacht werden. In einigen Fällen können NRER-Fehler ohne manuelles Eingreifen gelöscht werden. Wenn die Fehler nicht behoben werden, führen Sie die empfohlenen Maßnahmen durch.

Über diese Aufgabe

NRER-Alarme können durch die folgenden Probleme mit Netzwerk-Hardware verursacht werden, die eine Verbindung mit StorageGRID herstellt:

- Eine Vorwärtsfehlerkorrektur (FEC) ist erforderlich und wird nicht verwendet
- Switch-Port und MTU-NIC stimmen nicht überein
- Hohe Link-Fehlerraten
- NIC-Klingelpuffer überlaufen

Schritte

1. Befolgen Sie die Schritte zur Fehlerbehebung für alle möglichen Ursachen des NRER-Alarms bei der Netzwerkkonfiguration.
2. Führen Sie je nach Fehlerursache die folgenden Schritte aus:

FEC stimmt nicht überein



Diese Schritte gelten nur für NRER-Fehler, die durch 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 physikalische Integrität der Kabel vom Gerät zum Switch.
- c. Wenn Sie die FEC-Einstellungen ändern möchten, um zu versuchen, den NRER-Alarm zu lösen, stellen Sie zunächst sicher, dass das Gerät auf der Seite Verbindungskonfiguration des Installationsprogramms für das StorageGRID-Gerät für den Modus **Auto** konfiguriert ist (siehe Anweisungen für Ihr Gerät:
 - "SG6000"
 - "SG5700"
 - "SG100 und SG1000"
- d. Ändern Sie die FEC-Einstellungen an den Switch-Ports. Die StorageGRID-Appliance-Ports passen ihre FEC-Einstellungen nach Möglichkeit an.

Sie können die FEC-Einstellungen auf StorageGRID-Geräten nicht konfigurieren. Stattdessen versuchen die Geräte, die FEC-Einstellungen an den Switch-Ports zu erkennen und zu spiegeln, an denen sie angeschlossen sind. Wenn die Verbindungen zu 25-GbE- oder 100-GbE-Netzwerkgeschwindigkeiten gezwungen sind, können Switch und NIC eine gemeinsame FEC-Einstellung nicht aushandeln. Ohne eine gemeinsame FEC-Einstellung kehrt das Netzwerk in den Modus „no-FEC“ zurück. Wenn FEC nicht aktiviert ist, sind die Anschlüsse anfälliger für Fehler, die durch elektrische Geräusche verursacht werden.



StorageGRID Appliances unterstützen Firecode (FC) und Reed Solomon (RS) FEC sowie keine FEC.

Switch-Port und MTU-NIC stimmen nicht überein

Wenn der Fehler durch einen Switch Port und eine nicht übereinstimmende NIC MTU verursacht wird, überprüfen Sie, ob die auf dem Node konfigurierte MTU-Größe mit der MTU-Einstellung für den Switch-Port identisch ist.

Die auf dem Node konfigurierte MTU-Größe ist möglicherweise kleiner als die Einstellung am Switch-Port, mit dem der Node verbunden ist. Wenn ein StorageGRID-Knoten einen Ethernet-Frame empfängt, der größer ist als seine MTU, was mit dieser Konfiguration möglich ist, wird möglicherweise der NRER-Alarm gemeldet. Wenn Sie der Ansicht sind, dass dies geschieht, ändern Sie entweder die MTU des Switch Ports entsprechend der StorageGRID Netzwerkschnittstelle MTU oder ändern Sie die MTU der StorageGRID-Netzwerkschnittstelle je nach Ihren End-to-End-Zielen oder Anforderungen an den Switch-Port.



Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein. Siehe [Fehler bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU](#) Finden Sie weitere Informationen.



Siehe auch "[MTU-Einstellung ändern](#)".

Hohe Link-Fehlerraten

- a. Aktivieren Sie FEC, falls nicht bereits aktiviert.
- b. Stellen Sie sicher, dass Ihre Netzkabel von guter Qualität sind und nicht beschädigt oder nicht ordnungsgemäß angeschlossen sind.
- c. Wenn die Kabel nicht das Problem darstellen, wenden Sie sich an den technischen Support.



In einer Umgebung mit hohem elektrischen Rauschen können hohe Fehlerraten festgestellt werden.

NIC-Klingelpuffer überlaufen

Wenn es sich bei dem Fehler um einen NIC-Ringpuffer handelt, wenden Sie sich an den technischen Support.

Der Ruffpuffer kann bei Überlastung des StorageGRID-Systems überlaufen werden und kann Netzwerkereignisse nicht zeitnah verarbeiten.

3. Nachdem Sie das zugrunde liegende Problem gelöst haben, setzen Sie den Fehlerzähler zurück.
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **site > GRID Node > SSM > Ressourcen > Konfiguration > Main** aus.
 - c. Wählen Sie **Empfangspunkt zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Verwandte Informationen

["Alarmreferenz \(Altsystem\)"](#)

Fehler bei der Zeitsynchronisierung

Möglicherweise treten Probleme mit der Zeitsynchronisierung in Ihrem Raster auf.

Wenn Probleme mit der Zeitsynchronisierung auftreten, stellen Sie sicher, dass Sie mindestens vier externe NTP-Quellen angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern, und dass alle externen NTP-Quellen normal funktionieren und von Ihren StorageGRID-Knoten zugänglich sind.



Wenn "[Angabe der externen NTP-Quelle](#)" verwenden Sie für eine StorageGRID-Installation auf Produktionsebene nicht den Windows Time-Dienst (W32Time) auf einer Windows-Version vor Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, unterstützt.

Linux: Probleme mit der Netzwerkverbindung

Möglicherweise werden Probleme mit der Netzwerkverbindung für StorageGRID Grid-Nodes auftreten, die auf Linux-Hosts gehostet werden.

Klonen VON MAC Adressen

In einigen Fällen können Netzwerkprobleme mithilfe des Klonens von MAC-Adressen behoben werden. Wenn Sie virtuelle Hosts verwenden, legen Sie den Wert des MAC-Adressenklons für jedes Ihrer Netzwerke in der

Node-Konfigurationsdatei auf „true“ fest. Diese Einstellung bewirkt, dass die MAC-Adresse des StorageGRID-Containers die MAC-Adresse des Hosts verwendet. Informationen zum Erstellen von Node-Konfigurationsdateien finden Sie in den Anweisungen für ["Red hat Enterprise Linux oder CentOS"](#) Oder ["Ubuntu oder Debian"](#).



Erstellen Sie separate virtuelle Netzwerkschnittstellen, die vom Linux Host-Betriebssystem verwendet werden können. Die Verwendung derselben Netzwerkschnittstellen für das Linux-Hostbetriebssystem und den StorageGRID-Container kann dazu führen, dass das Host-Betriebssystem 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 CentOS"](#) Oder ["Ubuntu oder Debian"](#).

Promiscuous Modus

Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen erlauben möchten, Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen zu empfangen und zu übertragen, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppen für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen auf **Accept** gesetzt sind. Die auf dem virtuellen Switch eingestellten Werte können von den Werten auf der Portgruppenebene außer Kraft gesetzt werden. Stellen Sie also 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 CentOS"](#) Oder ["Ubuntu oder Debian"](#).

Linux: Node-Status lautet „verwaiste“

Ein Linux-Node in einem verwaisten Status gibt in der Regel an, dass entweder der StorageGRID-Service oder der StorageGRID-Node-Daemon, der den Container steuert, unerwartet gestorben ist.

Über diese Aufgabe

Wenn ein Linux-Knoten meldet, dass er sich in einem verwaisten Status befindet, sollten Sie Folgendes tun:

- Überprüfen Sie die Protokolle auf Fehler und Meldungen.
- Versuchen Sie, den Node erneut zu starten.
- Verwenden Sie bei Bedarf Befehle der Container-Engine, um den vorhandenen Node-Container zu beenden.
- Starten Sie den Node neu.

Schritte

1. Überprüfen Sie die Protokolle sowohl für den Service-Daemon als auch für den verwaisten Node auf offensichtliche Fehler oder Meldungen zum unerwarteten Beenden.
2. Melden Sie sich beim Host als Root an oder verwenden Sie ein Konto mit sudo-Berechtigung.
3. Versuchen Sie, den Node 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 Node verwaiste ist, wird die Antwort angezeigt

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Stoppen Sie von Linux die Container-Engine und alle kontrollierenden 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 angehalten wird (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 Sie bemerken, dass den Knoten-Containern keine IPv6-Adressen wie erwartet zugewiesen wurden.

Über diese Aufgabe

Die IPv6-Adresse, die einem Grid-Node zugewiesen wurde, wird in den folgenden Speicherorten im Grid Manager angezeigt:

- Wählen Sie **NODES** aus, und wählen Sie den Knoten aus. Wählen Sie dann auf der Registerkarte Übersicht neben **IP-Adressen** die Option **Mehr anzeigen** aus.

DC1-S2 (Storage Node)

Overview Hardware Network Storage Objects ILM Tasks

Node information

Name: DC1-S2
 Type: Storage Node
 ID: 352bd978-ff3e-45c5-aac1-24c7278206fa
 Connection state: ✔ Connected
 Storage used: Object data 0%
 Object metadata 0%
 Software version: 11.6.0 (build 20210924.1557.00a5eb9)
 IP addresses: 172.16.1.227 - eth0 (Grid Network)
 10.224.1.227 - eth1 (Admin Network)
[Hide additional IP addresses](#)

Interface	IP address
eth0 (Grid Network)	172.16.1.227
eth0 (Grid Network)	fd20:328:328:0:250:56ff:fe87:b532

- Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus. Wählen Sie dann **Node > SSM > Ressourcen** aus. Wenn eine IPv6-Adresse zugewiesen wurde, wird sie unter der IPv4-Adresse im Abschnitt **Netzwerkadressen** aufgelistet.

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 an oder verwenden Sie ein Konto mit sudo-Berechtigung.
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 die Dokumentation zum Ändern des Betriebssystems `sysctl` Einstellungen. Ändern Sie dann den Wert in 0, bevor Sie fortfahren.

3. Geben Sie den StorageGRID-Node-Container 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 Behälter: `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 beiden Zeilen, und entfernen Sie die Kommentar-Tags. Speichern und schließen Sie anschließend die Datei.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Führen Sie folgende Befehle aus, um den StorageGRID-Container neu zu starten:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Fehlerbehebung für einen externen Syslog-Server

In der folgenden Tabelle werden Fehlermeldungen des externen Syslog-Servers

beschrieben und Korrekturmaßnahmen aufgeführt.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Hostname kann nicht aufgelöst werden	<p>Der für den Syslog-Server eingegebene FQDN konnte nicht in eine IP-Adresse aufgelöst werden.</p> <ol style="list-style-type: none">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 der Schreibweise W.X.Y.Z („gepunktete Dezimalzahl“) handelt.2. Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind.3. Vergewissern Sie sich, dass jeder Knoten auf die IP-Adressen des DNS-Servers zugreifen kann.
Verbindung abgelehnt	<p>Eine TCP- oder TLS-Verbindung zum Syslog-Server wurde abgelehnt. Möglicherweise ist auf dem TCP- oder TLS-Port für den Host kein Service verfügbar, oder eine Firewall blockiert möglicherweise den Zugriff.</p> <ol style="list-style-type: none">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 der Host für den syslog-Service einen Syslog-Daemon ausführt, der auf dem angegebenen Port abhört.3. Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten auf die IP und den Port des Syslog-Servers blockiert.
Netzwerk nicht erreichbar	<p>Der Syslog-Server befindet sich nicht in einem direkt verbundenen Subnetz. Ein Router hat eine ICMP-Fehlermeldung zurückgegeben, um anzuzeigen, dass die Testmeldungen von den aufgeführten Knoten nicht an den Syslog-Server weitergeleitet werden konnten.</p> <ol style="list-style-type: none">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 Node die Liste des Grid-Netzwerksubnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese konfiguriert sind, um Datenverkehr zum Syslog-Server über die erwartete Netzwerkschnittstelle und das erwartete Gateway (Grid, Administrator oder Client) zu leiten.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Host nicht erreichbar	<p>Der Syslog-Server befindet sich in einem direkt verbundenen Subnetz (Subnetz, das von den aufgeführten Knoten für ihre Grid-, Admin- oder Client-IP-Adressen verwendet wird). Die Knoten versuchten, Testmeldungen zu senden, erhielten aber keine Antworten auf ARP-Anfragen für die MAC-Adresse des Syslog-Servers.</p> <ol style="list-style-type: none"> 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-Service ausgeführt wird, ausgeführt wird.
Zeitüberschreitung bei Verbindung	<p>Es wurde ein TCP/TLS-Verbindungsversuch unternommen, aber für lange Zeit wurde vom Syslog-Server keine Antwort empfangen. Möglicherweise gibt es eine Fehlkonfiguration bei Routing oder eine Firewall könnte den Datenverkehr ohne jede Antwort löschen (eine häufige Konfiguration).</p> <ol style="list-style-type: none"> 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 Node die Liste des Grid-Netzwerksnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese so konfiguriert sind, dass der Datenverkehr mithilfe der Netzwerkschnittstelle und des Gateways (Grid, Admin oder Client), über die Sie den Syslog-Server erreichen möchten, an den Syslog-Server weitergeleitet wird. 3. Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten blockiert, die in der IP und dem Port des Syslog-Servers aufgeführt sind.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Verbindung vom Partner geschlossen	<p>Eine TCP-Verbindung zum Syslog-Server wurde erfolgreich hergestellt, wurde aber später geschlossen. Gründe hierfür sind u. a.:</p> <ul style="list-style-type: none"> • Der Syslog-Server wurde möglicherweise neu gestartet oder neu gestartet. • Der Node und der Syslog-Server verfügen möglicherweise über unterschiedliche TCP/TLS-Einstellungen. • Bei einer Zwischenfirewall werden möglicherweise inaktive TCP-Verbindungen geschlossen. • Ein nicht-Syslog-Server, der auf dem Syslog-Server-Port hört, hat die Verbindung möglicherweise geschlossen. <ul style="list-style-type: none"> a. 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. b. Wenn Sie TLS verwenden, bestätigen Sie, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, bestätigen Sie, dass der Syslog-Server auch TCP verwendet. c. Überprüfen Sie, ob eine Zwischenfirewall nicht für das Schließen inaktiver TCP-Verbindungen konfiguriert ist.
Fehler beim TLS-Zertifikat	<p>Das vom Syslog-Server empfangene Serverzertifikat war nicht mit dem von Ihnen angegebenen CA-Zertifikatspaket und dem von Ihnen angegebenen Clientzertifikat kompatibel.</p> <ol style="list-style-type: none"> 1. Vergewissern Sie sich, dass das CA-Zertifikatsbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat auf dem Syslog-Server kompatibel sind. 2. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Weiterleitung angehalten	<p>Syslog-Datensätze werden nicht mehr an den Syslog-Server weitergeleitet, und StorageGRID kann den Grund nicht erkennen.</p> <p>Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln.</p>

Fehlermeldung	Beschreibung und empfohlene Aktionen
TLS-Sitzung beendet	<p>Der Syslog-Server hat die TLS-Sitzung beendet und StorageGRID kann den Grund nicht erkennen.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, 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, bestätigen Sie, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, bestätigen Sie, dass der Syslog-Server auch TCP verwendet. 4. Vergewissern Sie sich, dass das CA-Zertifikatbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat vom Syslog-Server kompatibel sind. 5. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Abfrage der Ergebnisse fehlgeschlagen	<p>Der für die Konfiguration und Tests des Syslog-Servers verwendete Admin-Node kann die Testergebnisse nicht von den aufgeführten Nodes anfordern. Mindestens ein Node ist ausgefallen.</p> <ol style="list-style-type: none"> 1. Befolgen Sie die Standardschritte zur Fehlerbehebung, um sicherzustellen, dass die Knoten online sind und alle erwarteten Services ausgeführt werden. 2. Starten Sie den falsch-Dienst auf den aufgeführten Knoten neu.

Prüfung von Audit-Protokollen

Audit-Protokolle: Übersicht

Diese Anweisungen enthalten Informationen zur Struktur und zum Inhalt der StorageGRID-Prüfmeldungen und Prüfprotokolle. Sie können diese Informationen zum Lesen und Analysieren des Prüfprotokolls der Systemaktivität verwenden.

Diese Anweisungen richten sich an Administratoren, die für die Erstellung von Berichten zu Systemaktivitäten und -Nutzung verantwortlich sind, für die eine Analyse der Audit-Meldungen des StorageGRID Systems erforderlich ist.

Um die Text-Log-Datei verwenden zu können, müssen Sie auf die konfigurierte Revisionsfreigabe im Admin-Knoten zugreifen können.

Informationen über das Konfigurieren von Meldungsebenen und die Verwendung eines externen Syslog-Servers finden Sie unter ["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#).

Meldungsfluss und -Aufbewahrung von Audits

Alle StorageGRID-Services generieren während des normalen Systembetriebs Audit-

Meldungen. Sie sollten verstehen, wie diese Audit-Meldungen über das StorageGRID-System in das übertragen werden `audit.log` Datei:

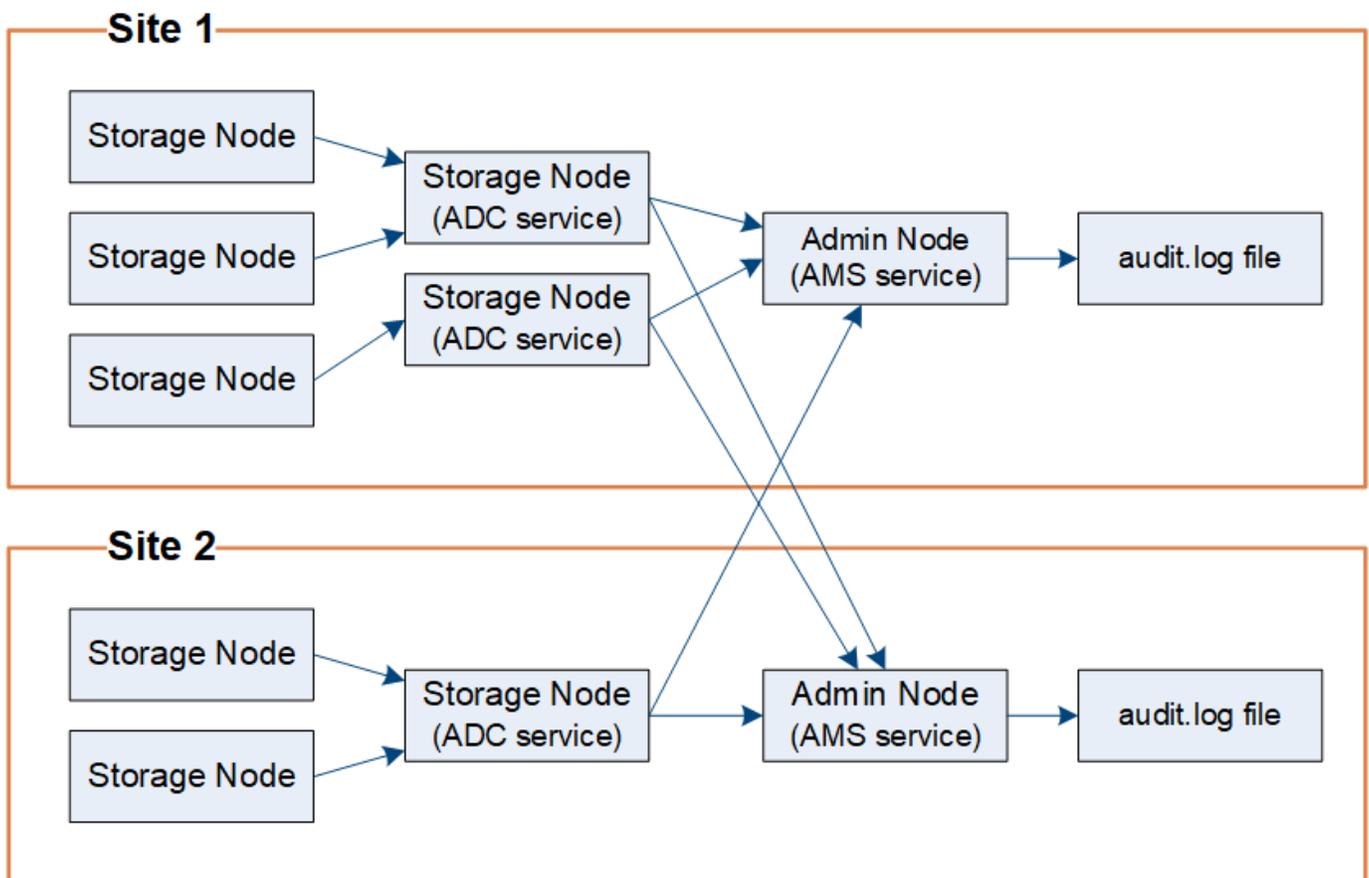
Audit-Nachrichtenfluss

Überwachungsmeldungen werden von Admin-Nodes und Storage-Nodes verarbeitet, die über einen ADC-Dienst (Administrative Domain Controller) verfügen.

Wie im Überwachungsmeldung-Flow-Diagramm dargestellt, sendet jeder StorageGRID Node seine Audit-Meldungen an einen der ADC-Services am Datacenter-Standort. Der ADC-Dienst wird automatisch für die ersten drei Speicherknotten aktiviert, die an jedem Standort installiert sind.

Jeder ADC-Dienst fungiert wiederum als Relais und sendet seine Sammlung von Audit-Meldungen an jeden Admin-Knoten im StorageGRID-System, wodurch jeder Admin-Knoten einen vollständigen Datensatz der Systemaktivität erhält.

Jeder Admin-Knoten speichert Audit-Meldungen in Text-Log-Dateien; die aktive Protokolldatei wird benannt `audit.log`.

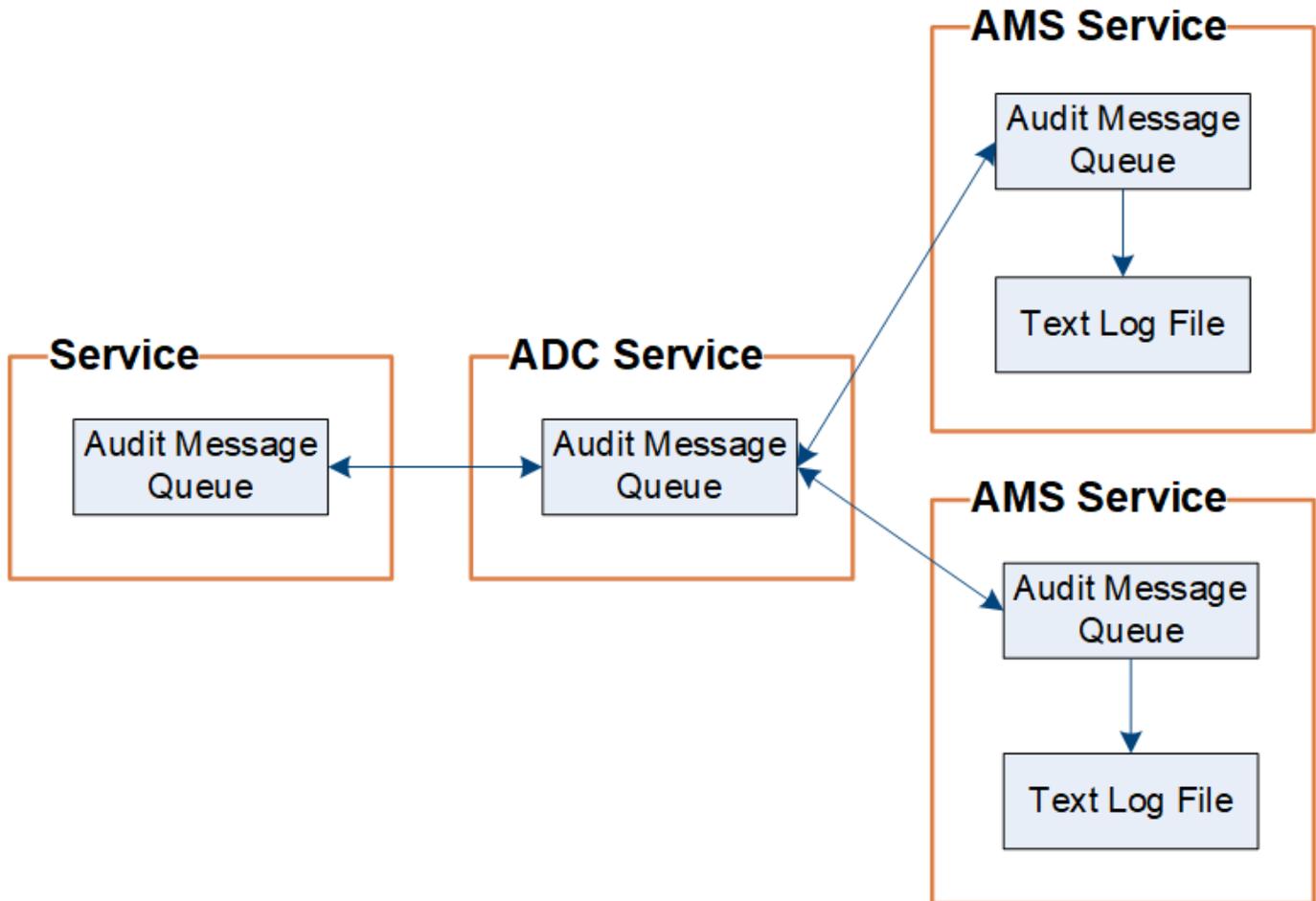


Aufbewahrung von Überwachungsnachrichten

StorageGRID verwendet einen Kopier- und Löschmodus, um sicherzustellen, dass keine Audit-Meldungen verloren gehen, bevor sie in das Audit-Protokoll geschrieben werden.

Wenn ein Knoten eine Überwachungsmeldung generiert oder sendet, wird die Meldung in einer Meldungswarteschlange auf der Systemfestplatte des Grid-Node gespeichert. Eine Kopie der Nachricht wird immer in einer Warteschlange mit Überwachungsmeldung gespeichert, bis die Nachricht in die Audit-Log-Datei

des Admin-Knotens geschrieben wird `/var/local/audit/export` Verzeichnis. Dadurch wird der Verlust einer Prüfmeldung während des Transports verhindert.



Die Warteschlange für Überwachungsnachrichten kann aufgrund von Problemen mit der Netzwerkverbindung oder aufgrund unzureichender Audit-Kapazität vorübergehend erhöht werden. Wenn die Warteschlangen steigen, verbrauchen sie mehr des verfügbaren Speicherplatzes in den einzelnen Nodes `/var/local/` Verzeichnis. Wenn das Problem weiterhin besteht und das Verzeichnis der Überwachungsmeldungen eines Knotens zu voll ist, werden die einzelnen Knoten die Verarbeitung ihres Rückstands priorisieren und für neue Meldungen vorübergehend nicht verfügbar sein.

Sie können insbesondere folgende Verhaltensweisen erkennen:

- Wenn der `/var/local/audit/export` Verzeichnis, das von einem Admin-Knoten verwendet wird, wird voll, der Admin-Knoten wird als nicht verfügbar für neue Audit-Meldungen markiert, bis das Verzeichnis nicht mehr voll ist. S3- und Swift-Client-Anforderungen werden nicht beeinträchtigt. Der Alarm XAMS (Unreachable Audit Repositories) wird ausgelöst, wenn ein Audit-Repository nicht erreichbar ist.
- Wenn der `/var/local/` Das von einem Speicherknoten mit dem ADC-Dienst verwendete Verzeichnis wird zu 92 % voll, der Knoten wird als nicht verfügbar markiert, um Meldungen zu prüfen, bis das Verzeichnis nur zu 87 % voll ist. Anforderungen von S3- und Swift-Clients an andere Nodes werden nicht beeinträchtigt. Der Alarm NRLY (Available Audit Relays) wird ausgelöst, wenn Audit-Relais nicht erreichbar sind.



Wenn keine Speicherknoten mit dem ADC-Dienst verfügbar sind, speichern die Speicherknoten die Überwachungsmeldungen lokal im `/var/local/log/localaudit.log` Datei:

- Wenn der `/var/local/` Das von einem Storage-Node verwendete Verzeichnis ist zu 85 % voll, wobei der Node die S3- und Swift-Client-Anforderungen ablehnen wird `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 Speicherknoten mit dem ADC-Dienst. Wenn einer der Systemknoten ausgefallen ist, werden die übrigen Knoten möglicherweise rückgemeldet.
- Eine nachhaltige Aktivitätsrate, die die Audit-Kapazität des Systems übersteigt.
- Der `/var/local/` Speicherplatz auf einem ADC-Speicherknoten wird aus Gründen voll, die nicht mit Audit-Meldungen zusammenhängen. In diesem Fall hört der Knoten auf, neue Überwachungsmeldungen zu akzeptieren und priorisiert seinen aktuellen Rückstand, was zu Backlogs auf anderen Knoten führen kann.

Großer Alarm für Überwachungswarteschlangen und Überwachungsmeldungen in Queued (AMQS)

Um Ihnen dabei zu helfen, die Größe der Überwachungsmeldungswarteschlangen im Laufe der Zeit zu überwachen, werden die Warnung **große Prüfwarteschlange** und der ältere AMQS-Alarm ausgelöst, wenn die Anzahl der Nachrichten in einer Speicherknotenwarteschlange oder Admin-Knoten-Warteschlange bestimmte Schwellenwerte erreicht.

Wenn der Alarm `* Large Audit queue*` oder der alte AMQS-Alarm ausgelöst wird, prüfen Sie zunächst die Auslastung des Systems – wenn eine beträchtliche Anzahl aktueller Transaktionen vorliegt, sollten sich die Warnung und der Alarm im Laufe der Zeit lösen und können ignoriert werden.

Wenn die Warnung oder der Alarm weiterhin besteht und die Schwere erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. Verringern Sie die Betriebsrate des Clients, oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie das Audit-Level für Client-Schreibvorgänge und Client-Lesevorgänge auf Fehler oder aus ändern. Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)".

Duplizieren von Nachrichten

Bei einem Netzwerk- oder Node-Ausfall ist das StorageGRID System konservativ. Aus diesem Grund können doppelte Nachrichten im Audit-Protokoll vorhanden sein.

Zugriff auf die Audit-Log-Datei

Die Revisionsfreigabe enthält die aktive `audit.log` Datei und alle komprimierten Audit-Log-Dateien. Für den einfachen Zugriff auf Audit-Protokolle können Sie "[Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS](#)". Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Bevor Sie beginnen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `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 im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält:

```
cd /var/local/audit/export
```

3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

Drehung der Audit-Log-Dateien

Audit-Log-Dateien werden auf einem Admin-Node gespeichert

`/var/local/audit/export` Verzeichnis. Die aktiven Audit-Log-Dateien werden benannt `audit.log`.



Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)".

Einmal am Tag, die aktive `audit.log` Die 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 mehrere Auditprotokolle erstellt werden, verwenden die Dateinamen das Datum, an dem die Datei im Format gespeichert wurde `yyyy-mm-dd.txt.n`. Beispiel: `2018-04-15.txt` Und `2018-04-15.txt.1` Sind die ersten und zweiten Log-Dateien, die am 15. April 2018 erstellt und gespeichert wurden.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt `yyyy-mm-dd.txt.gz`, Die das ursprüngliche Datum bewahrt. Im Lauf der Zeit führt dies zu einem Verbrauch von für Prüfprotokolle auf dem Admin-Node zugewiesenem Storage. Ein Skript überwacht den Verbrauch von Speicherplatz im Überwachungsprotokoll und löscht die Protokolldateien nach Bedarf, um Speicherplatz im freizugeben `/var/local/audit/export` Verzeichnis. Audit-Protokolle werden nach dem Erstellungsdatum der Prüfprotokolle gelöscht, wobei der älteste zuerst gelöscht wird. 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, Datei des Vortags (`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
```

Format der Auditprotokolldatei

Audit-Log-Dateiformat: Übersicht

Die Audit-Log-Dateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Nachrichten.

Jede Überwachungsmeldung enthält Folgendes:

- Die koordinierte Weltzeit (UTC) des Ereignisses, das die Meldung (ATIM) im ISO 8601-Format auslöste, gefolgt von einem Leerzeichen:

YYYY-MM-DDTHH:MM:SS.UUUUUU, Wo *UUUUUU* Nur Mikrosekunden.

- Die Meldung selbst, die in eckigen Klammern eingeschlossen ist und mit beginnt `AUDT`.

Das folgende Beispiel zeigt drei Audit-Nachrichten in einer Audit-Log-Datei (Zeilenumbrüche zur Lesbarkeit hinzugefügt). Diese Meldungen wurden generiert, wenn ein Mandant einen S3-Bucket erstellt und diesem Bucket zwei Objekte hinzugefügt hat.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(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][SAIP(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][SAIP(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 Überwachungsmeldungen in den Audit-Log-Dateien nicht einfach zu lesen oder zu interpretieren. Sie können das verwenden ["Audit-Explain-Tool"](#) Um vereinfachte Zusammenfassungen der Überwachungsmeldungen im Auditprotokoll zu erhalten. Sie können das verwenden ["Audit-Summe-Tool"](#) Zusammenfassen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

Verwenden Sie das Audit-Erklären-Tool

Sie können das verwenden `audit-explain` Tool zur Übersetzung der Audit-Meldungen

im Audit-Protokoll in ein leicht lesbares Format.

Bevor Sie beginnen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Über diese Aufgabe

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 hauptsächlich für den technischen Support bei der Fehlerbehebung vorgesehen. Wird Verarbeitet `audit-explain` Abfragen können eine große Menge an CPU-Energie verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt die typische Ausgabe von der `audit-explain` Werkzeug. Diese vier "SPUT" Audit-Meldungen wurden generiert, als der S3-Mandant mit Konto-ID 92484777680322627870 S3-PUT-Anforderungen 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` Tool kann Folgendes tun:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Mehrere Dateien gleichzeitig verarbeiten. Beispiel:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

- Nehmen Sie die Eingabe von einer Pipe an, mit der Sie die Eingabe filtern und vorverarbeiten können `grep` Befehl oder andere Mittel. Beispiel:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Da Überwachungsprotokolle sehr groß und langsam zu analysieren sind, können Sie Zeit sparen, indem Sie Teile filtern, die Sie ansehen und ausführen möchten `audit-explain` Auf die Teile, statt der gesamten Datei.



Der `audit-explain` Das Werkzeug akzeptiert keine komprimierten Dateien als Piper-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente an, oder verwenden Sie das `zcat` Werkzeug, 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-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als `root` angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` Gibt den Namen und den Speicherort der zu analysierenden Datei oder der zu analysierenden Dateien an:

```
$ audit-explain /var/local/audit/export/audit.log
```

Der `audit-explain` Werkzeug druckt menschliche Interpretationen aller Nachrichten in der angegebenen Datei oder Datei.



Um die Linienlänge zu verringern und die Lesbarkeit zu erleichtern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel anzeigen möchten, verwenden Sie den Zeitstempel (-t) Option.

Verwenden Sie das Audit-Sum-Tool

Sie können das verwenden `audit-sum` Tool zum Zählen der Schreib-, Lese-, Kopf- und Löschmeldungen und zum Anzeigen der minimalen, maximalen und durchschnittlichen Zeit (oder Größe) für jeden Operationstyp.

Bevor Sie beginnen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Über diese Aufgabe

Der `audit-sum` Tool, das auf dem primären Admin-Knoten verfügbar ist, fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.



Der `audit-sum` Das Tool ist hauptsächlich für den technischen Support bei der Fehlerbehebung vorgesehen. Wird Verarbeitet `audit-sum` Abfragen können eine große Menge an CPU-Energie verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt die typische Ausgabe von der `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

```

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 bietet Zählung und Zeiten für die folgenden S3, Swift und ILM-Audit-Meldungen in einem Prüfprotokoll:

Codieren	Beschreibung	Siehe
ARCT	Archivieren von Cloud-Tier	"ARCT: Archiv Abrufen aus Cloud-Tier"
ASCT	Archivspeicher Cloud-Tier	"ASCT: Archivspeicher Cloud-Tier"
IDEL	ILM initiated Delete: Protokolliert, wenn ILM den Prozess des Löschens eines Objekts startet.	"IDEL: ILM gestartet Löschen"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	"SDEL: S3 LÖSCHEN"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten.	"SGET S3 ABRUFEN"

Codieren	Beschreibung	Siehe
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	"SHEA: S3 KOPF"
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	"WDEL: Swift LÖSCHEN"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Container aufzulisten.	"WGET: Schneller ERHALTEN"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um das Vorhandensein eines Objekts oder Containers zu überprüfen.	"WHEA: Schneller KOPF"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Container zu erstellen.	"WPUT: Schnell AUSGEDRÜCKT"

Der `audit-sum` Tool kann Folgendes tun:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Mehrere Dateien gleichzeitig verarbeiten. Beispiel:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

- Nehmen Sie die Eingabe von einer Pipe an, mit der Sie die Eingabe filtern und vorverarbeiten können `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 Piper Input. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente an, oder verwenden Sie das `zcat` Werkzeug, um die Dateien zuerst zu dekomprimieren. Beispiel:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Mit Befehlszeilenoptionen können Operationen für Buckets separat von Operationen für Objekte zusammengefasst oder Nachrichtenübersichten nach Bucket-Namen, Zeitraum oder Zieltyp gruppieren. Standardmäßig werden in den Zusammenfassungen die minimale, maximale und durchschnittliche Betriebszeit angezeigt, Sie können jedoch die verwenden `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-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Wenn Sie alle Nachrichten analysieren möchten, die mit Schreibvorgängen, Lese-, Kopf- und Löschvorgängen zusammenhängen, führen Sie die folgenden Schritte aus:

- a. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` Gibt den Namen und den Speicherort der zu analysierenden Datei oder der zu analysierenden Dateien an:

```
$ audit-sum /var/local/audit/export/audit.log
```

Dieses Beispiel zeigt die typische Ausgabe von der `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

message group average(sec)	count	min(sec)	max(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 (S3 GET) Vorgänge im Durchschnitt mit 1.13 Sekunden die langsamsten. SGET und SPUT (S3 PUT) Vorgänge weisen jedoch lange Schlimmstfallszeiten von etwa 1,770 Sekunden auf.

- b. Um die langsamsten 10 Abruffunktionen anzuzeigen, wählen Sie mit dem grep-Befehl nur SGET-Nachrichten aus und fügen Sie die Long-Output-Option hinzu (-l) So fügen Sie Objektpfade ein:

```
grep SGET audit.log | audit-sum -l
```

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, mit dem Sie das Audit-Protokoll für andere Meldungen zu diesen speziellen Objekten grep erstellen können.

```

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/r9010aQ8JB-1566861764-4519.iso
1624414429  10.96.101.125      object    5375001556
backup/r9010aQ8JB-1566861764-6618.iso
1533143793  10.96.101.125      object    5183661466
backup/r9010aQ8JB-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

```

+

Aus diesem Beispielausgang sehen Sie, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von ca. 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe berücksichtigt die langsamen Abrufzeiten im schlimmsten Fall.

3. Wenn Sie feststellen möchten, welche Größe von Objekten in Ihr Raster aufgenommen und aus diesem abgerufen werden soll, verwenden Sie die Option „Größe“ (-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 deutlich größer. Die Anzahl der SPUT-Meldungen ist viel höher als die Anzahl der SGET-Nachrichten, was darauf hinweist, dass die meisten Objekte nie abgerufen werden.

4. Wenn Sie feststellen möchten, ob die Abrufvorgänge gestern langsam waren:
- Geben Sie den Befehl für das entsprechende Prüfprotokoll ein und verwenden Sie die Option „Gruppe für Zeit“ (-gt), gefolgt von dem Zeitraum (z. B. 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Diese Ergebnisse zeigen, dass S3 VERKEHR zwischen 06:00 und 07:00 Spikes. Auch die max- und Durchschnittszeiten sind zu diesen Zeiten deutlich höher, und sie stiegen nicht schrittweise auf, wenn die Zahl erhöht wurde. Dies deutet darauf hin, dass die Kapazität irgendwo überschritten wurde, vielleicht im Netzwerk oder in der Fähigkeit des Grids, Anfragen zu verarbeiten.

- b. Um zu bestimmen, welche Objekte in der Größe gestern jede Stunde abgerufen wurden, fügen Sie die Option Größe hinzu (-s) Zum Befehl:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Diese Ergebnisse zeigen, dass einige sehr große Rückrufe auftraten, als der gesamte Abrufverkehr seinen maximalen Wert hatte.

c. Verwenden Sie zum Anzeigen weiterer Details die **"Audit-Explain-Tool"** So überprüfen Sie alle SGET Vorgänge während dieser Stunde:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Wenn die Ausgabe des grep-Befehls viele Zeilen sein soll, fügen Sie den hinzu less Befehl zum Anzeigen des Inhalts der Audit-Log-Datei eine Seite (ein Bildschirm) gleichzeitig.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen auf Buckets langsamer sind als SPUT-Vorgänge für Objekte:

a. Verwenden Sie als erstes die -go Bei dieser Option werden Meldungen für Objekt- und Bucket-Vorgänge getrennt gruppiert:

```
grep SPUT sample.log | audit-sum -go
```

message group	count	min(sec)	max(sec)
SPUT.bucket	1	0.125	0.125
SPUT.object	12	0.025	1.019

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets unterschiedliche Leistungseigenschaften haben als SPUT-Operationen für Objekte.

- b. Um festzustellen, welche Buckets die langsamsten SPUT-Operationen haben, verwenden Sie den `-gb` Option, die Meldungen nach Bucket gruppiert:

```
grep SPUT audit.log | audit-sum -gb
```

message group	count	min(sec)	max(sec)
SPUT.cho-non-versioning	71943	0.046	1770.563
SPUT.cho-versioning	54277	0.047	1736.633
SPUT.cho-west-region	80615	0.040	55.557
SPUT.ldt002	1564563	0.011	51.569

- c. Um zu bestimmen, welche Buckets die größte SPUT-Objektgröße haben, verwenden Sie beide `-gb` Und das `-s` Optionen:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ldt002 0.352	1564563	0.000	999.972

Überwachungsmeldungsformat

Meldungsformat: Überblick

Im StorageGRID-System ausgetauschte Audit-Meldungen enthalten Standardinformationen, die für alle Meldungen und spezifische Inhalte zur Beschreibung des Ereignisses oder der Aktivität üblich sind.

Wenn die von bereitgestellten Zusammenfassungsdaten angezeigt werden ["Audit-Erklärung"](#) und ["Audit-Summe"](#) Tools reichen nicht aus. Lesen Sie in diesem Abschnitt, um das allgemeine Format aller Audit-Meldungen zu verstehen.

Im Folgenden finden Sie eine Beispielmeldung, wie sie in der Audit-Log-Datei angezeigt werden kann:

```
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):9445736326500603516]]
```

Jede Überwachungsmeldung enthält eine Zeichenfolge von Attributelementen. Der gesamte String ist in Klammern eingeschlossen ([]), und jedes Attributelement in der Zeichenfolge weist folgende Merkmale auf:

- In Halterungen eingeschlossen []
- Eingeführt durch den String AUDT, Das eine Audit-Nachricht anzeigt
- Ohne Trennzeichen (keine Kommata oder Leerzeichen) vor oder nach
- Wird durch ein Zeilenvorschub-Zeichen beendet \n

Jedes Element umfasst einen Attributcode, einen Datentyp und einen Wert, der in diesem Format angegeben wird:

```
[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 werden in keiner bestimmten Reihenfolge aufgeführt.

In der folgenden Liste werden die Attributelemente beschrieben:

- `ATTR` Ist ein 4-Zeichen-Code für das Attribut, das gemeldet wird. Es gibt einige Attribute, die für alle Audit-Meldungen und andere, die ereignisspezifisch sind, gelten.
- `type` Ist eine 4-Zeichen-Kennung des Programmierdatentyps des Wertes, wie UI64, FC32 usw. Der Typ ist in Klammern eingeschlossen ().
- `value` Ist der Inhalt des Attributs, in der Regel ein numerischer Wert oder Textwert. Werte folgen immer einem Doppelpunkt (:). Werte des Datentyps CSTR werden von doppelten Anführungszeichen umgeben " ".

Datentypen

Verschiedene Datentypen werden zur Speicherung von Informationen in Audit-Meldungen verwendet.

Typ	Beschreibung
UI32	Unsigned long integer (32 Bit); es kann die Zahlen 0 bis 4,294,967,295 speichern.
UI64	Unsigned double long integer (64 Bit); es kann die Zahlen 0 bis 18,446,744,073,709,551,615 speichern.
FC32	4-Zeichen-Konstante; ein 32-Bit-Integer-Wert ohne Vorzeichen, der als vier ASCII-Zeichen wie „ABCD“ dargestellt wird.
IPAD	Wird für IP-Adressen verwendet.
CSTR	Ein Array mit variabler Länge von UTF-8 Zeichen. Zeichen können mit den folgenden Konventionen entgangen werden: <ul style="list-style-type: none">• Backslash ist \.• Der Schlittenrücklauf beträgt \r• Doppelte Anführungszeichen sind \".• Zeilenvorschub (neue Zeile) ist \n.• Zeichen können durch ihre hexadezimalen Äquivalente ersetzt werden (im Format \xHH, wobei HH der hexadezimale Wert ist, der das Zeichen darstellt).

Ereignisspezifische Daten

Jede Überwachungsmeldung im Prüfprotokoll zeichnet Daten auf, die für ein

Codieren	Typ	Beschreibung
ATIM	UI64	<p>Zeitstempel: Die Zeit, zu der das Ereignis generiert wurde, das die Audit-Nachricht auslöste, gemessen in Mikrosekunden seit der Betriebssystemepoche (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.</p> <p>Möglicherweise ist ein Aufrundung oder Verkürzung des protokollierten Zeitstempels erforderlich. Die vom Benutzer lesbare Zeit, die am Anfang der Überwachungsmeldung im angezeigt wird <code>audit.log</code> Die Datei ist das ATIM-Attribut im ISO 8601-Format. Das Datum und die Uhrzeit werden als dargestellt <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, Wo der T Ist ein Literalzeichenzeichen, das den Beginn des Zeitsegments des Datums angibt. <code>UUUUUU</code> Nur Mikrosekunden.</p>
ATYP	FC32	Ereignistyp: Eine vierstellige Kennung des zu protokollierenden Ereignisses. Dies regelt den "Nutzlastinhalt" der Nachricht: Die Attribute, die enthalten sind.
AVER	UI32	Version: Die Version der Audit-Nachricht. Wenn die StorageGRID Software weiterentwickelt wird, können neue Serviceversionen neue Funktionen in die Audit-Berichte integrieren. Dieses Feld ermöglicht die Abwärtskompatibilität im AMS-Dienst zur Verarbeitung von Meldungen aus älteren Serviceversionen.
RSLT	FC32	Ergebnis: Das Ergebnis von Ereignis, Prozess oder Transaktion. Wenn für eine Nachricht nicht relevant ist, WIRD KEINE verwendet, sondern SUCS, damit die Nachricht nicht versehentlich gefiltert wird.

Beispiele für Überwachungsnachrichten

Detaillierte Informationen finden Sie in jeder Audit-Nachricht. Alle Überwachungsmeldungen verwenden das gleiche Format.

Im Folgenden finden Sie eine Beispielmeldung für Audits, wie sie im angezeigt werden kann `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):"s3small11"][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 Überwachungsmeldung enthält Informationen über das zu protokollierte Ereignis sowie Informationen über die Meldung selbst.

Um festzustellen, welches Ereignis durch die Überwachungsmeldung 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):"s3small11"][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 Meldung des Audits zeigt auch den Bucket an, dem das Objekt zugeordnet ist:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK\CSTR\):"s3small11"][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 zu ermitteln, wann das PUT-Ereignis aufgetreten ist, notieren Sie den UTC-Zeitstempel (Universal Coordinated Time, Universal Coordinated Time, koordinierte Zeit) zu Beginn der Überwachungsmeldung. Dieser Wert ist eine vom Menschen lesbare Version des ATIM-Attributs der Überwachungsmeldung selbst:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][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. Im Beispiel der Wert 1405631878959669 Übersetzt bis Donnerstag, 17. Juli 2014 21:17:59 UTC.

Überwachungsmeldungen und der Lebenszyklus von Objekten

Wann werden Audit-Meldungen generiert?

Audit-Nachrichten werden bei jeder Aufnahme, jedem Abruf oder jedem Löschen eines Objekts generiert. Sie können diese Transaktionen im Audit-Protokoll identifizieren, indem Sie API-spezifische (S3 oder Swift) Audit-Nachrichten suchen.

Überwachungsmeldungen werden durch Kennungen verknüpft, die für jedes Protokoll spezifisch sind.

Protokoll	Codieren
Verknüpfen von S3-Vorgängen	S3BK (Eimer), S3KY (Schlüssel) oder beide
Swift-Vorgänge verknüpfen	WCON (Container), WOBJ (Object) oder beides
Verknüpfen interner Vorgänge	CBID (interne Kennung des Objekts)

Timing von Audit-Meldungen

Aufgrund von Faktoren wie Zeitunterschieden zwischen Grid-Nodes, Objektgröße und Netzwerkverzögerungen kann die Reihenfolge der durch die verschiedenen Services erzeugten Audit-Meldungen von den Beispielen in diesem Abschnitt abweichen.

Archiv-Nodes

Die Reihe von Meldungen, die beim Senden von Objektdaten an ein externes Archiv-Speichersystem generiert werden, ist ähnlich wie bei Storage-Nodes, es sei denn, es gibt keine SCMT-Meldung (Store Object Commit). Und die ATCE (Archive Object Store Begin) und ASCE (Archive Object Store End) Nachrichten werden für jede archivierte Kopie von Objektdaten generiert.

Die Reihe von Audit-Meldungen, die beim Abrufen von Objektdaten aus einem externen Archiv-Storage-System generiert werden, ähnelt der für Storage-Nodes, jedoch werden für jede abgerufene Kopie von Objektdaten ARCB (Archivobjekt Retrieve Begin) und ARCE (Archive Object Retrieve End) Nachrichten generiert.

Die beim Löschen von Objektdaten aus einem externen Archivspeichersystem generierte Reihe von Überwachungsmeldungen ähnelt der für Speicherknotten, es sei denn, ES gibt keine SREM (Object Store Remove)-Nachricht und für jede Löschanforderung gibt es eine AREM-Nachricht (Archive Object Remove).

Objektaufnahme von Transaktionen

Sie können Transaktionen zur Client-Aufnahme im Prüfprotokoll identifizieren, indem API-spezifische (S3 oder Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Aufnahmetransaktion generierten Audit-Meldungen aufgeführt. Es sind nur die Nachrichten enthalten, die für die Aufzeichnung der Transaktion erforderlich sind.

S3 Aufnahme von Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SPUT	S3 PUT-Transaktion	Eine S3-PUT-Aufnahmerate 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 Ingest-Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
WPUT	Swift PUT-Transaktion	EINE Swift PUT-Aufnahme-Transaktion wurde erfolgreich abgeschlossen.	CBID, WCON, WOBJ	"WPUT: Schnell AUSGEDRÜCKT"
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Beispiel: S3-Objektaufnahme

Die folgende Serie von Audit-Meldungen ist ein Beispiel für die im Revisionsprotokoll generierten und gespeicherten Audit-Meldungen, wenn ein S3-Client ein Objekt in einen Storage-Node (LDR-Service) einspeist.

In diesem Beispiel umfasst die aktive ILM-Richtlinie die ILM-Regel „2 Kopien erstellen“.



Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Audit-Meldungen aufgeführt. Es werden nur solche aufgeführt, die sich auf die S3-Aufnahmetransaktion (SPUT) beziehen.

In diesem Beispiel wird vorausgesetzt, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Meldung gibt an, 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):"SGKHya1RU_5cLflqajtaFmxJn9461AWRJfBF33gAOg=="][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-Meldung gibt an, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Meldung enthält die CBID des Objekts und den Namen der verwendeten ILM-Regel.

Bei replizierten Objekten umfasst das Feld LOCS die LDR-Node-ID und 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]]
```

Für Objekte, die mit Erasure Coding codiert wurden, enthält das Feld LOCS die Profil-ID für Erasure Coding und die Gruppen-ID für Erasure Coding

```
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 PFADFELD umfasst S3-Bucket und wichtige Informationen sowie 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]]
```

Löschen von Objekttransaktionen

Sie können Transaktionen zum Löschen von Objekten im Prüfprotokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Meldungen angezeigt werden.

In den folgenden Tabellen sind nicht alle während einer Löschttransaktion generierten

Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die zum Verfolgen der Löschransaktion erforderlich sind.

S3-Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	Anforderung zum Löschen des Objekts aus einem Bucket gemacht.	CBID, S3KY	"SDEL: S3 LÖSCHEN"

Swift Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WDEL	Swift Löschen	Anforderung gemacht, das Objekt aus einem Container oder Container zu löschen.	CBID, WOBJ	"WDEL: Swift LÖSCHEN"

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt aus einem Storage-Node (LDR-Service) löscht, wird eine Überwachungsmeldung generiert und im Revisionsprotokoll gespeichert.



Im folgenden Beispiel sind nicht alle während einer Löschransaktion generierten Audit-Meldungen aufgeführt. Es werden nur diejenigen aufgelistet, die mit der S3-Löschransaktion (SDEL) in Verbindung stehen.

SDEL: S3 Löschen

Die Objektlöschung beginnt, wenn der Client eine LÖSCHANFORDERUNG an einen LDR-Dienst sendet. Die Meldung 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_5cLflqajtaFmxJn9461AWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity:70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SBA
C(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]]
```

Abrufen von Objekttransaktionen

Sie können Transaktionen zum Abrufen von Objekten im Audit-Protokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Abruftransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die für die Rückrufs-Transaktion erforderlich sind.

S3-Abruf von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 ABRUFEN	Anforderung zum Abrufen eines Objekts aus einem Bucket	CBID, S3BK, S3KY	"SGET S3 ABRUFEN"

Schnelles Abrufen von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WGET	Swift GET	Anforderung gemacht, ein Objekt aus einem Container abzurufen.	CBID, WCON, WOBJ	"WGET: Schneller ERHALTEN"

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Storage-Node (LDR-Service) abrufen, wird eine Audit-Meldung erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET S3 ABRUFEN

Der Objektabruf beginnt, wenn der Client eine GET Object-Anforderung an einen LDR-Service sendet. Die Meldung 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][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\ (FC32\) :SGET\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Wenn die Bucket-Richtlinie ermöglicht, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört. Die Überwachungsmeldung enthält Informationen über das Mandantenkonto des Bucket-Inhabers, sodass Sie diese anonymen und Cross-Account-Anforderungen verfolgen können.

In der folgenden Beispielnachricht sendet der Client eine GET Object-Anforderung für ein in einem Bucket gespeichertes Objekt, das nicht Eigentümer ist. Die Werte für SBAI und SBAC zeichnen die Konto-ID und den Namen des Mandanten des Bucket-Besitzers auf. Diese Werte unterscheiden sich von der Konto-ID und dem Namen des in S3AI und SACC aufgezeichneten Clients.

```
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(UI
32):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 Audit-Meldungen erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3 Select-Transaktion (SelectObjectContent) beziehen.

Jede Abfrage ergibt zwei Überwachungsmeldungen: Eine, die die Autorisierung der S3 Select-Anforderung ausführt (das S3SR-Feld ist auf "select" gesetzt) und eine nachfolgende Standard-GET-Operation, die die Daten während der Verarbeitung aus dem Speicher abrufen.

```
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] ]

```

Nachrichten zum Metadatenupdate

Audit-Meldungen werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

Audit-Meldungen zu S3-Metadaten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3-Metadaten wurden aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert.	CBID, S3KY, HTRH	"SUPD: S3-Metadaten wurden aktualisiert"

Beispiel: S3-Metadatenaktualisierung

Das Beispiel zeigt eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes S3-Objekt.

SUPD: S3-Metadatenaktualisierung

Der S3-Client fordert eine SUPD (SUPD) auf, die angegebenen Metadaten zu aktualisieren (`x-amz-meta-*`) Für das S3-Objekt (S3KY). In diesem Beispiel sind Anforderungsheader im Feld HTRH enthalten, da sie als Audit-Protokoll-Header konfiguriert wurde (**KONFIGURATION > Monitoring > Audit- und Syslog-Server**). Siehe ["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]]
```

Audit-Meldungen

Audit-Meldungen: Übersicht

Detaillierte Beschreibungen der vom System zurückgegebenen Audit-Meldungen finden Sie in den folgenden Abschnitten. Jede Überwachungsmeldung wird zuerst in einer Tabelle aufgeführt, in der verwandte Nachrichten nach der Aktivitätsklasse gruppiert werden, für die die Meldung steht. Diese Gruppierungen sind sowohl für das Verständnis der Arten von Aktivitäten, die geprüft werden, als auch für die Auswahl der gewünschten Art der Filterung von Überwachungsnachrichten nützlich.

Die Überwachungsmeldungen werden auch alphabetisch nach ihren vier-Zeichen-Codes aufgelistet. Mit dieser alphabetischen Liste können Sie Informationen zu bestimmten Nachrichten finden.

Die in diesem Kapitel verwendeten 4-Zeichen-Codes sind die ATYP-Werte, die in den Audit-Meldungen gefunden werden, wie in der folgenden Beispielmeldung dargestellt:

```
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 über das Festlegen von Meldungsebenen, das Ändern von Protokollzielen und die Verwendung eines externen Syslog-Servers für Ihre Audit-Informationen finden Sie unter ["Konfigurieren von"](#)

Kategorien von Überwachungsnachrichten

Systemaudits Meldungen

Die Audit-Meldungen, die zur Systemauditkategorie gehören, werden für Ereignisse im Zusammenhang mit dem Überwachungssystem selbst, Grid-Node-Status, systemweiter Aufgabenaktivität (Grid-Aufgaben) und Service-Backup-Vorgängen verwendet.

Codieren	Titel und Beschreibung der Nachricht	Siehe
ECMC	Datenfragment mit Löschcode fehlt: Zeigt an, dass ein fehlendes Datenfragment mit Löschungscode erkannt wurde.	"ECMC: Fehlendes Erasure coded Data Fragment"
ECOC	Beschädigte Datenfragment mit Erasure-Code: Zeigt an, dass ein korruptes Datenfragment mit Löschungscode erkannt wurde.	"ECOC: Korrupte, mit Erasure codierte Datenfragment"
ETAF	Sicherheitsauthentifizierung fehlgeschlagen: Verbindungsversuch mit TLS (Transport Layer Security) fehlgeschlagen.	"ETAF: Sicherheitsauthentifizierung fehlgeschlagen"
GNRG	GNDS Registrierung: Ein Dienst aktualisiert oder registriert Informationen über sich selbst im StorageGRID-System.	"GNRG: GNDS Registrierung"
GNUR	GNDS Unregistrierung: Ein Dienst hat sich vom StorageGRID-System nicht registriert.	"GNUR: GNDS Registrierung aufheben"
GTED	Grid Task beendet: Der CMN-Dienst hat die Verarbeitung der Grid-Aufgabe abgeschlossen.	"GTED: Grid Task beendet"
GTST	Grid Task gestartet: Der CMN-Dienst hat mit der Verarbeitung der Grid-Aufgabe begonnen.	"GTST: Grid Task gestartet"
GSU	Grid Task übermittelt: Eine Grid-Aufgabe wurde an den CMN-Dienst übermittelt.	"GTSU: Grid Task übermittelt"
LLST	Standort verloren: Diese Überwachungsmeldung wird generiert, wenn ein Standort verloren geht.	"LLST: Standort verloren"
OLST	Objekt verloren: Ein angeforderter Gegenstand kann nicht innerhalb des StorageGRID Systems gefunden werden.	"OLST: System hat Lost Object erkannt"

Codieren	Titel und Beschreibung der Nachricht	Siehe
SADD	Sicherheitsüberprüfung deaktivieren: Die Protokollierung von Überwachungsnachrichten wurde deaktiviert.	"SADD: Security Audit deaktiviert"
SADE	Sicherheitsüberprüfung aktivieren: Die Protokollierung von Prüfnachrichten wurde wiederhergestellt.	"SADE: Sicherheits-Audit aktivieren"
SVRF	Objektspeicherüberprüfung fehlgeschlagen: Überprüfung durch einen Inhaltsblock fehlgeschlagen.	"SVRF: Objektspeicherüberprüfung fehlgeschlagen"
SVRU	Objektspeicher Verify Unbekannt: Unerwartete Objektdaten im Objektspeicher erkannt.	"SVRU: Objektspeicher überprüfen Unbekannt"
SYSD	Knotenstopp: Es wurde ein Herunterfahren angefordert.	"SYSD: Knoten stoppen"
SYST	Knoten stoppen: Ein Dienst hat einen graziösen Stopp initiiert.	"SYST: Knoten wird angehalten"
SYSU	Node Start: Ein Dienst gestartet. In der Meldung wird der Charakter des vorherigen Herunterfahrens angezeigt.	"SYSU: Knoten Start"

Audit-Meldungen zu Objekt-Storage

Die Audit-Meldungen der Objekt-Storage-Audit-Kategorie werden für Ereignisse im Zusammenhang mit der Speicherung und Verwaltung von Objekten im StorageGRID System verwendet. Dazu zählen Objekt-Storage und -Abruf, Grid-Node zu Grid-Node-Transfers und Verifizierungen.

Codieren	Beschreibung	Siehe
APCT	Archiv aus Cloud-Tier: Archivierte Objektdaten werden aus einem externen Archiv-Storage-System gelöscht, das über die S3-API eine Verbindung zur StorageGRID herstellt.	"APCT: Löschen von Archiven aus der Cloud-Ebene"
ARCB	Archiv Objekt abrufen Begin: Der ARC-Dienst beginnt den Abruf von Objektdaten aus dem externen Archivspeichersystem.	"ARCB: Archiv Objekt abrufen beginnen"
ARCE	Archivobjekt Retrieve End: Objektdaten wurden von einem externen Archivspeichersystem abgerufen, und der ARC-Dienst meldet den Status des Abruffvorgangs.	"ARCE: Archiv Objekt abrufen Ende"

Codieren	Beschreibung	Siehe
ARCT	Archive Retrieve von Cloud-Tier: Archivierte Objektdaten werden von einem externen Archiv-Storage-System abgerufen, das über die S3-API eine Verbindung zur StorageGRID herstellt.	"ARCT: Archiv Abrufen aus Cloud-Tier"
AREM	Archiv Objekt entfernen: Ein Inhaltsblock wurde erfolgreich oder erfolglos aus dem externen Archiv-Speichersystem gelöscht.	"ARM: Archivobjekt Entfernen"
ASCE	Archiv Objekt Store Ende: Ein Inhaltsblock wurde auf das externe Archivspeichersystem geschrieben und der ARC-Dienst meldet den Status des Schreibvorgangs.	"ASCE: Archiv-Objektspeicher Ende"
ASCT	Archivspeicher Cloud-Tier: Objektdaten werden in einem externen Archiv-Storage-System gespeichert, das über die S3-API eine Verbindung zur StorageGRID herstellt.	"ASCT: Archivspeicher Cloud-Tier"
ATCE	Archive Object Store Begin: Das Schreiben eines Inhaltsblocks in einen externen Archiv-Speicher hat begonnen.	"ATCE: Archiv-Objektspeicher beginnen"
AVCC	Archiv Validierung der Cloud-Tier-Konfiguration: Die angegebenen Account- und Bucket-Einstellungen wurden erfolgreich oder nicht erfolgreich validiert.	"AVCC: Archiv Validierung der Cloud-Tier-Konfiguration"
BROR	Bucket Read Only Request: Ein Bucket wurde in den schreibgeschützten Modus eingegeben oder beendet.	"BROR: Bucket Read Only Request"
CBSES	Objekt Send End: Die Quelleinheit hat einen Grid-Node zum Grid-Node-Datentransfer abgeschlossen.	"CBSE: Objekt Senden Ende"
CBRE	Empfang des Objekts: Die Zieleinheit hat einen Grid-Node zum Datentransfer des Grid-Node abgeschlossen.	"CBRE: Das Objekt erhält das Ende"
CGRR	Grid-übergreifende Replizierungsanforderung: StorageGRID hat einen Grid-übergreifenden Replizierungsvorgang versucht, um Objekte zwischen Buckets in einer Grid-Verbundverbindung zu replizieren.	"CGRR: Grid-übergreifende Replikationsanforderung"
EBDL	Löschen von leeren Buckets: Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, das alle Objekte löscht (es wurde ein leerer Bucket-Vorgang durchgeführt).	"EBDL: Leerer Bucket löschen"

Codieren	Beschreibung	Siehe
EBKR	Anforderung für leere Bucket: Ein Benutzer hat eine Anforderung gesendet, Leere Bucket ein- oder auszuschalten (d. h. Bucket-Objekte zu löschen oder das Löschen von Objekten zu stoppen).	"EBKR: Anforderung für leeren Bucket"
SCMT	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	"SCMT: Object Store Commit Request"
SREM	Objektspeicher Remove: Ein Inhaltsblock wurde von einem Grid-Knoten gelöscht und kann nicht mehr direkt angefordert werden.	"SREM: Objektspeicher Entfernen"

Client liest Audit-Meldungen

Client-Read-Audit-Meldungen werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Abrufen eines Objekts vorgibt.

Codieren	Beschreibung	Verwendet von	Siehe
S3SL	S3 Select-Anforderung: Protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Meldung kann Fehlermeldungen und Fehlercodedetails enthalten. Die Anforderung war möglicherweise nicht erfolgreich.	S3-Client	"S3SL: S3 Select Request"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SGET S3 ABRUFEN"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	S3-Client	"SHEA: S3 KOPF"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Container aufzulisten.	Swift Client	"WGET: Schneller ERHALTEN"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um das Vorhandensein eines Objekts oder Containers zu überprüfen.	Swift Client	"WHEA: Schneller KOPF"

Audit-Meldungen des Clients schreiben

Audit-Meldungen zu Clientschreibmeldungen werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Erstellen oder Ändern eines Objekts macht.

Codieren	Beschreibung	Verwendet von	Siehe
OVWR	Objekt-Überschreiben: Protokolliert eine Transaktion, um ein Objekt mit einem anderen Objekt zu überschreiben.	S3 und Swift Clients	"OVWR: Objektüberschreibung"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SDEL: S3 LÖSCHEN"
SPOS	S3 POST: Protokolliert eine erfolgreiche Transaktion zur Wiederherstellung eines Objekts aus AWS Glacier Storage in einem Cloud Storage Pool.	S3-Client	"SPOS: S3-BEITRAG"
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SPUT: S3 PUT"
SUPD	Aktualisierte S3 Metadaten: Protokolliert eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes Objekt oder Bucket.	S3-Client	"SUPD: S3-Metadaten wurden aktualisiert"
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	Swift Client	"WDEL: Swift LÖSCHEN"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Container zu erstellen.	Swift Client	"WPUT: Schnell AUSGEDRÜCKT"

Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API.

Codieren	Titel und Beschreibung der Nachricht	Siehe
MGAU	Management-API-Audit-Nachricht: Ein Protokoll von Benutzeranfragen.	"MGAU: Management-Audit-Nachricht"

Prüfmeldungen für den ILM-Betrieb

Die Audit-Meldungen der ILM-Audit-Kategorie werden für Ereignisse im Zusammenhang mit ILM-Vorgängen (Information Lifecycle Management) verwendet.

Codieren	Titel und Beschreibung der Nachricht	Siehe
IDEL	ILM-Initiated Delete: Diese Audit-Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.	"IDEL: ILM gestartet Löschen"
LKCU	Bereinigung Des Objekts Überschrieben. Diese Überwachungsmeldung wird erzeugt, wenn ein überschriebenes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	"LKCU: Objektbereinigung überschrieben"
ORLM	Erfüllt Objektregeln: Diese Überwachungsmeldung wird generiert, wenn Objektdaten gemäß den ILM-Regeln gespeichert werden.	"ORLM: Objektregeln erfüllt"

Referenz für Überwachungsmeldung

APCT: Löschen von Archiven aus der Cloud-Ebene

Diese Meldung wird erzeugt, wenn archivierte Objektdaten aus einem externen Storage-System gelöscht werden, das eine Verbindung zur StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den gelöschten Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte. Gibt immer 0 zurück.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Eindeutige Kennung (UUID) des Cloud-Tiers, aus dem das Objekt gelöscht wurde.

ARCB: Archiv Objekt abrufen beginnen

Diese Meldung wird erzeugt, wenn eine Anfrage zum Abrufen der archivierten

Objektdaten gestellt wird und der Abrufvorgang beginnt. Abrufanfragen werden sofort bearbeitet, können jedoch neu geordnet werden, um die Effizienz des Abrufs von linearen Medien wie z. B. Bandmedien zu verbessern.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivspeichersystem abgerufen werden soll.
RSLT	Ergebnis	Zeigt das Ergebnis des Speicherabrufs an. Aktuell definierter Wert ist: SUCS: Die Inhaltsanforderung wurde empfangen und zum Abruf in die Warteschlange gestellt.

Diese Überwachungsmeldung markiert den Zeitpunkt eines Archivabrufs. Damit können Sie die Nachricht mit einer entsprechenden ARCE-End-Nachricht abgleichen, um die Dauer des Archivabrufs zu bestimmen und ob der Vorgang erfolgreich war.

ARCE: Archiv Objekt abrufen Ende

Diese Meldung wird erzeugt, wenn ein Versuch des Archiv-Knotens, Objektdaten von einem externen Archivspeichersystem abzurufen, abgeschlossen wird. Wenn die Meldung erfolgreich ist, zeigt die Meldung an, dass die angeforderten Objektdaten vollständig aus dem Archivverzeichnis gelesen und erfolgreich verifiziert wurden. Nachdem die Objektdaten abgerufen und verifiziert wurden, werden sie an den anfragenden Service geliefert.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivspeichersystem abgerufen werden soll.
VLID	Volume-Kennung	Der Bezeichner des Volumes, auf dem die Daten archiviert wurden. Wenn kein Archivspeicherort für den Inhalt gefunden wird, wird eine Volume-ID von 0 zurückgegeben.
RSLT	Abrufergebnis	Der Abschlussstatus des Archivabrufs: <ul style="list-style-type: none"> • ERFOLGREICH • VRFL: Fehlgeschlagen (Objektverifizierung fehlgeschlagen) • ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar) • STORNO: Fehlgeschlagen (Abrufvorgang abgebrochen) • GERR: Fehlgeschlagen (allgemeiner Fehler)

Wenn Sie diese Nachricht mit der entsprechenden ARCB-Nachricht abstimmen, können Sie die Zeit angeben, die für den Archivabruf benötigt wurde. Diese Meldung gibt an, ob der Abruf erfolgreich war, und im Falle eines Fehlers die Ursache für das Abrufen des Inhaltsblocks.

ARCT: Archiv Abrufen aus Cloud-Tier

Diese Meldung wird generiert, wenn archivierte Objektdaten von einem externen Archiv-Storage-System abgerufen werden, das eine Verbindung mit der StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den abgerufenen Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte. Der Wert ist nur für erfolgreiche Abrufen genau.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Unique Identifier (UUID) des externen Archivspeichersystems.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

ARM: Archivobjekt Entfernen

Die Meldung „Archiv Objekt entfernen“ zeigt an, dass ein Inhaltsblock erfolgreich oder nicht erfolgreich von einem Archiv-Knoten gelöscht wurde. Wenn das Ergebnis erfolgreich ist, hat der Archivknoten das externe Archivspeichersystem erfolgreich darüber informiert, dass StorageGRID einen Objektspeicherort freigegeben hat. Ob das Objekt aus dem externen Archivspeichersystem entfernt wird, hängt vom Systemtyp und dessen Konfiguration ab.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivmediensystem abgerufen werden soll.
VLID	Volume-Kennung	Die Kennung des Volumes, auf dem die Objektdaten archiviert wurden.
RSLT	Ergebnis	Der Abschlussstatus des Löschvorgangs für das Archiv: <ul style="list-style-type: none">• ERFOLGREICH• ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar)• GERR: Fehlgeschlagen (allgemeiner Fehler)

ASCE: Archiv-Objektspeicher Ende

Diese Meldung zeigt an, dass das Schreiben eines Inhaltsblocks in ein externes Archiv-Speichersystem beendet ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die Kennung des Inhaltsblocks, der auf dem externen Archivspeichersystem gespeichert ist.
VLID	Volume-Kennung	Die eindeutige Kennung des Archiv-Volume, auf das die Objektdaten geschrieben werden.
VREN	Überprüfung Aktiviert	Zeigt an, ob eine Überprüfung für Inhaltsblöcke durchgeführt wird. Aktuell definierte Werte sind: <ul style="list-style-type: none">• VENA: Die Überprüfung ist aktiviert• VDSA: Die Überprüfung ist deaktiviert
MCLS	Management-Klasse	Eine Zeichenfolge, die die TSM-Managementklasse identifiziert, der der Inhaltsblock zugeordnet ist, falls zutreffend.
RSLT	Ergebnis	Zeigt das Ergebnis des Archivierungsvorgangs an. Aktuell definierte Werte sind: <ul style="list-style-type: none">• ERFOLGREICH (Archivierungsprozess erfolgreich)• OFFL: Fehlgeschlagen (Archivierung ist offline)• VRFL: Fehlgeschlagen (Objektüberprüfung fehlgeschlagen)• ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar)• GERR: Fehlgeschlagen (allgemeiner Fehler)

Diese Überwachungsmeldung bedeutet, dass der angegebene Inhaltsblock auf das externe Archivspeichersystem geschrieben wurde. Wenn der Schreibvorgang fehlschlägt, liefert das Ergebnis grundlegende Informationen zur Fehlerbehebung über den Fehlerort. Ausführlichere Informationen zu Archivfehlern finden Sie unter Untersuchung der Attribute von Archivierungs-Knoten im StorageGRID System.

ASCT: Archivspeicher Cloud-Tier

Diese Meldung wird generiert, wenn archivierte Objektdaten in einem externen Storage-System gespeichert werden, das eine Verbindung mit StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den abgerufenen Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Unique Identifier (UUID) des Cloud-Tiers, in dem der Inhalt gespeichert wurde.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

ATCE: Archiv-Objektspeicher beginnen

Diese Meldung weist darauf hin, dass das Schreiben eines Inhaltsblocks in einen externen Archivspeicher gestartet wurde.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des zu archivierenden Inhaltsblocks.
VLID	Volume-Kennung	Die eindeutige Kennung des Volumes, auf das der Inhaltsblock geschrieben wird. Wenn der Vorgang fehlschlägt, wird eine Volume-ID von 0 zurückgegeben.
RSLT	Ergebnis	Gibt das Ergebnis der Übertragung des Inhaltsblocks an. Aktuell definierte Werte sind: <ul style="list-style-type: none"> • ERFOLGREICH (Inhaltsblock erfolgreich gespeichert) • EXIS: Ignoriert (Inhaltsblock wurde bereits gespeichert) • ISFD: Fehlgeschlagen (nicht genügend Speicherplatz) • STER: Fehlgeschlagen (Fehler beim Speichern der CBID) • OFFL: Fehlgeschlagen (Archivierung ist offline) • GERR: Fehlgeschlagen (allgemeiner Fehler)

AVCC: Archiv Validierung der Cloud-Tier-Konfiguration

Diese Meldung wird generiert, wenn die Konfigurationseinstellungen für einen Cloud Tiering – Simple Storage Service (S3)-Zieltyp validiert werden.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	UUID, die dem validierten externen Archivspeichersystem zugeordnet ist.

BROR: Bucket Read Only Request

Der LDR-Service generiert diese Überwachungsmeldung, wenn ein Bucket in den schreibgeschützten Modus wechselt oder diesen beendet. Beispielsweise wechselt ein Bucket in den schreibgeschützten Modus, während alle Objekte gelöscht werden.

Codieren	Feld	Beschreibung
BKHD	Bucket-UUID	Die Bucket-ID.
BROV	Wert der schreibgeschützten Bucket-Anforderung	Gibt an, ob der Bucket schreibgeschützt ist oder den schreibgeschützten Status verlässt (1 = schreibgeschützt, 0 = nicht schreibgeschützt).
BROS	Grund für schreibgeschützten Bucket	Der Grund, warum der Bucket schreibgeschützt ist oder den schreibgeschützten Status verlässt. Beispiel: LeptyBucket.
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, das die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3 Bucket	Der S3-Bucket-Name

CBRB: Objekt empfangen beginnen

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn der Transfer eines Inhaltsblocks von einem Node zum anderen initiiert wird, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungs-kennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.

Codieren	Feld	Beschreibung
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikatanzahl verwendet werden.

CBRE: Das Objekt erhält das Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen abgeschlossen ist, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungsken- nung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsric- htung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.

Codieren	Feld	Beschreibung
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung wurde aufgrund des Empfangs von beschädigten oder ungültigen Daten beendet

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

CBSB: Objektsendebeginn

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen initiiert wird, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungs-kennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.

Codieren	Feld	Beschreibung
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikanzahl verwendet werden.

CBSE: Objekt Senden Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen abgeschlossen ist, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungsken- nung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.

Codieren	Feld	Beschreibung
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung wurde aufgrund des Empfangs von beschädigten oder ungültigen Daten beendet

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

CGRR: Grid-übergreifende Replikationsanforderung

Diese Meldung wird generiert, wenn StorageGRID versucht, Objekte zwischen Buckets in einer Grid-Federation-Verbindung in einem Grid-Replizierungsvorgang zu replizieren. Eine Audit-Meldung wird nur gesendet, wenn die Anforderung dauerhaft fehlgeschlagen

ist (ERGEBNIS GERR).

Codieren	Feld	Beschreibung
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, dem der Bucket gehört, von dem das Objekt repliziert wird.
GFID	Verbindungs-ID des Grid-Verbunds	Die ID der Grid-Verbundverbindung, die für die Grid-übergreifende Replizierung verwendet wird.
BETR.	CGR-Betrieb	Der Typ des Grid-übergreifenden Replikationsvorgangs, der versucht wurde: <ul style="list-style-type: none"> • 0 = Objekt replizieren • 1 = Mehrteiliges Objekt replizieren • 2 = Löschmarkierung replizieren
S3BK	S3 Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens.
VSID	Version-ID	Die Versions-ID der spezifischen Version eines Objekts, das repliziert wurde.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder allgemeinen Fehler (GERR) zurück.

EBDL: Leerer Bucket löschen

Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, das alle Objekte löscht (und einen leeren Bucket-Vorgang durchgeführt).

Codieren	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Byte.
PFAD	S3-Bucket/Key	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 im StorageGRID System.

Codieren	Feld	Beschreibung
RSLT	Ergebnis des Löschvorgangs	Das Ergebnis eines Ereignisses, Prozesses oder einer Transaktion. Wenn für eine Nachricht nicht relevant ist, WIRD KEINE verwendet, sondern SUCS, damit die Nachricht nicht versehentlich gefiltert wird.

EBKR: Anforderung für leeren Bucket

Diese Meldung zeigt an, dass ein Benutzer eine Anforderung zum ein- und Ausschalten von leeren Buckets gesendet hat (d. h. zum Löschen von Bucket-Objekten oder zum Beenden des Löschens von Objekten).

Codieren	Feld	Beschreibung
BUID	Bucket-UUID	Die Bucket-ID.
EBJS	Leere Bucket-JSON-Konfiguration	Enthält den JSON, der die aktuelle leere Bucket-Konfiguration darstellt.
S3AI	S3-Mandantenkonto-ID	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name

ECMC: Fehlendes Erasure coded Data Fragment

Diese Meldung zeigt an, dass das System ein fehlendes Datenfragment mit Löschungscode erkannt hat.

Codieren	Feld	Beschreibung
VCMC	VCS-ID	Der Name des VCS, der den fehlenden Teil enthält.
MCID	Block-ID	Der Bezeichner des fehlenden Fragments mit Löschungscode.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein obligatorisches Nachrichtenfeld, ist aber für diese bestimmte Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

ECOC: Korrupte, mit Erasure codierte Datenfragment

Diese Meldung zeigt an, dass das System ein korruptes Datenfragment mit Löschungscode erkannt hat.

Codieren	Feld	Beschreibung
VCCO	VCS-ID	Der Name des VCS, der den beschädigten Teil enthält.
VLID	Volume-ID	Das RangeDB-Volume, das das korrupte Fragment mit Löschungscode enthält.
CCID	Block-ID	Der Identifier des beschädigten Fragments zur Löschung.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein obligatorisches Nachrichtenfeld, ist aber für diese bestimmte Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

ETAF: Sicherheitsauthentifizierung fehlgeschlagen

Diese Meldung wird erzeugt, wenn ein Verbindungsversuch mit Transport Layer Security (TLS) fehlgeschlagen ist.

Codieren	Feld	Beschreibung
CNID	Verbindungsken- nung	Die eindeutige Systemkennung für die TCP/IP-Verbindung, über die die Authentifizierung fehlgeschlagen ist.
RUID	Benutzeridentität	Eine dienstabhängige Kennung, die die Identität des Remote-Benutzers darstellt.
RSLT	Ursachencode	Der Grund für den Fehler: SCNI: Sichere Verbindungseinrichtung fehlgeschlagen. CERM: Zertifikat fehlt. Zertifikat: Zertifikat war ungültig. CERE: Das Zertifikat ist abgelaufen. CERR: Zertifikat wurde widerrufen. CSGN: Die Zertifikatsignatur war ungültig. CSGU: Zertifikatssignator war unbekannt. UCRM: Benutzerkennungen fehlten. UCRI: Die Benutzeranmeldeinformationen waren ungültig. UCRU: Benutzeranmeldeinformationen wurden nicht zulässig. TOUT: Zeitüberschreitung bei der Authentifizierung.

Wenn eine Verbindung zu einem sicheren Service hergestellt wird, der TLS verwendet, werden die Anmeldeinformationen der Remote-Einheit mithilfe des TLS-Profiles und der zusätzlichen Logik, die in den Service integriert ist, überprüft. Wenn diese Authentifizierung aufgrund ungültiger, unerwarteter oder unzulässiger Zertifikate oder Anmeldeinformationen fehlschlägt, wird eine Überwachungsmeldung protokolliert. Dies ermöglicht Abfragen für nicht autorisierte Zugriffsversuche und andere sicherheitsrelevante Verbindungsprobleme.

Die Meldung kann dazu führen, dass eine Remoteeinheit eine falsche Konfiguration hat oder dass versucht wird, ungültige oder unzulässige Anmeldedaten für das System vorzulegen. Diese Überwachungsmeldung sollte überwacht werden, um Versuche zu erkennen, unbefugten Zugriff auf das System zu erlangen.

GNRG: GNDS Registrierung

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst Informationen über sich selbst im StorageGRID-System aktualisiert oder registriert hat.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: <ul style="list-style-type: none"> • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.
GNTTP	Gerätetyp	Der Gerätetyp des Grid-Knotens (z. B. BLDR für einen LDR-Dienst).
GNDV	Modellversion des Geräts	Der String, der die Gerätemodellversion des Grid-Knotens im DMDL-Bundle identifiziert.
GNGP	Gruppieren	Die Gruppe, zu der der Grid-Knoten gehört (im Zusammenhang mit Verbindungskosten und Service-Query-Ranking).
GNIA	IP-Adresse	Die IP-Adresse des Grid-Node.

Diese Meldung wird generiert, wenn ein Grid-Knoten seinen Eintrag im Grid-Knoten-Paket aktualisiert.

GNUR: GNDS Registrierung aufheben

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst nicht registrierte Informationen über sich selbst vom StorageGRID-System enthält.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: <ul style="list-style-type: none"> • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.

GTED: Grid Task beendet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst die Verarbeitung der angegebenen Rasteraufgabe abgeschlossen hat und die Aufgabe in die Tabelle „Historisch“ verschoben hat. Wenn es sich um SUCS, ABRT oder ROLF handelt, wird eine entsprechende Überwachungsmeldung für die mit Grid Task gestartete Aufgabe angezeigt. Die anderen Ergebnisse zeigen, dass die Verarbeitung dieser Grid-Aufgabe nie gestartet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Grid-Aufgabe über den gesamten Lebenszyklus. Hinweis: die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
RSLT	Ergebnis	Das endgültige Statusergebnis der Grid-Aufgabe: <ul style="list-style-type: none"> • SUCS: Die Grid-Aufgabe wurde erfolgreich abgeschlossen. • ABRT: Die Grid-Aufgabe wurde ohne Rollback-Fehler beendet. • ROLF: Die Grid-Aufgabe wurde beendet und konnte den Rollback-Vorgang nicht abschließen. • STORNO: Die Grid-Aufgabe wurde vom Benutzer vor dem Start abgebrochen. • EXPR: Der Grid-Task ist vor dem Start abgelaufen. • IVLD: Die Grid-Aufgabe war ungültig. • AUTH: Die Grid-Aufgabe war nicht zulässig. • DUPL: Die Grid-Aufgabe wurde als Duplikat abgelehnt.

GTST: Grid Task gestartet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst mit der Verarbeitung der angegebenen Grid-Aufgabe begonnen hat. Die Meldung „Audit“ folgt unmittelbar der Nachricht „Grid Task Submission Submitted“ für Grid-Aufgaben, die vom internen Grid Task Submission Service initiiert und für die automatische Aktivierung ausgewählt wurde. Für Grid-Aufgaben, die in die Tabelle „Ausstehend“ eingereicht werden, wird diese Meldung generiert, wenn der Benutzer die Grid-Aufgabe startet.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. Hinweis: die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
RSLT	Ergebnis	Das Ergebnis. Dieses Feld hat nur einen Wert: <ul style="list-style-type: none">• SUCS: Die Grid-Aufgabe wurde erfolgreich gestartet.

GTSU: Grid Task übermittelt

Diese Überwachungsmeldung zeigt an, dass eine Grid-Aufgabe an den CMN-Dienst gesendet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Identifiziert eindeutig eine generierte Grid-Aufgabe und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. Hinweis: die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
TTYP	Aufgabentyp	Der Typ der Rasteraufgabe.
TVER	Aufgabenversion	Eine Zahl, die die Version der Grid-Aufgabe angibt.
TDSC	Aufgabenbeschreibung	Eine vom Menschen lesbare Beschreibung der Grid-Aufgabe.

Codieren	Feld	Beschreibung
VATS	Gültig Nach Zeitstempel	Die früheste Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX-Zeit), zu der die Grid-Aufgabe gültig ist.
VBTS	Gültig Vor Zeitstempel	Die letzte Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX Zeit), zu der die Grid-Aufgabe gültig ist.
TSRC	Quelle	Die Quelle der Aufgabe: <ul style="list-style-type: none"> • TXTB: Die Grid-Aufgabe wurde über das StorageGRID-System als signierter Textblock gesendet. • GRID: Die Grid-Aufgabe wurde über den internen Grid Task Submit Service übermittelt.
ACTV	Aktivierungstyp	Die Art der Aktivierung: <ul style="list-style-type: none"> • AUTO: Die Grid-Aufgabe wurde zur automatischen Aktivierung eingereicht. • PEND: Die Grid-Aufgabe wurde in die ausstehende Tabelle übermittelt. Dies ist die einzige Möglichkeit für die TXTB-Quelle.
RSLT	Ergebnis	Das Ergebnis der Einreichung: <ul style="list-style-type: none"> • SUCS: Die Grid-Aufgabe wurde erfolgreich übermittelt. • FAIL: Die Aufgabe wurde direkt in die historische Tabelle verschoben.

IDEL: ILM gestartet Löschen

Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.

Die IDEL-Nachricht wird in einer der folgenden Situationen erzeugt:

- **Für Objekte in konformen S3-Buckets:** Diese Meldung wird generiert, wenn ILM den Prozess des automatischen Löschens eines Objekts startet, da der Aufbewahrungszeitraum abgelaufen ist (vorausgesetzt, die Einstellung zum automatischen Löschen ist aktiviert und die Legal Hold ist deaktiviert).
- **Für Objekte in nicht konformen S3 Buckets oder Swift Containern.** Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet, da derzeit keine Platzierungsanweisungen in der aktiven ILM-Richtlinie für das Objekt gelten.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.

Codieren	Feld	Beschreibung
CMPA	Compliance: Automatisches Löschen	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true) geben an, ob ein konformes Objekt automatisch gelöscht werden soll, wenn der Aufbewahrungszeitraum endet, es sei denn, der Bucket befindet sich unter einer gesetzlichen Aufbewahrungspflichten.
CMPL	Einhaltung: Gesetzliche Aufbewahrungspflichten	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true), die angeben, ob der Bucket derzeit unter einer gesetzlichen Aufbewahrungspflichten steht.
CMPR	Compliance: Aufbewahrungszeitraum	Nur für Objekte in S3-konformen Buckets. Die Länge der Aufbewahrungsdauer des Objekts in Minuten.
CTME	Compliance: Aufnahmezeit	Nur für Objekte in S3-konformen Buckets. Die Aufnahmezeit des Objekts. Sie können den Aufbewahrungszeitraum in Minuten zu diesem Wert hinzufügen, um zu bestimmen, wann das Objekt aus dem Bucket gelöscht werden kann.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschermarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde Vorgänge in Buckets enthalten dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
STANDORT	Standorte	Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht). CLEC: Für Objekte mit Erasure-Coding-Verfahren, die Profil-ID für das Erasure-Coding-Verfahren und die Gruppen-ID für das Erasure-Coding-Verfahren, die auf die Daten des Objekts angewendet werden. CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts. CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.

Codieren	Feld	Beschreibung
REGEL	Regelbezeichnung	<ul style="list-style-type: none"> • Wenn ein Objekt in einem konformen S3-Bucket automatisch gelöscht wird, weil der Aufbewahrungszeitraum abgelaufen ist, ist dieses Feld leer. • Wenn das Objekt gelöscht wird, da derzeit keine Anweisungen zur Platzierung für das Objekt vorhanden sind, zeigt dieses Feld den vom Menschen lesbaren Namen der letzten ILM-Regel an, die auf das Objekt angewendet wurde.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

LKCU: Objektbereinigung überschrieben

Diese Meldung wird generiert, wenn StorageGRID ein überschriebenes Objekt entfernt, das zuvor zur Freigabe von Speicherplatz erforderlich war. Ein Objekt wird überschrieben, wenn ein S3- oder Swift-Client ein Objekt in einen Pfad schreibt, der bereits ein Objekt enthält. Die Entfernung erfolgt automatisch und im Hintergrund.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
LTYP	Art der Bereinigung	<i>Nur zur internen Verwendung.</i>
LUID	Objekt-UUID entfernt	Die Kennung des entfernten Objekts.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.

Codieren	Feld	Beschreibung
UUID	Universell Eindeutige Kennung	Die Kennung des noch vorhandenen Objekts. Dieser Wert ist nur verfügbar, wenn das Objekt nicht gelöscht wurde.

LLST: Standort verloren

Diese Meldung wird immer dann generiert, wenn ein Speicherort für eine Objektkopie (repliziert oder Erasure Coded) nicht gefunden werden kann.

Codieren	Feld	Beschreibung
CBIL	CBID	Die betroffene CBID.
ECPR	Verfahren Zur Einhaltung Von Datenkonsistenz	Für Erasure-Coding-Objektdaten. Die ID des verwendeten Erasure Coding-Profiles.
LTYP	Positionstyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für Erasure-codierte Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
PCLD	Pfad zu repliziertem Objekt	Der vollständige Pfad zum Speicherort der verlorenen Objektdaten. Wird nur zurückgegeben, wenn LTYP einen Wert von CLDI (d.h. für replizierte Objekte) hat. Nimmt das Formular an <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
RSLT	Ergebnis	Immer KEINE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.
TSRC	Auslösequelle	BENUTZER: Benutzer ausgelöst SYST: System ausgelöst
UUID	Universally Unique ID	Die Kennung des betroffenen Objekts im StorageGRID-System.

MGAU: Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API. Jede Anfrage, die keine GET- oder HEAD-Anforderung an die API ist, protokolliert eine Antwort

mit dem Benutzernamen, der IP und der Art der Anfrage an die API.

Codieren	Feld	Beschreibung
MDIP	Ziel-IP-Adresse	Die IP-Adresse des Servers (Ziel).
MDNA	Domain-Name	Der Host-Domain-Name.
MPAT	AnfraPfad	Der Anfraspfad.
MPQP	Abfrageparameter anfordern	Die Abfrageparameter für die Anforderung.
MRBD	Text anfordern	<p>Der Inhalt des Anforderungsinstanz. Während der Antwortkörper standardmäßig protokolliert wird, wird der Anforderungskörper in bestimmten Fällen protokolliert, wenn der Antwortkörper leer ist. Da die folgenden Informationen im Antwortkörper nicht verfügbar sind, werden sie von der Anforderungsstelle für die folgenden POST-Methoden übernommen:</p> <ul style="list-style-type: none"> • Benutzername und Konto-ID in POST authorize • Neue Subnetze-Konfiguration in POST /Grid/Grid-Networks/Update • Neue NTP-Server in POST /grid/ntp-Servers/Update • Ausgemusterte Server-IDs in POST /Grid/Servers/Decommission <p>Hinweis: sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.</p>
MRMD	Anforderungsmethode	<p>Die HTTP-Anforderungsmethode:</p> <ul style="list-style-type: none"> • POST • PUT • Löschen • PATCH
MRSC	Antwortcode	Der Antwortcode.
MRSP	Antwortkörper	<p>Der Inhalt der Antwort (der Antwortkörper) wird standardmäßig protokolliert.</p> <p>Hinweis: sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.</p>
MSIP	Quell-IP-Adresse	Die Client (Quell-) IP-Adresse.

Codieren	Feld	Beschreibung
MUUN	User-URN	Der URN (einheitlicher Ressourcenname) des Benutzers, der die Anforderung gesendet hat.
RSLT	Ergebnis	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.

OLST: System hat Lost Object erkannt

Diese Meldung wird generiert, wenn der DDS-Dienst keine Kopien eines Objekts im StorageGRID-System finden kann.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des verlorenen Objekts.
NID	Node-ID	Falls verfügbar, die letzte bekannte direkte oder Nearline-Position des verlorenen Objekts. Es ist möglich, nur die Knoten-ID ohne eine Volume-ID zu haben, wenn die Volume-Informationen nicht verfügbar sind.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Falls verfügbar: Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.
UUID	Universally Unique ID	Die Kennung des verlorenen Objekts im StorageGRID System.
VOLI	Volume-ID	Falls verfügbar, die Volume-ID des Speicherknoten oder Archiv-Knotens für den letzten bekannten Speicherort des verlorenen Objekts.

ORLM: Objektregeln erfüllt

Diese Meldung wird generiert, wenn das Objekt erfolgreich gespeichert und wie durch die ILM-Regeln festgelegt kopiert wird.



Die ORLM-Meldung wird nicht generiert, wenn ein Objekt erfolgreich mit der Regel 2 Kopien erstellen gespeichert wird, wenn eine andere Regel in der Richtlinie den erweiterten Filter Objektgröße verwendet.

Codieren	Feld	Beschreibung
BUID	Bucket-Header	Bucket-ID-Feld Wird für interne Vorgänge verwendet. Wird nur angezeigt, wenn STAT PRGD ist.
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
STANDORT	Standorte	<p>Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht).</p> <p>CLEC: Für Objekte mit Erasure-Coding-Verfahren, die Profil-ID für das Erasure-Coding-Verfahren und die Gruppen-ID für das Erasure-Coding-Verfahren, die auf die Daten des Objekts angewendet werden.</p> <p>CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts.</p> <p>CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.</p>
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
RSLT	Ergebnis	<p>Das Ergebnis des ILM-Vorgangs.</p> <p>SUCS: Der ILM-Vorgang war erfolgreich.</p>
REGEL	Regelbezeichnung	Das von Menschen lesbare Etikett, das der ILM-Regel gegeben wurde, die auf dieses Objekt angewendet wurde.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
SGCB	Container-CBID	CBID des Containers für das segmentierte Objekt. Dieser Wert ist nur für segmentierte und mehrteilige Objekte verfügbar.

Codieren	Feld	Beschreibung
STAT	Status	Der Status des ILM-Betriebs. FERTIG: ILM-Vorgänge für das Objekt wurden abgeschlossen. DFER: Das Objekt wurde für zukünftige ILM-Neuevaluierungen markiert. PRGD: Das Objekt wurde aus dem StorageGRID-System gelöscht. NLOC: Die Objektdaten können nicht mehr im StorageGRID-System gefunden werden. Dieser Status kann darauf hinweisen, dass alle Kopien von Objektdaten fehlen oder beschädigt sind.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Versionsnummer eines neuen Objekts, das in einem versionierten Bucket erstellt wurde Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

Die ORLM-Überwachungsmeldung kann für ein einzelnes Objekt mehr als einmal ausgegeben werden. Sie wird beispielsweise immer dann ausgegeben, wenn eines der folgenden Ereignisse eintritt:

- ILM-Regeln für das Objekt sind dauerhaft erfüllt.
- ILM-Regeln für das Objekt werden für diese Epoche erfüllt.
- Das Objekt wurde durch ILM-Regeln gelöscht.
- Bei der Hintergrundüberprüfung wird erkannt, dass eine Kopie replizierter Objektdaten beschädigt ist. Das StorageGRID System führt eine ILM-Bewertung durch, um das beschädigte Objekt zu ersetzen.

Verwandte Informationen

- ["Objektaufnahme von Transaktionen"](#)
- ["Löschen von Objekttransaktionen"](#)

OVWR: Objektüberschreibung

Diese Meldung wird erzeugt, wenn ein externer (Client-angeforderter) Vorgang ein Objekt durch ein anderes Objekt überschrieben.

Codieren	Feld	Beschreibung
CBID	Kennung für Inhaltsblock (neu)	Die CBID für das neue Objekt.
CSIZ	Vorherige Objektgröße	Die Größe des Objekts in Byte, das überschrieben wird.

Codieren	Feld	Beschreibung
OCBD	Kennung für Inhaltsblock (vorherige)	Die CBID für das vorherige Objekt.
UUID	Universally Unique ID (neu)	Die Kennung des neuen Objekts im StorageGRID System.
OUID	Universally Unique ID (vorherige)	Die Kennung für das vorherige Objekt innerhalb des StorageGRID-Systems.
PFAD	S3 oder Swift Objektpfad	Der S3- oder Swift-Objektpfad wird sowohl für das vorherige als auch für das neue Objekt verwendet
RSLT	Ergebniscode	Ergebnis der Transaktion Objekt überschreiben. Das Ergebnis ist immer: ERFOLGREICH
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das überschreibende Objekt am angegebenen Standort gelöscht, was nicht der Standort ist, an dem das überschreibende Objekt aufgenommen wurde.

S3SL: S3 Select Request

Diese Meldung protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Meldung kann Fehlermeldungen und Fehlercodedetails enthalten. Die Anforderung war möglicherweise nicht erfolgreich.

Codieren	Feld	Beschreibung
BYSC	Gescannte Bytes	Anzahl der von Speicherknoten gescannten (empfangenen) Bytes. BYSC und BYPR unterscheiden sich wahrscheinlich, wenn das Objekt komprimiert wird. Wenn das Objekt komprimiert ist, hätte BYSC die komprimierte Byte-Anzahl und BYPR wären die Bytes nach der Dekomprimierung.
BYPR	Verarbeitete Byte	Anzahl der verarbeiteten Bytes. Gibt an, wie viele Byte „gescannte Bytes“ tatsächlich von einem S3 Select-Job verarbeitet oder bearbeitet wurden.
BYRT	Bytes Zurückgegeben	Anzahl der Bytes, die ein S3 Select-Job an den Client zurückgegeben hat.
REPR	Datensätze Verarbeitet	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job von Storage-Nodes empfangen hat.

Codieren	Feld	Beschreibung
RERT	Datensätze Zurückgegeben	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job an den Client zurückgegeben hat.
JOFI	Job Abgeschlossen	Zeigt an, ob die Verarbeitung des S3 Select-Jobs abgeschlossen ist oder nicht. Wenn dies falsch ist, konnte der Job nicht abgeschlossen werden, und die Fehlerfelder enthalten wahrscheinlich Daten. Der Kunde hat möglicherweise Teilergebnisse oder gar keine Ergebnisse erhalten.
REID	Anforderung-ID	Kennung für die S3-Select-Anforderung.
EXTM	Ausführungszeit	Die Zeit in Sekunden, die für den Abschluss des S3 Select Jobs benötigt wurde.
FEHLER	Fehlermeldung	Fehlermeldung, die der S3 Select-Job generiert hat.
ERY	Fehlertyp	Fehlertyp, den der S3 Select-Job generiert hat.
ERST	Fehler Bei Stacktrace	Fehler bei Stacktrace, den der S3 Select-Job generiert hat.
S3BK	S3 Bucket	Der S3-Bucket-Name
S3AK	S3 Access Key ID (Absender anfordern)	Die S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat.
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens.

SADD: Security Audit deaktiviert

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung der Überwachungsmeldungen deaktiviert hat; Audit-Meldungen werden nicht mehr erfasst oder geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, mit der das Audit deaktiviert wird.

Codieren	Feld	Beschreibung
AEUN	Benutzername	Der Benutzername, der den Befehl zum Deaktivieren der Revisionsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Meldung besagt, dass die Protokollierung zuvor aktiviert, aber jetzt deaktiviert wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt (SADE) und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SADE: Sicherheits-Audit aktivieren

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung von Überwachungsmeldungen wiederhergestellt hat; Audit-Meldungen werden erneut erfasst und geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, die zum Aktivieren des Audits verwendet wird.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Aktivieren der Audit-Protokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Nachricht bedeutet, dass die Protokollierung vorher deaktiviert (SADD) war, aber jetzt wiederhergestellt wurde. Dies wird in der Regel nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SCMT: Objekt Store Commit

Grid-Inhalte werden erst dann zur Verfügung gestellt oder als gespeichert erkannt, wenn sie bereitgestellt wurden (was bedeutet, dass sie dauerhaft gespeichert wurden). Dauerhaft gespeicherte Inhalte wurden vollständig auf Festplatte geschrieben und haben entsprechende Integritätsprüfungen bestanden. Diese Meldung wird ausgegeben, wenn ein Inhaltsblock auf den Speicher gesetzt wird.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der zu permanentem Speicher verpflichtet ist.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Status zum Zeitpunkt, zu dem das Objekt auf Festplatte gespeichert wurde: SUCS: Objekt erfolgreich gespeichert.

Diese Meldung bedeutet, dass ein bestimmter Inhaltsblock vollständig gespeichert und überprüft wurde und nun angefordert werden kann. Er kann zur Nachverfolgung des Datenflusses im System eingesetzt werden.

SDEL: S3 LÖSCHEN

Wenn ein S3-Client eine LÖSCHTRANSAKTION ausgibt, wird eine Anforderung ausgeführt, das angegebene Objekt oder Bucket zu entfernen oder eine Bucket/Objekt-Unterressource zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungs-kennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschemarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde. Vorgänge in Buckets enthalten dieses Feld nicht.
GFID	Verbindungs-ID der Grid-Verbindung	Die Verbindungs-ID der Grid-Verbundverbindung, die einer Grid-übergreifenden Löschanforderung für die Replikation zugeordnet ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation Source Account ID	Die Konto-ID des Mandanten im Quellraster für eine Grid-übergreifende Löschanforderung für die Replikation. Nur in Prüfprotokollen im Zielraster enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	<p>Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p><code>`X-Forwarded-For`</code> Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der <code>`X-Forwarded-For`</code> Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</p> </div> <p><code>x-amz-bypass-governance-retention</code> Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist.</p>
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der LÖSCHAKTION. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkonto name (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.

Codieren	Feld	Beschreibung
SBAC	S3-Mandantenkonto name (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SGET S3 ABRUFEN

Wenn ein S3-Client eine GET-Transaktion ausgibt, wird eine Anforderung gestellt, ein Objekt abzurufen, die Objekte in einem Bucket aufzulisten oder eine Bucket/Objektunterressource zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.

Codieren	Feld	Beschreibung
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungsbezeichnung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
HTRH	HTTP-Anforderungskopf	<p>Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der <code>`X-Forwarded-For`</code> Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</p> </div>
KLINGELTE	Bereichsleser	Nur für Bereichslesevorgänge. Gibt den Bereich der Bytes an, die von dieser Anforderung gelesen wurden. Der Wert nach dem Schrägstrich (/) zeigt die Größe des gesamten Objekts an.
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkonto name (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkonto name (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: urn:sgws:identity::03393893651506583485:root Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SHEA: S3 KOPF

Wenn ein S3-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, ob es sich um ein Objekt oder einen Bucket handelt und die Metadaten zu einem Objekt abzurufen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CNID	Verbindungsken- nung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des überprüften Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
HTRH	HTTP- Anforderungsko- pf	<p>Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der <code>`X-Forwarded-For`</code> Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</p> </div>
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3- Mandantenkonto- ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
SACC	S3- Mandantenkonto name (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.

Codieren	Feld	Beschreibung
SBAC	S3-Mandantenkonto name (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SPOS: S3-BEITRAG

Wenn ein S3-Client eine POST Object-Anforderung ausgibt, wird diese Meldung vom Server ausgegeben, wenn die Transaktion erfolgreich durchgeführt wurde.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.

Codieren	Feld	Beschreibung
CNID	Verbindungsken- nung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte.
HTRH	HTTP- Anforderungsko- pf	<p>Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre>`X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</pre> </div> <p>(Nicht erwartet für SPOS).</p>
RSLT	Ergebniscode	<p>Ergebnis der Anforderung ZUR Wiederherstellung DES POSTOBJEKTS. Das Ergebnis ist immer:</p> <p>ERFOLGREICH</p>
S3AI	S3- Mandantenkonto- ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3- Unterressource	<p>Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend</p> <p>Für einen S3-Select-Vorgang auf „select“ setzen.</p>
SACC	S3- Mandantenkonto name (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.

Codieren	Feld	Beschreibung
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkonto name (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Stellen Sie Informationen wieder her.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SPUT: S3 PUT

Wenn ein S3-Client eine PUT-Transaktion ausgibt, wird eine Anforderung gestellt, ein neues Objekt oder einen Bucket zu erstellen oder eine Bucket/Objekt-Unterressource zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CMPS	Compliance-Einstellungen	Die beim Erstellen des Buckets verwendeten Compliance-Einstellungen, sofern diese in DER PUT Bucket-Anforderung vorhanden sind (abgeschnitten auf die ersten 1024 Zeichen).
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungs-kennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
GFID	Verbindungs-ID der Grid-Verbindung	Die Verbindungs-ID der Grid-Verbundverbindung, die einer Grid-übergreifenden REPLIKATIONSANFORDERUNG ZUGEORDNET ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation Source Account ID	Die Konto-ID des Mandanten im Quellraster für eine Grid-übergreifende Replikations-PUT-Anforderung. Nur in Prüfprotokollen im Zielraster enthalten.
HTRH	HTTP-Anforderungskopf	<p>Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p><code>`X-Forwarded-For`</code> Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der <code>`X-Forwarded-For`</code> Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</p> </div> <p><code>x-amz-bypass-governance-retention</code> Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist.</p>
LKEN	Objektsperre Aktiviert	Der Wert der Anfrageüberschrift <code>x-amz-bucket-object-lock-enabled</code> , Wenn vorhanden in DER PUT Bucket Anforderung.
LKLH	Gesetzliche Sperren Für Objekte	Der Wert der Anfrageüberschrift <code>x-amz-object-lock-legal-hold</code> , Wenn vorhanden in DER PUT-Objekt-Anforderung.

Codieren	Feld	Beschreibung
LKMD	Aufbewahrungsmodus Für Objektsperre	Der Wert der Anfrageüberschrift <code>x-amz-object-lock-mode</code> , Wenn vorhanden in DER PUT-Objekt-Anforderung.
LKRU	Objektsperre Bis Datum Beibehalten	Der Wert der Anfrageüberschrift <code>x-amz-object-lock-retain-until-date</code> , Wenn vorhanden in DER PUT-Objekt-Anforderung.
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkonto name (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkonto name (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.

Codieren	Feld	Beschreibung
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Die neue Subressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
ULID	Upload-ID	Nur in SPUT-Nachrichten für komplette mehrteilige Uploadvorgänge enthalten. Zeigt an, dass alle Teile hochgeladen und zusammengesetzt wurden.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Versionsnummer eines neuen Objekts, das in einem versionierten Bucket erstellt wurde Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.
VSST	Status Der Versionierung	Der neue Versionierungs-Status eines Buckets. Es werden zwei Zustände verwendet: "Aktiviert" oder "ausgesetzt". Operationen für Objekte enthalten dieses Feld nicht.

SREM: Objektspeicher Entfernen

Diese Meldung wird ausgegeben, wenn Inhalte aus einem persistenten Storage entfernt werden und nicht mehr über regelmäßige APIs zugänglich sind.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der aus dem permanenten Speicher gelöscht wurde.
RSLT	Ergebniscode	Gibt das Ergebnis der Aktionen zum Entfernen von Inhalten an. Der einzige definierte Wert ist: SUCS: Inhalt aus persistentem Storage entfernt

Diese Überwachungsmeldung bedeutet, dass ein bestimmter Inhaltsblock von einem Knoten gelöscht wurde und nicht mehr direkt angefordert werden kann. Die Nachricht kann verwendet werden, um den Fluss gelöschter Inhalte innerhalb des Systems zu verfolgen.

SUPD: S3-Metadaten wurden 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 Metadatenaktualisierung erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert des HTTP-Anfrageheaders Consistency-Control, falls in der Anfrage vorhanden, beim Aktualisieren der Compliance-Einstellungen eines Buckets.
CNID	Verbindungs-kennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <pre>`X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</pre> </div>

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
SACC	S3-Mandantenkonto name (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkonto name (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

Codieren	Feld	Beschreibung
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Versionsnummer der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SVRF: Objektspeicherüberprüfung fehlgeschlagen

Diese Meldung wird ausgegeben, wenn ein Inhaltsblock den Verifizierungsprozess nicht erfolgreich durchführt. Jedes Mal, wenn replizierte Objektdaten von der Festplatte gelesen oder auf die Festplatte geschrieben werden, werden verschiedene Verifizierungsprüfungen durchgeführt, um sicherzustellen, dass die an den anfordernden Benutzer gesendeten Daten mit den ursprünglich im System aufgenommenen Daten identisch sind. Wenn eine dieser Prüfungen fehlschlägt, werden die beschädigten replizierten Objektdaten vom System automatisch gesperrt, um ein erneutes Abrufen der Daten zu verhindern.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, bei der die Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	<p>Fehlertyp Verifikation:</p> <p>CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen.</p> <p>HMAC: Prüfung des Hashbasierten Nachrichtenauthentifizierungscodes (HMAC) fehlgeschlagen.</p> <p>EHS: Unerwarteter verschlüsselter Content-Hash.</p> <p>PHS: Unerwarteter Originalinhalt Hash.</p> <p>SEQC: Falsche Datensequenz auf der Festplatte.</p> <p>PERR: Ungültige Struktur der Festplattendatei.</p> <p>DERR: Festplattenfehler.</p> <p>FNAM: Ungültiger Dateiname.</p>



Diese Meldung sollte genau überwacht werden. Fehler bei der Inhaltsüberprüfung können auf drohende Hardwareausfälle hinweisen.

Um zu bestimmen, welcher Vorgang die Meldung ausgelöst hat, lesen Sie den Wert des FELDS AMID (Modul-ID). Beispielsweise gibt ein SVFY-Wert an, dass die Meldung vom Storage Verifier-Modul generiert wurde, d. h. eine Hintergrundüberprüfung und STOR zeigt an, dass die Meldung durch den Abruf von Inhalten ausgelöst wurde.

SVRU: Objektspeicher überprüfen Unbekannt

Die Storage-Komponente des LDR-Service scannt kontinuierlich alle Kopien replizierter Objektdaten im Objektspeicher. Diese Meldung wird ausgegeben, wenn eine unbekannte oder unerwartete Kopie replizierter Objektdaten im Objektspeicher erkannt und in das Quarantäneverzeichnis verschoben wird.

Codieren	Feld	Beschreibung
FPTH	Dateipfad	Dateipfad der unerwarteten Objektkopie.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.



Die Meldung SVRU: Object Store Verify Unknown Audit sollte genau überwacht werden. Es bedeutet, dass im Objektspeicher unerwartete Kopien von Objektdaten erkannt wurden. Diese Situation sollte sofort untersucht werden, um festzustellen, wie diese Kopien erstellt wurden, da sie auf drohende Hardwareausfälle hinweisen können.

SYSD: Knoten stoppen

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde. Normalerweise wird diese Meldung erst nach einem anschließenden Neustart gesendet, da die Warteschlange für Überwachungsmeldungen vor dem Herunterfahren nicht gelöscht wird. Suchen Sie nach der SYST-Meldung, die zu Beginn der Abschaltsequenz gesendet wird, wenn der Dienst nicht neu gestartet wurde.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Die RSLT eines SYSD kann nicht auf ein „schmutziges“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYST: Knoten wird angehalten

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde und dass der Dienst seine Abschaltsequenz initiiert hat. SYST kann verwendet werden, um festzustellen, ob das Herunterfahren angefordert wurde, bevor der Dienst neu gestartet wird (im Gegensatz zu SYSD, das normalerweise nach dem Neustart des Dienstes gesendet wird).

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Der RSLT-Code einer SYST-Meldung kann nicht auf ein „schmutziges“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYSU: Knoten Start

Wenn ein Dienst neu gestartet wird, wird diese Meldung erzeugt, um anzugeben, ob die vorherige Abschaltung sauber (befehl) oder ungeordnet (unerwartet) war.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SUCS: Das System wurde sauber abgeschaltet. DSDN: Das System wurde nicht sauber heruntergefahren. VRGN: Das System wurde erstmals nach der Server-Installation (oder Neuinstallation) gestartet.

Die Meldung gibt nicht an, ob der Host-Server gestartet wurde, sondern nur der Reporting-Service. Diese Meldung kann verwendet werden, um:

- Diskontinuität im Prüfprotokoll erkennen.
- Ermitteln Sie, ob ein Service während des Betriebs ausfällt (da die verteilte Natur des StorageGRID Systems diese Fehler maskieren kann). Der Server Manager startet einen fehlgeschlagenen Dienst automatisch neu.

WDEL: Swift LÖSCHEN

Wenn ein Swift-Client eine LÖSCHTRANSAKTION ausgibt, wird eine Anfrage zum Entfernen des angegebenen Objekts oder Containers gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Containern enthalten dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Vorgänge in Containern enthalten dieses Feld nicht.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>`X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</pre> </div>
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der LÖSCHAKTION. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.

Codieren	Feld	Beschreibung
WOW	Swift Container	Der Swift-Containername.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Vorgänge in Containern enthalten dieses Feld nicht.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WGET: Schneller ERHALTEN

Wenn ein Swift-Client eine GET-Transaktion ausgibt, wird eine Anfrage gestellt, um ein Objekt abzurufen, die Objekte in einem Container aufzulisten oder die Container in einem Konto aufzulisten. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge auf Konten und Containern enthalten dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge auf Konten und Containern enthalten dieses Feld nicht.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der <code>`X-Forwarded-For`</code> Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</p> </div>
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

Codieren	Feld	Beschreibung
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername. Die Operationen auf Konten enthalten dieses Feld nicht.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Vorgänge auf Konten und Containern enthalten dieses Feld nicht.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WHEA: Schneller KOPF

Wenn ein Swift-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, ob ein Konto, Container oder Objekt vorhanden ist, und alle relevanten Metadaten abzurufen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge auf Konten und Containern enthalten dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge auf Konten und Containern enthalten dieses Feld nicht.
HTRH	HTTP-Anforderungskopf	<p>Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der <code>`X-Forwarded-For`</code> Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).</p> </div>

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der HAUPTTRANSAKTION. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername. Die Operationen auf Konten enthalten dieses Feld nicht.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Vorgänge auf Konten und Containern enthalten dieses Feld nicht.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WPUT: Schnell AUSGEDRÜCKT

Wenn ein Swift-Client eine PUT-Transaktion ausgibt, wird eine Anfrage zum Erstellen eines neuen Objekts oder Containers gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Containern enthalten dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge in Containern enthalten dieses Feld nicht.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit). </div>
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Vorgänge in Containern enthalten dieses Feld nicht.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

Wartung

Erweitern Sie Ihr Raster

Raster erweitern: Übersicht

Mithilfe dieser Anweisungen können Sie die Kapazität oder die Funktionen Ihres StorageGRID Systems erweitern, ohne den Betrieb des Systems zu unterbrechen.

Informationen zu diesen Anweisungen

Diese Anweisungen beschreiben die Durchführung einer StorageGRID Erweiterung zum Hinzufügen von Storage Volumes zu Storage-Nodes, zu einem vorhandenen Standort neue Grid-Nodes oder einen gesamten neuen Standort.

Diese Anweisungen gelten für technische Mitarbeiter, die nach der Installation für die Konfiguration und den Support des StorageGRID Systems verantwortlich sind.

Erweiterungs-Workflow

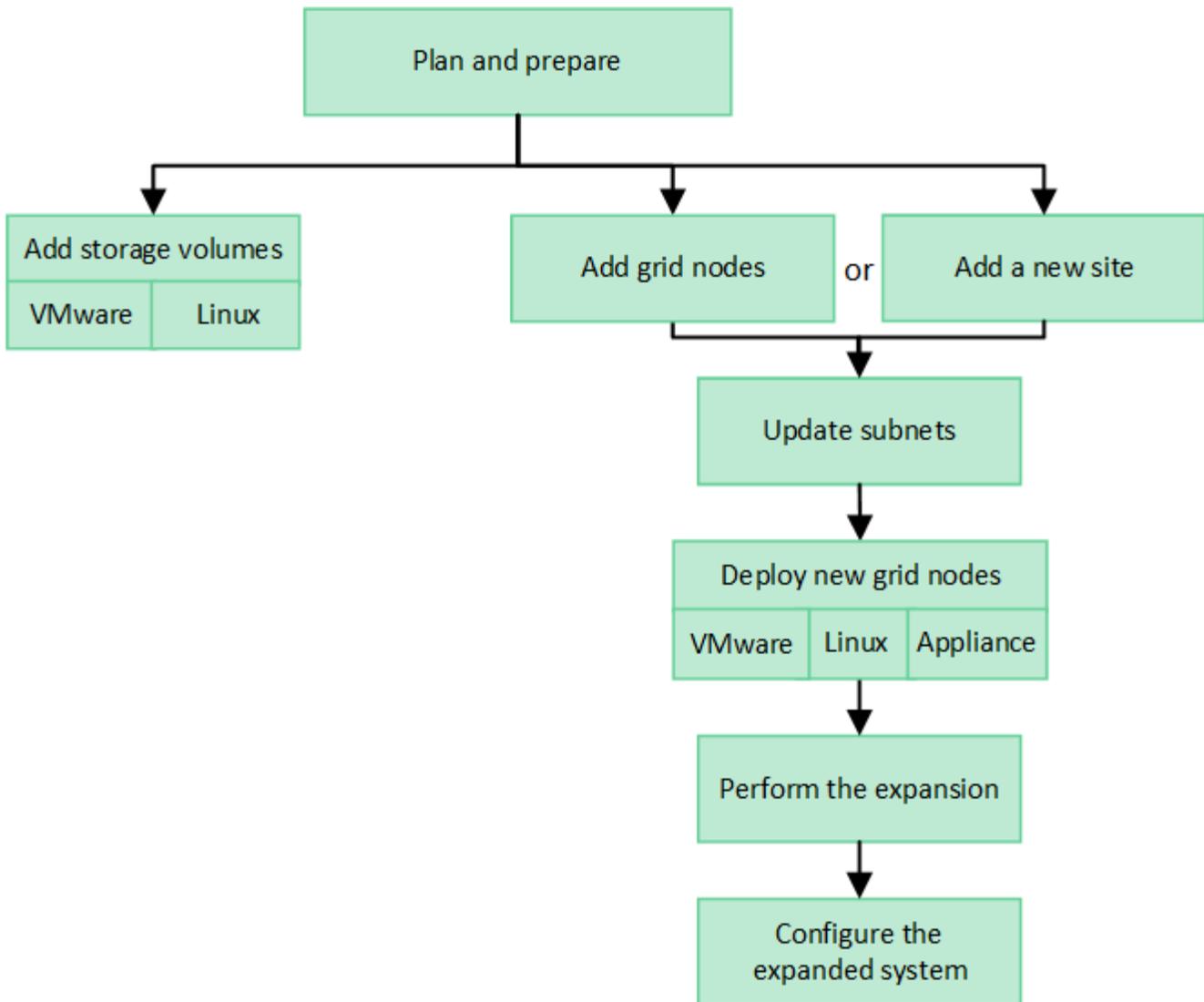
Der Grund für die Erweiterung ist ausschlaggebend dafür, wie viele neue Nodes jeden Typs Sie hinzufügen müssen, und Speicherort dieser neuen Nodes. Beispielsweise bestehen unterschiedliche Node-Anforderungen, wenn Sie eine Erweiterung zur Erhöhung der Storage-Kapazität, das Hinzufügen von Metadaten-Kapazität oder das Hinzufügen von Redundanz oder neuen Funktionen durchführen.

Wie im Workflow dargestellt, hängen die Schritte zur Durchführung einer Erweiterung davon ab, ob Sie Speichervolumes zu einem Speicher-Node hinzufügen, einem vorhandenen Standort neue Nodes hinzufügen oder einen neuen Standort hinzufügen. In allen Fällen können Sie die Erweiterung durchführen, ohne den Betrieb des aktuellen Systems zu unterbrechen.

Die Schritte zum Hinzufügen von Nodes hängen auch davon ab, ob Sie StorageGRID-Appliances oder Hosts mit VMware oder Linux hinzufügen.



„Linux“ bezieht sich auf eine Red hat® Enterprise Linux®, Ubuntu®, CentOS- oder Debian®-Bereitstellung. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um eine Liste der unterstützten Versionen zu erhalten.



Planen Sie eine Erweiterung von StorageGRID

Erweitern Sie Ihre Storage-Kapazität

Richtlinien zum Hinzufügen von Objektkapazität

Sie können die Objekt-Storage-Kapazität Ihres StorageGRID Systems erweitern, indem Sie vorhandenen Storage-Nodes Storage-Volumes hinzufügen oder vorhandenen Standorten neue Storage-Nodes hinzufügen. Storage-Kapazität muss so hinzugefügt werden, dass sie den Anforderungen Ihrer Information Lifecycle Management (ILM)-Richtlinie entspricht.

Richtlinien für das Hinzufügen von Storage Volumes

Lesen Sie vor dem Hinzufügen von Storage-Volumes zu vorhandenen Storage-Nodes die folgenden Richtlinien und Einschränkungen:

- Sie müssen Ihre aktuellen ILM-Regeln prüfen, um zu bestimmen, wo und wann Sie dies tun "[Storage-Volumes hinzufügen](#)" Um den verfügbaren Speicher für zu erhöhen "[Replizierte Objekte](#)" Oder "[Objekte, die mit Erasure Coding codiert wurden](#)".

- Die Metadatenkapazität des Systems kann nicht durch Hinzufügen von Storage-Volumes erhöht werden, da Objekt-Metadaten nur auf Volume 0 gespeichert werden.
- Jeder softwarebasierte Storage Node kann maximal 16 Storage Volumes unterstützen. Wenn Sie darüber hinaus Kapazität hinzufügen möchten, müssen Sie neue Storage-Nodes hinzufügen.
- Sie können jeder SG6060 Appliance ein oder zwei Erweiterungs-Shelfs hinzufügen. Mit jedem Erweiterungs-Shelf werden 16 Storage-Volumes hinzugefügt. Mit beiden installierten Erweiterungs-Shelfs kann das SG6060 insgesamt 48 Storage Volumes unterstützen.
- Storage Volumes können keiner anderen Storage Appliance hinzugefügt werden.
- Sie können die Größe eines vorhandenen Storage Volumes nicht vergrößern.
- Storage Volumes können nicht gleichzeitig zu einem Storage Node hinzugefügt werden, wenn Sie ein System-Upgrade, einen Wiederherstellungsvorgang oder eine andere Erweiterung durchführen.

Nachdem Sie sich entschieden haben, Storage Volumes hinzuzufügen und festgestellt haben, welche Storage Nodes Sie erweitern müssen, um Ihre ILM-Richtlinie zu erfüllen, befolgen Sie die Anweisungen für Ihren Storage Node-Typ:

- Wenn Sie einer SG6060 Storage-Appliance ein oder zwei Erweiterungseinschübe hinzufügen möchten, fahren Sie mit fort "[Erweiterungs-Shelf für das implementierte SG6060 hinzufügen](#)".
- Befolgen Sie die Anweisungen für für, um einen softwarebasierten Node zu erhalten "[Hinzufügen von Storage-Volumes zu Storage-Nodes](#)".

Richtlinien zum Hinzufügen von Speicherknoten

Lesen Sie vor dem Hinzufügen von Speicherknoten zu vorhandenen Standorten die folgenden Richtlinien und Einschränkungen durch:

- Sie müssen Ihre aktuellen ILM-Regeln prüfen, um zu bestimmen, wo und wann Storage-Nodes hinzugefügt werden müssen, um den verfügbaren Speicher zu vergrößern "[Replizierte Objekte](#)" Oder "[Objekte, die mit Erasure Coding codiert wurden](#)".
- Sie sollten nicht mehr als 10 Speicherknoten in einem einzigen Erweiterungsverfahren hinzufügen.
- Sie können Speicherknoten zu mehr als einem Standort in einem einzigen Erweiterungsverfahren hinzufügen.
- Sie können Storage-Nodes und andere Node-Typen in einem einzigen Erweiterungsverfahren hinzufügen.
- Bevor Sie mit dem Erweiterungsverfahren beginnen, müssen Sie bestätigen, dass alle Datenreparaturvorgänge, die im Rahmen einer Wiederherstellung durchgeführt werden, abgeschlossen sind. Siehe "[Prüfen Sie die Reparatur von Daten](#)".
- Wenn Sie Storage-Nodes vor oder nach einer Erweiterung entfernen müssen, sollten Sie nicht mehr als 10 Storage-Nodes in einem einzigen Dekommissions-Node-Verfahren außer Betrieb nehmen.

Richtlinien für ADC-Service auf Storage-Nodes

Beim Konfigurieren der Erweiterung müssen Sie festlegen, ob der Dienst Administrative Domain Controller (ADC) auf jedem neuen Speicherknoten enthalten soll. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services.

- Das StorageGRID System erfordert eine "[Quorum von ADC-Services](#)" Zu jeder Zeit und an jedem Standort verfügbar zu sein.
- Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten.

- Es wird nicht empfohlen, jedem Speicherknoten den ADC-Dienst hinzuzufügen. Die Einbeziehung von zu vielen ADC-Services kann zu Verlangsamungen führen, da die Kommunikation zwischen den Knoten größer ist.
- Ein einzelnes Grid sollte nicht mehr als 48 Storage-Nodes mit dem ADC-Dienst aufweisen. Dies entspricht 16 Standorten mit drei ADC-Diensten an jedem Standort.
- Wenn Sie im Allgemeinen die Einstellung **ADC-Dienst** für einen neuen Knoten auswählen, sollten Sie **automatisch** wählen. Wählen Sie **Ja** nur aus, wenn der neue Knoten einen anderen Speicherknoten ersetzt, der den ADC-Dienst enthält. Da ein Storage Node nicht stillgelegt werden kann, wenn zu wenige ADC-Dienste verbleiben, wird dadurch sichergestellt, dass ein neuer ADC-Service verfügbar ist, bevor der alte Service entfernt wird.
- Sie können den ADC-Dienst nicht zu einem Knoten hinzufügen, nachdem er bereitgestellt wurde.

Storage-Kapazitäten für replizierte Objekte hinzufügen

Wenn die Information Lifecycle Management-Richtlinie (ILM) für Ihre Implementierung eine Regel umfasst, die replizierte Kopien von Objekten erstellt, müssen Sie berücksichtigen, wie viel Storage hinzugefügt werden muss und wo die neuen Storage Volumes oder Storage-Nodes hinzugefügt werden müssen.

Anweisungen zum Hinzufügen von zusätzlichem Storage finden Sie in den ILM-Regeln, die replizierte Kopien erstellen. Wenn ILM-Regeln zwei oder mehr Objektkopien erstellen, planen Sie das Hinzufügen von Storage an jedem Speicherort, an dem Objektkopien erstellt werden. Wenn Ihnen beispielsweise ein Grid mit zwei Standorten und eine ILM-Regel zur Erstellung einer Objektkopie an jedem Standort zur Verfügung steht, müssen Sie dies unbedingt tun "[Fügen Sie Speicher hinzu](#)" Zu jedem Standort, um die Gesamtkapazität des Grids zu erhöhen. Informationen zur Objektreplikation finden Sie unter "[Was ist Replikation?](#)".

Aus Performance-Gründen sollten Sie versuchen, die Storage-Kapazität und die Rechenleistung über die Standorte hinweg gleichmäßig zu verteilen. In diesem Beispiel sollten Sie also jedem Standort die gleiche Anzahl an Storage-Nodes oder an jedem Standort zusätzliche Storage-Volumes hinzufügen.

Falls Sie eine komplexere ILM-Richtlinie haben, die Regeln enthält, die Objekte basierend auf Kriterien wie Bucket-Name oder Regeln, die Objektorte im Laufe der Zeit ändern, wird Ihre Analyse, wo Storage für die Erweiterung erforderlich ist, ähnlich, aber komplexer.

Wenn Sie verstehen, wie schnell die insgesamt genutzte Storage-Kapazität verbraucht wird, können Sie verstehen, wie viel Storage in der Erweiterung hinzugefügt werden muss und wann der zusätzliche Speicherplatz erforderlich ist. Sie können den Grid-Manager für verwenden "[Überwachen und graten Sie die Speicherkapazität](#)".

Denken Sie bei der Planung des Zeitpunkts einer Erweiterung daran, wie lange die Beschaffung und Installation von zusätzlichem Storage dauern könnte.

Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden

Wenn Ihre ILM-Richtlinie eine Regel zur Erstellung von Kopien zur Fehlerkorrektur enthält, müssen Sie planen, wo neuer Storage hinzugefügt werden muss und wann neuer Storage hinzugefügt werden muss. Die Menge des Hinzufügen von Speicherplatz und der Zeitpunkt der Hinzufügung können die nutzbare Speicherkapazität des Grid beeinflussen.

Der erste Schritt bei der Planung einer Storage-Erweiterung ist das untersuchen der Regeln in Ihrer ILM-

Richtlinie, die Objekte mit Erasure-Coding-Verfahren erstellt. Da StorageGRID für jedes Objekt, das mit Erasure-Coding-Verfahren codiert wurde, $k+m$ Fragmente erstellt und jedes Fragment auf einem anderen Storage-Node speichert, müssen Sie sicherstellen, dass mindestens $k+m$ Storage-Nodes nach der Erweiterung über Platz für neue Daten mit Erasure-Code verfügen. Wenn das Erasure Coding-Profil Site-Loss-Schutz bietet, müssen Sie jedem Standort Storage hinzufügen. Siehe ["Was sind Erasure Coding-Systeme?"](#) Um Informationen zu Profilen für das Erasure Coding zu erhalten.

Die Anzahl der Nodes, die Sie hinzufügen müssen, hängt auch davon ab, wie voll die vorhandenen Nodes sind, wenn Sie die Erweiterung durchführen.

Allgemeine Empfehlung für die Erweiterung der Storage-Kapazität für Objekte mit Erasure-Coding-Verfahren

Wenn detaillierte Berechnungen vermieden werden sollen, können Sie zwei Storage-Nodes pro Standort hinzufügen, wenn vorhandene Storage-Nodes eine Kapazität von 70 % erreichen.

Diese allgemeine Empfehlung liefert angemessene Ergebnisse für eine Vielzahl von Erasure Coding-Schemata für Grids an einem Standort und für Grids, bei denen ein Erasure Coding-Verfahren einen Site-Loss-Schutz bietet.

Informationen über die Faktoren, die zu dieser Empfehlung geführt haben, oder die Entwicklung eines genaueren Plans für Ihren Standort finden Sie unter ["Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind"](#). Für individuelle Empfehlungen, die auf Ihre Situation abgestimmt sind, wenden Sie sich an Ihren NetApp Professional Services Berater.

Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind

Wenn Sie eine Erweiterung zum Hinzufügen von Storage Nodes durchführen und ILM-Regeln zum Löschen von Code-Daten verwenden, müssen Sie möglicherweise das EC-Ausgleichs-Verfahren durchführen, wenn Sie nicht genügend Storage Nodes für das von Ihnen verwendete Erasure-Coding-Schema hinzufügen können.

Führen Sie die Erweiterung durch, und fahren Sie mit fort ["Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes"](#) Zum Ausführen des Verfahrens.

Was ist die Neuausrichtung der EG?

Bei der EC-Ausbalancierung handelt es sich um ein StorageGRID-Verfahren, das nach einer Erweiterung des Storage-Nodes erforderlich sein kann. Das Verfahren wird als Kommandozeilenskript vom primären Admin-Knoten ausgeführt. Beim Ausführen des EC-Ausgleichs verteilt StorageGRID Fragmente, die mit Löschvorgängen codiert wurden, auf die vorhandenen und die neu hinzugefügten Storage-Nodes an einem Standort.

Das EC-Ausgleichsverfahren:

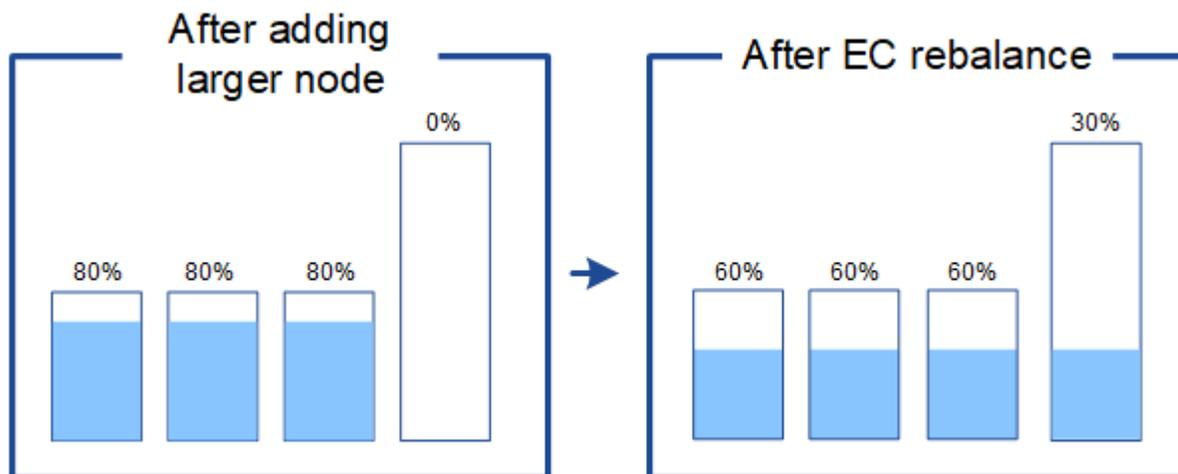
- Verschiebt nur Objektdaten, die Erasure Coding verwenden. Es werden keine replizierten Objektdaten verschoben.
- Verteilt die Daten an einem Standort neu. Es werden keine Daten zwischen Standorten verschoben.
- Verteilt Daten auf alle Storage-Nodes an einem Standort neu. Daten werden nicht innerhalb von Storage Volumes neu verteilt.
- Berücksichtigt nicht die Verwendung replizierter Daten auf jedem Storage Node bei der Festlegung, wo Daten mit Erasure Coding verschoben werden sollen.

- Verteilt Daten, die mit Erasure Coding codiert wurden, gleichmäßig zwischen Storage-Nodes, ohne die relativen Kapazitäten jedes Nodes zu berücksichtigen.
- Die Daten, die nach einer Erasure Coded codiert wurden, werden nicht an Storage-Nodes verteilt, die zu mehr als 70 % voll sind.
- Könnte die Performance von ILM-Vorgängen und S3- und Swift-Client-Operationen beeinträchtigen, wenn sie ausgeführt werden—zusätzliche Ressourcen sind erforderlich, um die Fragmente des Erasure-Coding neu zu verteilen.
- Bei Systemen mit einer sehr großen Anzahl von Objekten, die zur Fehlerkorrektur codiert wurden, muss eventuell mehr als einmal ausgeführt werden. Um die Ressourcennutzung zu begrenzen, ist die maximale Anzahl der Verschiebungen für jeden Job begrenzt.

Wenn das EC-Ausgleichsverfahren abgeschlossen ist:

- Daten, die mit Erasure coded werden, werden von Storage-Nodes mit weniger verfügbarem Speicherplatz auf Storage-Nodes mit mehr verfügbarem Speicherplatz verschoben.
- Die Datensicherung von Objekten, die mit Erasure Coding versehen sind, wird unverändert beibehalten.
- Die verwendeten (%) Werte können zwischen den Storage-Nodes aus zwei Gründen unterschiedlich sein:
 - Replizierte Objektkopien verbrauchen weiterhin Speicherplatz auf den vorhandenen Nodes—beim EC-Ausgleichsverfahren werden keine replizierten Daten verschoben.
 - Nodes mit höherer Kapazität sind relativ weniger voll als Nodes mit geringerer Kapazität, obwohl alle Nodes am Ende ungefähr das gleiche Volumen an Daten mit Erasure-Coded-Verfahren aufweisen.

Angenommen, drei 200-TB-Nodes werden jeweils zu 80 % gefüllt ($200 \times 0.8 = 160$ TB auf jedem Node oder 480 TB für den Standort). Wenn Sie einen 400-TB-Node hinzufügen und das Ausgleichsverfahren ausführen, verfügen alle Nodes nun über ungefähr die gleiche Menge an Daten aus dem Lösocode ($480/4 = 120$ TB). Der verwendete Wert (%) für den größeren Knoten ist jedoch kleiner als der verwendete Wert (%) für die kleineren Knoten.

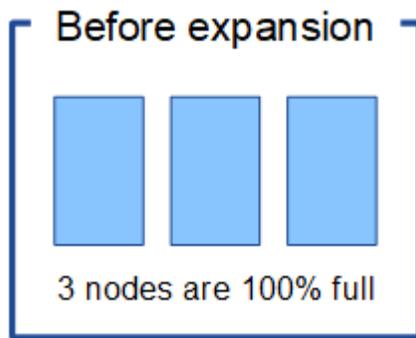


Zeitpunkt für den Ausgleich von Daten, die mit Erasure Coding codiert wurden

Betrachten wir das folgende Szenario:

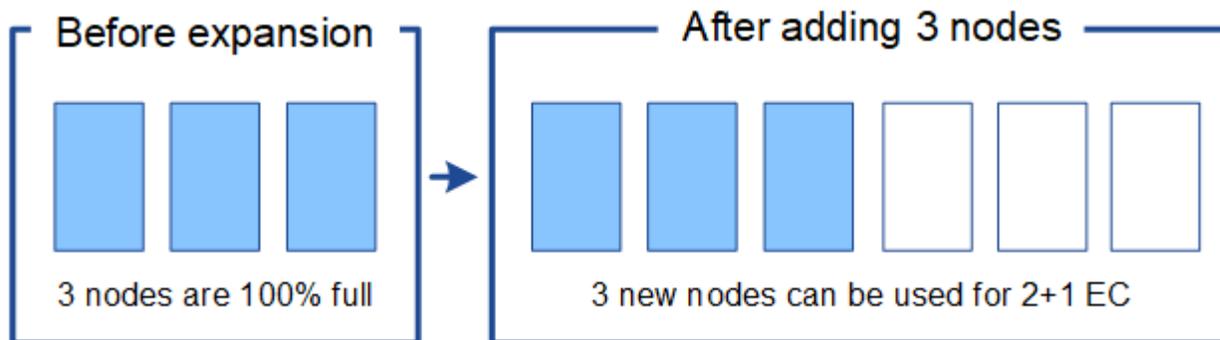
- StorageGRID wird an einem Standort ausgeführt, der drei Storage-Nodes enthält.
- Die ILM-Richtlinie verwendet eine 2+1-Regel zur Einhaltung von Datenkonsistenz für alle Objekte, die größer als 1.0 MB sind, und eine Replizierungsregel mit 2 Kopien für kleinere Objekte.

- Alle Storage-Nodes sind vollständig voll geworden. Der Alarm **Low Object Storage** wurde auf dem Hauptschweregrad ausgelöst.



Eine Neuverteilung ist nicht erforderlich, wenn genügend Nodes hinzugefügt werden

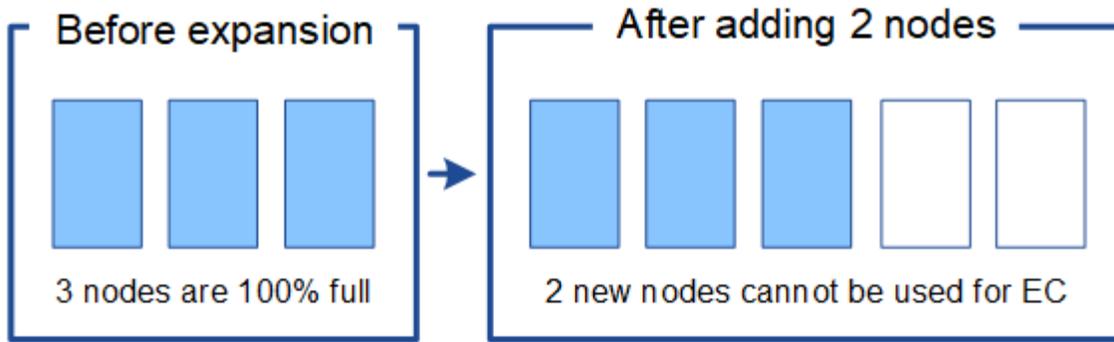
Um zu verstehen, wann EC-Lastausgleich nicht erforderlich ist, nehmen wir an, Sie haben drei (oder mehr) neue Storage-Nodes hinzugefügt. In diesem Fall müssen Sie keine EC-Ausbalancierung durchführen. Die ursprünglichen Speicher-Nodes bleiben voll, aber neue Objekte verwenden nun die drei neuen Knoten für 2+1 Erasure Coding—die beiden Datenfragmente und das eine Parity Fragment können jeweils auf einem anderen Knoten gespeichert werden.



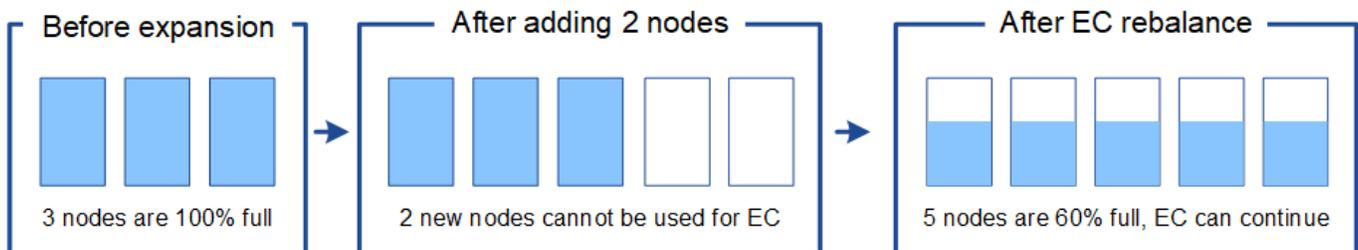
In diesem Fall können Sie zwar das Verfahren zum Lastausgleich der EC ausführen, jedoch wird durch das Verschieben der vorhandenen Daten, die nach der Löschung codiert wurden, die Performance des Grids vorübergehend beeinträchtigt, was sich auf die Client-Operationen auswirken kann.

Eine Neuverteilung ist erforderlich, wenn nicht genügend Nodes hinzugefügt werden können

Um zu verstehen, wann EC-Lastausgleich erforderlich ist, nehmen wir an, dass Sie nur zwei Storage Nodes anstelle von drei hinzufügen können. Da für das Schema 2+1 mindestens drei Speicher-Nodes Speicherplatz verfügbar sein muss, können die leeren Knoten nicht für neue mit Löschkode codierte Daten verwendet werden.



Um die neuen Storage-Nodes zu verwenden, sollten Sie das EC-Neuenausgleich-Verfahren ausführen. Wenn dieses Verfahren ausgeführt wird, verteilt StorageGRID vorhandene Daten und Paritätsfragmente über alle Storage Nodes am Standort. Wenn in diesem Beispiel der EC-Ausgleichvorgang abgeschlossen ist, sind alle fünf Nodes nun nur zu 60 % voll und die Objekte können auf allen Storage-Nodes weiterhin in das Erasure Coding-Schema 2+1 aufgenommen werden.



Empfehlungen für eine Neuverteilung der EG

NetApp erfordert eine Ausbalancierung anhand von EC-Vorgaben, wenn *alle* der folgenden Aussagen treffen:

- Sie verwenden das Erasure Coding für Ihre Objektdaten.
- Die Warnung **Low Object Storage** wurde für einen oder mehrere Storage Nodes an einem Standort ausgelöst, was darauf hinweist, dass die Knoten zu mindestens 80 % voll sind.
- Sie können nicht genügend neue Storage-Nodes für das verwendete Erasure-Coding-Schema hinzufügen. Siehe "[Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden](#)".
- Während das EC-Ausgleichsverfahren läuft, tolerieren Ihre S3- und Swift-Clients eine niedrigere Performance bei Schreib- und Leseoperationen.

Sie können optional das EC-Ausgleichsverfahren ausführen, wenn Storage Nodes auf ähnliche Ebenen gefüllt werden sollen. Ihre S3- und Swift-Clients können eine geringere Performance für ihre Schreib- und Lesevorgänge tolerieren, während das EC-Ausgleichsverfahren ausgeführt wird.

Wie EC-Ausgleichs-Verfahren mit anderen Wartungsaufgaben interagiert

Sie können bestimmte Wartungsverfahren nicht gleichzeitig durchführen, während Sie das EC-Ausgleichs-Verfahren ausführen.

Verfahren	Während des EC-Ausgleichs erlaubt?
Weitere EC-Ausgleichsverfahren	Nein Sie können nur ein EC-Ausgleichsverfahren gleichzeitig ausführen.
Verfahren zur Deaktivierung EC-Datenreparaturauftrag	Nein <ul style="list-style-type: none"> • Während des EC-Ausgleichs werden Sie daran gehindert, eine Stilllegung oder eine EC-Datenreparatur zu starten. • Sie können den EC-Ausgleichsvorgang nicht starten, während ein Ausmustern von Storage Nodes oder eine EC-Datenreparatur ausgeführt wird.
Expansionsverfahren	Nein Wenn Sie neue Storage-Nodes in einer Erweiterung hinzufügen müssen, führen Sie nach dem Hinzufügen aller neuen Nodes das Verfahren zur EC-Neuverteilung aus.
Upgrade-Verfahren	Nein Wenn Sie ein Upgrade der StorageGRID-Software durchführen müssen, führen Sie das Upgrade vor oder nach dem Ausführen des EC-Ausgleichs durch. Bei Bedarf können Sie den EC-Ausgleichsvorgang beenden, um ein Software-Upgrade durchzuführen.
Klonvorgang für Appliance-Node	Nein Wenn Sie einen Appliance-Storage-Node klonen müssen, führen Sie nach dem Hinzufügen des neuen Node das Verfahren zur EC-Neuverteilung aus.
Hotfix-Verfahren	Ja. Sie können einen StorageGRID-Hotfix anwenden, während der EC-Ausgleichsvorgang ausgeführt wird.
Andere Wartungsarbeiten	Nein Sie müssen das EC-Ausgleichsverfahren beenden, bevor Sie andere Wartungsverfahren durchführen.

Wechselwirkungen zwischen EC-Ausgleichsoperationen und ILM

Während des EC-Ausgleichs ausgeführt wird, vermeiden Sie ILM-Änderungen, die den Standort vorhandener Objekte, die mit Erasure-Coding-Verfahren codiert wurden, ändern könnten. Verwenden Sie beispielsweise nicht eine ILM-Regel mit einem anderen Profil für Erasure Coding. Wenn Sie solche ILM-Änderungen vornehmen müssen, sollten Sie das EC-Neuausgleich-Verfahren beenden.

Hinzufügen von Metadatenkapazität

Um sicherzustellen, dass ausreichend Speicherplatz für Objektmetadaten verfügbar ist, müssen Sie möglicherweise ein Erweiterungsverfahren durchführen, um neue Storage-Nodes an jedem Standort hinzuzufügen.

StorageGRID reserviert Speicherplatz für Objekt-Metadaten auf Volume 0 jedes Storage-Nodes. An jedem Standort werden drei Kopien aller Objektmetadaten aufbewahrt und gleichmäßig auf alle Storage-Nodes verteilt.

Mit Grid Manager lässt sich die Metadatenkapazität von Storage Nodes überwachen und schätzen, wie schnell Metadaten verbraucht werden. Darüber hinaus wird die Warnung **Low Metadaten Storage** für einen Speicherknoten ausgelöst, wenn der verwendete Metadaten-Speicherplatz bestimmte Schwellenwerte erreicht.

Beachten Sie, dass die Objekt-Metadatenkapazität eines Grid je nach Verwendung des Grid möglicherweise schneller belegt als die Objekt-Storage-Kapazität. Wenn Sie beispielsweise normalerweise eine große Anzahl kleiner Objekte aufnehmen oder Objekte mit großen Mengen von Benutzer-Metadaten oder -Tags versehen, müssen Sie möglicherweise Storage-Nodes hinzufügen, um die Metadaten-Kapazität zu erhöhen, obwohl weiterhin ausreichend Objekt-Storage-Kapazität vorhanden ist.

Weitere Informationen finden Sie im Folgenden:

- ["Management von Objekt-Metadaten-Storage"](#)
- ["Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node"](#)

Richtlinien zur Erhöhung der Metadaten-Kapazität

Bevor Sie Storage-Nodes hinzufügen, um die Metadatenkapazität zu steigern, lesen Sie die folgenden Richtlinien und Einschränkungen:

- Wenn eine ausreichende Objekt-Storage-Kapazität verfügbar ist, erhöht sich aufgrund der Verfügbarkeit von mehr Speicherplatz für Objekt-Metadaten die Anzahl der Objekte, die Sie in Ihrem StorageGRID System speichern können.
- Die Metadatenkapazität eines Grids lässt sich erhöhen, indem jedem Standort ein oder mehrere Storage-Nodes hinzugefügt werden.
- Der tatsächlich für Objektmetadaten auf einem bestimmten Storage-Node reservierte Speicherplatz hängt von der Option Metadaten reservierter Speicherplatz (systemweite Einstellung), der RAM-Größe des Node und der Größe des Volumes 0 des Node ab.
- Die Metadatenkapazität kann nicht durch das Hinzufügen von Storage Volumes zu vorhandenen Storage Nodes erhöht werden, da Metadaten nur auf Volume 0 gespeichert werden.
- Die Metadatenkapazität kann nicht durch das Hinzufügen eines neuen Standorts erhöht werden.
- StorageGRID speichert drei Kopien aller Objektmetadaten an jedem Standort. Daher wird die Metadaten-Kapazität Ihres Systems durch die Metadaten-Kapazität Ihres kleinsten Standorts begrenzt.
- Wenn Sie Metadaten hinzufügen, sollten Sie jedem Standort die gleiche Anzahl an Storage-Nodes hinzufügen.

Siehe ["beschreibung des reservierten Speicherplatzes für Metadaten"](#).

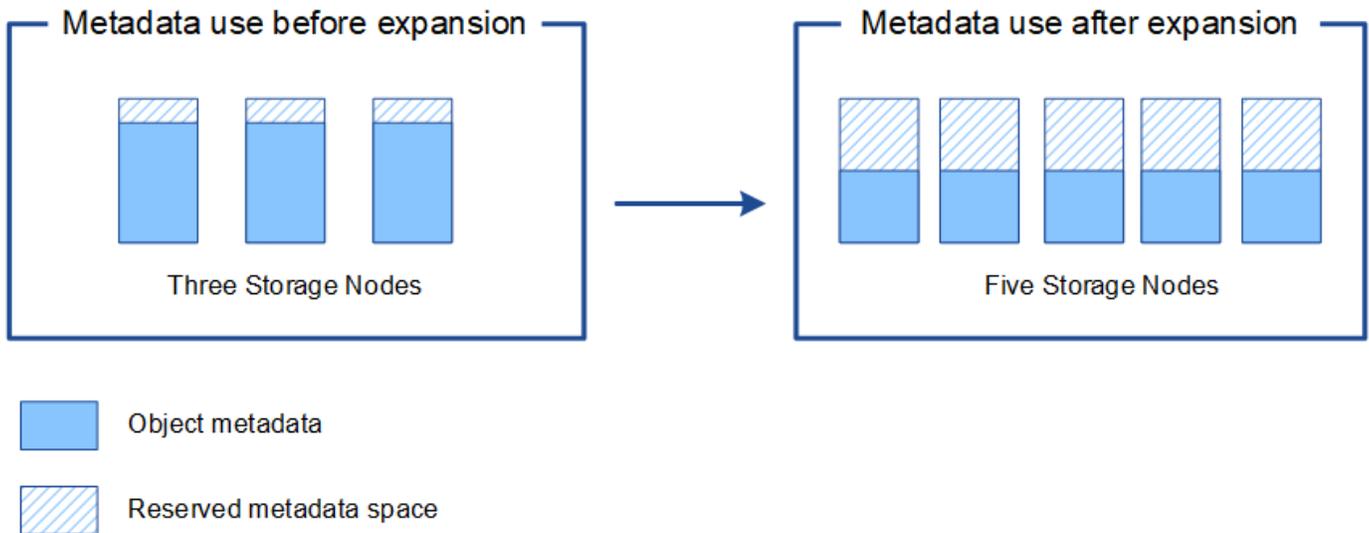
Verteilung von Metadaten beim Hinzufügen von Storage-Nodes

Wenn Sie Storage-Nodes zu einer Erweiterung hinzufügen, verteilt StorageGRID die vorhandenen Objekt-

Metadaten an die neuen Nodes an jedem Standort, wodurch die allgemeine Metadaten des Grid erhöht werden. 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 zeigt das Volumen 0 von drei Storage-Nodes vor einer Erweiterung. Metadaten verbrauchen einen relativ großen Teil des verfügbaren Metadaten-Speicherplatzes jedes Nodes und die Warnung **Low Metadaten Storage** wurde ausgelöst.

Die rechte Seite der Abbildung zeigt, wie die vorhandenen Metadaten nach dem Hinzufügen von zwei Storage-Nodes zum Standort neu verteilt werden. Die Menge der Metadaten auf jedem Node ist gesunken, die Warnung * Storage mit niedrigen Metadaten* wird nicht mehr ausgelöst, und der für Metadaten verfügbare Platz hat sich erhöht.



Grid-Nodes werden hinzugefügt, um Funktionen zu Ihrem System hinzuzufügen

Einem StorageGRID-System können Sie Redundanz oder zusätzliche Funktionen hinzufügen, indem Sie vorhandenen Standorten neue Grid-Nodes hinzufügen.

Beispielsweise können Sie Gateway-Nodes hinzufügen, die in einer HA-Gruppe (High Availability) verwendet werden sollen, oder Sie können einen Admin-Node an einem Remote-Standort hinzufügen, um die Überwachung mithilfe eines lokalen Knotens zu ermöglichen.

In einem einzigen Erweiterungsvorgang können Sie mindestens einen der folgenden Node-Typen zu einem oder mehreren bestehenden Standorten hinzufügen:

- Nicht primäre Admin-Nodes
- Storage-Nodes
- Gateway-Nodes

Beachten Sie bei der Vorbereitung des Hinzufügens von Grid-Knoten die folgenden Einschränkungen:

- Der primäre Admin-Node wird während der Erstinstallation bereitgestellt. Sie können während einer Erweiterung keinen primären Admin-Node hinzufügen.
- Sie können Storage-Nodes und andere Node-Typen in der gleichen Erweiterung hinzufügen.
- Beim Hinzufügen von Speicherknoten müssen Sie die Anzahl und Position der neuen Knoten sorgfältig

planen. Siehe ["Richtlinien zum Hinzufügen von Objektkapazität"](#).

- Wenn die Option **set New Node default** auf der Registerkarte UnTrusted Client Networks auf der Seite Firewall Control die Option **set New Node default** ist, müssen sich Client-Anwendungen, die sich über das Client-Netzwerk mit einem Load Balancer-Endpunkt-Port verbinden (**CONFIGURATION > Security > Firewall control**), mit einem Load Balancer-Endpunkt-Port verbinden. Siehe die Anweisungen zu ["Ändern Sie die Sicherheitseinstellung für den neuen Knoten"](#) Und nach ["Konfigurieren Sie die Endpunkte des Load Balancer"](#).

Fügen Sie einen neuen Standort hinzu

Sie können Ihr StorageGRID System durch Hinzufügen eines neuen Standorts erweitern.

Richtlinien zum Hinzufügen eines Standorts

Überprüfen Sie vor dem Hinzufügen eines Standorts die folgenden Anforderungen und Einschränkungen:

- Sie können nur einen Standort pro Erweiterungsvorgang hinzufügen.
- Sie können einem vorhandenen Standort keine Grid-Nodes im Rahmen derselben Erweiterung hinzufügen.
- Alle Standorte müssen mindestens drei Storage-Nodes enthalten.
- Das Hinzufügen eines neuen Standorts erhöht nicht automatisch die Anzahl der zu speichernden Objekte. Die Gesamtkapazität eines Grids hängt von der Menge des verfügbaren Storage, der ILM-Richtlinie und der Metadatenkapazität an jedem Standort ab.
- Bei der Dimensionierung eines neuen Standorts müssen Sie sicherstellen, dass dieser genügend Metadaten enthält.

Bei StorageGRID werden die Kopien aller Objektmetadaten an jedem Standort gespeichert. Wenn Sie einen neuen Standort hinzufügen, müssen Sie sicherstellen, dass dieser ausreichend Metadaten für die vorhandenen Objektmetadaten und genügend Metadaten für Wachstum enthält.

Weitere Informationen finden Sie im Folgenden:

- ["Management von Objekt-Metadaten-Storage"](#)
- ["Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node"](#)
- Dabei muss die verfügbare Netzwerkbandbreite zwischen Standorten und das Maß der Netzwerklatenz berücksichtigt werden. Metadatenaktualisierungen werden kontinuierlich zwischen Standorten repliziert, selbst wenn alle Objekte nur am Standort gespeichert werden, an dem sie aufgenommen werden.
- Da Ihr StorageGRID System während der Erweiterung betriebsbereit bleibt, müssen Sie ILM-Regeln prüfen, bevor Sie mit dem Erweiterungsverfahren beginnen. Sie müssen sicherstellen, dass Objektkopien erst am neuen Standort gespeichert werden, wenn der Erweiterungsvorgang abgeschlossen ist.

Legen Sie z. B. vor Beginn der Erweiterung fest, ob Regeln den Standardspeicherpool (Alle Speicherknoten) verwenden. In diesem Fall 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 auf den neuen Standort kopiert, sobald der erste Node an diesem Standort aktiv ist.

Weitere Informationen zum Ändern des ILM beim Hinzufügen eines neuen Standorts finden Sie im ["Beispiel zum Ändern einer ILM-Richtlinie"](#).

Sammeln Sie die erforderlichen Materialien

Bevor Sie eine Erweiterung durchführen, sammeln Sie die Materialien und installieren und konfigurieren Sie neue Hardware und Netzwerke.

Element	Hinweise
StorageGRID Installationsarchiv	<p>Wenn Sie neue Grid-Nodes oder einen neuen Standort hinzufügen, müssen Sie das StorageGRID Installationsarchiv herunterladen und extrahieren. Sie müssen dieselbe Version verwenden, die derzeit im Raster ausgeführt wird.</p> <p>Weitere Informationen finden Sie in den Anweisungen für Herunterladen und Extrahieren der StorageGRID-Installationsdateien.</p> <p>Hinweis: Sie müssen keine Dateien herunterladen, wenn Sie neue Speichervolumen zu vorhandenen Speicherknoten hinzufügen oder eine neue StorageGRID-Appliance installieren.</p>
Service-Laptop	<p>Der Service-Laptop verfügt über Folgendes:</p> <ul style="list-style-type: none">• Netzwerkport• SSH-Client (z. B. PuTTY)• "Unterstützter Webbrowser"
Passwords.txt Datei	<p>Enthält die Passwörter, die für den Zugriff auf Grid-Nodes in der Befehlszeile erforderlich sind. Im Wiederherstellungspaket enthalten.</p>
Provisioning-Passphrase	<p>Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im Passwords.txt Datei:</p>
StorageGRID-Dokumentation	<ul style="list-style-type: none">• "StorageGRID verwalten"• "Versionshinweise"• Installationsanweisungen für Ihre Plattform<ul style="list-style-type: none">◦ "Installieren Sie Red hat Enterprise Linux oder CentOS"◦ "Installieren Sie Ubuntu oder Debian"◦ "VMware installieren"
Aktuelle Dokumentation für Ihre Plattform	<p>Informationen zu unterstützten Versionen finden Sie im "Interoperabilitäts-Matrix-Tool (IMT)".</p>

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Bevor Sie neue Grid-Nodes oder einen neuen Standort hinzufügen können, müssen Sie das entsprechende StorageGRID-Installationsarchiv herunterladen und die Dateien extrahieren.

Über diese Aufgabe

Sie müssen Erweiterungsvorgänge mit der Version von StorageGRID durchführen, die derzeit im Grid ausgeführt wird.

Schritte

1. Gehen Sie zu "[NetApp Downloads: StorageGRID](#)".
2. Wählen Sie die Version von StorageGRID aus, die derzeit im Grid ausgeführt wird.
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
4. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren** aus.
5. Wählen Sie in der Spalte **Install StorageGRID** der Download-Seite die aus `.tgz` Oder `.zip` Datei für Ihre Plattform.

Die in der Archivdatei der Installation angezeigte Version muss mit der Version der derzeit installierten Software übereinstimmen.

Verwenden Sie die `.zip` Datei, wenn Windows auf dem Service-Laptop ausgeführt wird.

Plattform	Installationsarchiv
Red hat Enterprise Linux oder CentOS	<code>StorageGRID-Webscale-version-RPM-uniqueID.zip</code> <code>StorageGRID-Webscale-version-RPM-uniqueID.tgz</code>
Ubuntu oder Debian oder Appliances	<code>StorageGRID-Webscale-version-DEB-uniqueID.zip</code> <code>StorageGRID-Webscale-version-DEB-uniqueID.tgz</code>
VMware	<code>StorageGRID-Webscale-version-VMware-uniqueID.zip</code> <code>StorageGRID-Webscale-version-VMware-uniqueID.tgz</code>
OpenStack/anderer Hypervisor	Um eine vorhandene Implementierung auf OpenStack zu erweitern, müssen Sie eine Virtual Machine mit einer der oben aufgeführten unterstützten Linux-Distributionen implementieren und die entsprechenden Anweisungen für Linux befolgen.

6. Laden Sie die Archivdatei herunter und extrahieren Sie sie.
7. Führen Sie den entsprechenden Schritt für Ihre Plattform aus, um die benötigten Dateien basierend auf Ihrer Plattform, der geplanten Grid-Topologie und der Erweiterung des StorageGRID Systems auszuwählen.

Die im Schritt für jede Plattform aufgeführten Pfade beziehen sich auf das von der Archivdatei installierte Verzeichnis auf der obersten Ebene.

8. Wenn Sie ein Red hat Enterprise Linux oder CentOS System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	RPM Paket für die Installation der StorageGRID Node Images auf Ihren RHEL- oder CentOS-Hosts.
	RPM Paket für die Installation des StorageGRID Host Service auf Ihren RHEL- oder CentOS-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können. Sie können dieses Skript auch für Ping Federate verwenden.
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel für die Ansible-Rolle und das Playbook zur Konfiguration von RHEL- oder CentOS-Hosts für die Implementierung von StorageGRID Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure

Pfad und Dateiname	Beschreibung
	<p>API-Schemata für StorageGRID:</p> <p>Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.</p>

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-Download-Datei enthaltenen Dateien beschreibt.
	Eine NetApp Lizenzdatei, die nicht in der Produktionsumgebung enthalten ist und für Tests und Proof of Concept-Implementierungen genutzt werden kann
	DEB-Paket zum Installieren der StorageGRID-Knoten-Images auf Ubuntu oder Debian-Hosts.
	MD5-Prüfsumme für die Datei <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	DEB-Paket zur Installation des StorageGRID-Hostdienstes auf Ubuntu oder Debian-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können. Sie können dieses Skript auch für Ping Federate verwenden.

Pfad und Dateiname	Beschreibung
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel-Rolle und Playbook für Ansible zur Konfiguration von Ubuntu oder Debian-Hosts für die Implementierung von StorageGRID-Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests 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-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	Die Festplattendatei für Virtual Machines, die als Vorlage für die Erstellung von Grid-Node-Virtual Machines verwendet wird.

Pfad und Dateiname	Beschreibung
	Die Vorlagendatei „Open Virtualization Format“ (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung des primären Admin-Knotens.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von nicht-primären Admin-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Archiv-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Gateway-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Zur Bereitstellung von virtuellen Maschinen-basierten Speicher-knoten.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Bash Shell-Skript, das zur Automatisierung der Implementierung virtueller Grid-Nodes verwendet wird.
	Eine Beispielfunktionsdatei für die Verwendung mit dem <code>deploy-vsphere-ovftool.sh</code> Skript:
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) aktiviert ist. Sie können dieses Skript auch für Ping Federate verwenden.
	Eine Beispielfunktionsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:

Pfad und Dateiname	Beschreibung
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.

1. Wenn Sie ein Appliance-basiertes StorageGRID System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	DEB-Paket zum Installieren der StorageGRID Node Images auf den Geräten.
	MD5-Prüfsumme für die Datei <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .



Für die Installation der Appliance sind diese Dateien nur erforderlich, wenn Sie den Netzwerkverkehr vermeiden müssen. Die Appliance kann die erforderlichen Dateien vom primären Admin-Knoten herunterladen.

Überprüfung der Hardware und des Netzwerks

Stellen Sie vor Beginn der Erweiterung Ihres StorageGRID-Systems Folgendes sicher:

- Die zur Unterstützung der neuen Grid-Nodes erforderliche Hardware oder der neue Standort wurde installiert und konfiguriert.
- Alle neuen Nodes verfügen über bidirektionale Kommunikationspfade zu allen vorhandenen und neuen Nodes (Voraussetzung für das Grid Network). Vergewissern Sie sich insbesondere, dass die folgenden TCP-Ports zwischen den neuen Nodes, die Sie in der Erweiterung hinzufügen, und dem primären Admin-Node geöffnet sind:
 - 1055

- 7443
- 8011
- 10342

Siehe "[Interne Kommunikation mit Grid-Nodes](#)".

- 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 Subnetz hat, das zuvor nicht verwendet wurde, haben Sie bereits "[Das neue Subnetz wurde hinzugefügt](#)". In die Liste Raster Netzwerk. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und den Vorgang erneut starten.
- Sie verwenden keine Network Address Translation (NAT) im Grid-Netzwerk zwischen Grid-Knoten oder zwischen StorageGRID-Standorten. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt routingfähig sein. Die Verwendung von NAT zur Brücke des Grid-Netzwerks über ein öffentliches Netzwerksegment wird nur unterstützt, wenn Sie eine Tunneling-Anwendung verwenden, die für alle Knoten im Netz transparent ist, was bedeutet, dass die Grid-Knoten keine Kenntnisse über öffentliche IP-Adressen benötigen.

Diese NAT-Einschränkung gilt für Grid-Knoten und Grid-Netzwerk. Sie können NAT je nach Bedarf zwischen externen Clients und Grid-Nodes verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway-Node bereitzustellen.

Hinzufügen von Storage-Volumes

Fügen Sie Storage-Volumes zu Storage-Nodes hinzu

Sie können die Storage-Kapazität von Storage-Nodes mit maximal 16 Storage-Volumes erweitern, indem Sie zusätzliche Storage-Volumes hinzufügen. Möglicherweise müssen Sie Storage Volumes zu mehr als einem Storage Node hinzufügen, um ILM-Anforderungen für replizierte oder mit Erasure Coding versehenen Kopien zu erfüllen.

Bevor Sie beginnen

Prüfen Sie vor dem Hinzufügen von Speicher-Volumes den "[Richtlinien zum Hinzufügen von Objektkapazität](#)". Um sicherzustellen, dass Sie wissen, wo Volumes hinzugefügt werden müssen, um die Anforderungen Ihrer ILM-Richtlinie zu erfüllen.



Diese Anweisungen gelten nur für softwarebasierte Speicher-knoten. Siehe "[Erweiterungs-Shelf für das implementierte SG6060 hinzufügen](#)". Erfahren Sie, wie Sie Storage Volumes zum SG6060 hinzufügen, indem Sie Erweiterungs-Shelfs installieren. Storage-Nodes anderer Appliances können nicht erweitert werden.

Über diese Aufgabe

Der zugrunde liegende Storage eines Storage-Node wird in Storage-Volumes unterteilt. Storage Volumes sind blockbasierte Storage-Geräte, die vom StorageGRID System formatiert und zum Speichern von Objekten gemountet werden. Jeder Storage Node kann bis zu 16 Storage Volumes unterstützen, die im Grid Manager als *Object Stores* bezeichnet werden.



Objekt-Metadaten werden immer im Objektspeicher 0 gespeichert.

Jeder Objektspeicher wird auf einem Volume gemountet, das seiner ID entspricht. Der Objektspeicher mit einer ID von 0000 entspricht zum Beispiel dem `/var/local/rangedb/0` Bereitstellungspunkt.

Bevor Sie neue Speicher-Volumes hinzufügen, zeigen Sie mit Grid Manager die aktuellen Objektspeicher für jeden Storage-Node sowie die entsprechenden Mount-Punkte an. Diese Informationen können Sie beim Hinzufügen von Speicher-Volumes verwenden.

Schritte

1. Wählen Sie **NODES > site > Storage Node > Storage** aus.
2. Blättern Sie nach unten, um die verfügbaren Speichermengen für jedes Volume und jeden Objektspeicher anzuzeigen.

Bei Appliance-Storage-Nodes entspricht der weltweite Name jeder Festplatte der WWID (World-Wide Identifier) des Volumes, die angezeigt wird, wenn Sie die Standard-Volume-Eigenschaften in SANtricity OS (der mit dem Storage Controller der Appliance verbundenen Managementsoftware) anzeigen.

Um Ihnen bei der Auswertung von Datenträger-Lese- und Schreibstatistiken zu Volume-Mount-Punkten zu helfen, entspricht der erste Teil des Namens, der in der Spalte **Name** der Tabelle Disk Devices (d. h. `sd`, `sdd`, `sde` usw.) in der Spalte **Gerät** der Tabelle Volumes angezeigt wird.

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, mit denen Ihre Plattform dem Storage-Node neue Storage Volumes hinzufügen kann.
 - ["VMware: Hinzufügen von Storage Volumes zum Storage-Node"](#)
 - ["Linux: Hinzufügen von Direct-Attached oder SAN-Volumes zu Storage Node"](#)

VMware: Hinzufügen von Storage Volumes zum Storage-Node

Wenn ein Storage-Node weniger als 16 Storage-Volumes enthält, können Sie seine Kapazität mithilfe von VMware vSphere erhöhen, um Volumes hinzuzufügen.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anweisungen zur Installation von StorageGRID für VMware Implementierungen.
 - ["VMware installieren"](#)
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, Speicher-Volumes zu einem Speicher-Node hinzuzufügen, während ein Softwareupgrade, ein Wiederherstellungsverfahren oder ein anderer Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Der Storage-Node ist für kurze Zeit nicht verfügbar, wenn Sie Storage Volumes hinzufügen. Sie sollten dieses Verfahren jeweils auf einem Storage-Knoten durchführen, um die Grid-Services für Clients zu beeinträchtigen.

Schritte

1. Installieren Sie bei Bedarf neue Storage Hardware und erstellen Sie neue VMware Datenspeicher.
2. Fügen Sie eine oder mehrere Festplatten zur virtuellen Maschine als Speicher hinzu (Objektspeicher).
 - a. Öffnen Sie den VMware vSphere Client.
 - b. Bearbeiten Sie die Einstellungen der virtuellen Maschine, um eine oder mehrere zusätzliche Festplatten hinzuzufügen.

Die Festplatten werden in der Regel als Virtual Machine Disks (VMDKs) konfiguriert. VMDKs werden häufiger verwendet und sind einfacher zu managen. RDMs bieten dagegen eine bessere Performance für Workloads, die größere Objektgrößen verwenden (beispielsweise mehr als 100 MB). Weitere Informationen über das Hinzufügen von Festplatten zu virtuellen Maschinen finden Sie in der Dokumentation zu VMware vSphere.

3. Starten Sie die virtuelle Maschine neu, indem Sie im VMware vSphere Client die Option **Gastbetriebssystem neu starten** verwenden oder den folgenden Befehl in einer ssh-Sitzung zur virtuellen Maschine eingeben:`sudo reboot`



Verwenden Sie nicht **Power Off** oder **Reset**, 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-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

- ii. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

b. Konfiguration der neuen Storage Volumes:

```
sudo add_rangedbs.rb
```

Dieses Skript sucht neue Speicher-Volumes und fordert Sie zur Formatierung auf.

- c. Geben Sie **y** ein, um die Formatierung zu akzeptieren.
- d. Wenn eines der Volumes zuvor formatiert wurde, entscheiden Sie, ob Sie sie neu formatieren möchten.
 - Geben Sie *** y*** ein, um die Formatierung 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 richtig starten:

- a. Eine Liste des Status aller Dienste auf dem Server anzeigen:

```
sudo storagegrid-status
```

Der Status wird automatisch aktualisiert.

- a. Warten Sie, bis alle Dienste ausgeführt oder verifiziert sind.
- b. Statusbildschirm verlassen:

```
Ctrl+C
```

6. Vergewissern Sie sich, dass der Speicherknoten online ist:

- a. Melden Sie sich mit einem bei Grid Manager an "[Unterstützter Webbrowser](#)".
- b. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- c. Wählen Sie **site > Storage Node > LDR > Storage** aus.
- d. Wählen Sie die Registerkarte **Konfiguration** und dann die Registerkarte **Main**.
- e. Wenn die Dropdown-Liste **Speicherstatus - gewünscht** auf schreibgeschützt oder offline gesetzt ist, wählen Sie **Online** aus.
- f. Wählen Sie **Änderungen Anwenden**.

7. So sehen Sie die neuen Objektspeicher:

- a. Wählen Sie **NODES > site > Storage Node > Storage** aus.
- b. Sehen Sie sich die Details in der Tabelle **Object Stores** an.

Ergebnis

Sie können die erweiterte Kapazität der Speicherknoten zum Speichern von Objektdaten verwenden.

Linux: Hinzufügen von Direct-Attached oder SAN-Volumes zu Storage Node

Wenn ein Speicherknoten weniger als 16 Speicher-Volumes umfasst, können Sie seine Kapazität erhöhen, indem Sie neue Block-Speichergeräte hinzufügen, sie für die Linux-Hosts sichtbar machen und die neuen Blockgeräte-Zuordnungen zur StorageGRID-Konfigurationsdatei hinzufügen, die für den Speicherknoten verwendet wurde.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anweisungen für die Installation von StorageGRID für Ihre Linux-Plattform.
 - ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
 - ["Installieren Sie Ubuntu oder Debian"](#)
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, Speicher-Volumes zu einem Speicher-Node hinzuzufügen, während ein Softwareupgrade, ein Wiederherstellungsverfahren oder ein anderer Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Der Storage-Node ist für kurze Zeit nicht verfügbar, wenn Sie Storage Volumes hinzufügen. Sie sollten dieses Verfahren jeweils auf einem Storage-Knoten durchführen, um die Grid-Services für Clients zu beeinträchtigen.

Schritte

1. Installieren Sie die neue Speicherhardware.

Weitere Informationen finden Sie in der Dokumentation Ihres Hardware-Anbieters.

2. Erstellung neuer Block-Storage-Volumes 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 erlauben Sie dem Linux-Host, darauf zuzugreifen.
 - Verwenden Sie dasselbe persistente Benennungsschema, das Sie für die Storage Volumes auf dem vorhandenen Storage Node verwendet haben.
 - Wenn Sie die Funktion StorageGRID-Node-Migration verwenden, machen Sie die neuen Volumes für andere Linux-Hosts sichtbar, die Migrationsziele für diesen Storage-Node sind. Weitere Informationen finden Sie in den Anweisungen zum Installieren von StorageGRID für Ihre Linux-Plattform.
3. Melden Sie sich beim Linux-Host an, der den Storage Node unterstützt, als root oder mit einem Konto, das über Sudo-Berechtigung verfügt.
4. Vergewissern Sie sich, dass die neuen Speicher-Volumes auf dem Linux-Host sichtbar sind.

Möglicherweise müssen Sie nach Geräten erneut 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 Konfigurationsdatei des Knotens für den Speicherknoten, der unter gefunden werden kann `/etc/storagegrid/nodes/<node-name>.conf`.

7. Suchen Sie den Abschnitt der Node-Konfigurationsdatei, die die vorhandenen Objekt-Storage-Block-Gerätezuordnungen enthält.

Im Beispiel `BLOCK_DEVICE_RANGEDB_00` Bis `BLOCK_DEVICE_RANGEDB_03` Sind die vorhandenen Geräte-Zuordnungen für Objekt-Storage-Blöcke vorhanden.

```
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 Objekt-Storage-Block-Gerätezuordnungen hinzu, die den Block-Speicher-Volumes entsprechen, die Sie für diesen Storage-Node hinzugefügt haben.

Stellen Sie sicher, dass Sie bei der nächsten beginnen `BLOCK_DEVICE_RANGEDB_nn`. Lassen Sie keine Lücke.

- Beginnen Sie anhand des obigen Beispiels mit `BLOCK_DEVICE_RANGEDB_04`.
- Im folgenden Beispiel wurden dem Node vier neue Block-Storage-Volumes hinzugefügt:
`BLOCK_DEVICE_RANGEDB_04` Bis `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 Node-Konfigurationsdatei für den Storage Node zu validieren:

```
sudo storagegrid node validate <node-name>
```

Beheben Sie Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

Wenn Sie einen ähnlichen Fehler beobachten, bedeutet dies, dass die Knoten-Konfigurationsdatei versucht, das von verwendete Blockgerät zuzuordnen `<node-name>` Für `<PURPOSE>` Dem angegebenen `<path-name>` Im Linux-Dateisystem gibt es jedoch keine gültige Sonderdatei für Blockgeräte (oder Softlink zu einer Sonderdatei für Blockgeräte) an diesem Speicherort.



```

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 korrekte Eingabe durchgeführt haben `<path-name>`.

10. Führen Sie den folgenden Befehl aus, um den Knoten mit den neuen Blockgerätszuordnungen neu zu starten:

```
sudo storagegrid node start <node-name>
```

11. Melden Sie sich mit dem im angegebenen Passwort beim Storage-Node als Administrator an `Passwords.txt` Datei:
12. Überprüfen Sie, ob die Dienste richtig starten:
 - a. Eine Liste des Status aller Dienste auf dem Server anzeigen:

```
sudo storagegrid-status
```

Der Status wird automatisch aktualisiert.

- b. Warten Sie, bis alle Dienste ausgeführt oder verifiziert sind.
- c. Statusbildschirm verlassen:

```
Ctrl+C
```

13. Konfigurieren Sie den neuen Speicher für die Verwendung durch den Speicherknoten:

- a. Konfiguration der neuen Storage Volumes:

```
sudo add_rangedbs.rb
```

Dieses Skript sucht neue Speicher-Volumes und fordert Sie zur Formatierung auf.

- b. Geben Sie **y** ein, um die Speicher-Volumes zu formatieren.
- c. Wenn eines der Volumes zuvor formatiert wurde, entscheiden Sie, ob Sie sie neu formatieren möchten.
 - Geben Sie *** y*** ein, um die Formatierung neu zu formatieren.
 - Geben Sie **n** ein, um die Neuformatierung zu überspringen.

Der `setup_rangedbs.sh` Skript wird automatisch ausgeführt.

14. Vergewissern Sie sich, dass der Speicherknoten online ist:

- a. Melden Sie sich mit einem bei Grid Manager an "[Unterstützter Webbrowser](#)".
- b. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- c. Wählen Sie **site > Storage Node > LDR > Storage** aus.
- d. Wählen Sie die Registerkarte **Konfiguration** und dann die Registerkarte **Main**.
- e. Wenn die Dropdown-Liste **Speicherstatus - gewünscht** auf schreibgeschützt oder offline gesetzt ist, wählen Sie **Online** aus.
- f. Klicken Sie Auf **Änderungen Übernehmen**.

15. So sehen Sie die neuen Objektspeicher:

- a. Wählen Sie **NODES > site > Storage Node > Storage** aus.
- b. Sehen Sie sich die Details in der Tabelle **Object Stores** an.

Ergebnis

Sie können jetzt die erweiterte Kapazität der Speicherknoten zum Speichern von Objektdaten verwenden.

Grid-Nodes oder Standort hinzufügen

Grid-Nodes zu vorhandenem Standort hinzufügen oder neuen Standort hinzufügen

Gehen Sie wie folgt vor, um bestehenden Standorten Grid-Nodes hinzuzufügen oder einen neuen Standort hinzuzufügen. Sie können jedoch nicht beide Arten von Erweiterungen gleichzeitig ausführen.

Bevor Sie beginnen

- Sie haben die Berechtigung Root-Zugriff oder Wartung.
- Alle bestehenden Nodes im Grid sind über alle Standorte hinweg betriebsbereit.
- Alle vorherigen Erweiterungs-, Upgrade-, Stilllegungs- oder Recovery-Verfahren sind abgeschlossen.



Sie können eine Erweiterung nicht starten, während noch ein weiteres Verfahren zur Erweiterung, Aktualisierung, Wiederherstellung oder aktiven Deaktivierung ausgeführt wird. Sie können jedoch bei Bedarf eine Deaktivierung unterbrechen, um eine Erweiterung zu starten.

Schritte

1. ["Subnetze für Grid Network aktualisieren"](#).
2. ["Neue Grid-Nodes implementieren"](#).
3. ["Erweiterung durchführen"](#).

Subnetze für Grid Network aktualisieren

Wenn Sie Grid-Nodes oder einen neuen Standort in einer Erweiterung hinzufügen, müssen Sie möglicherweise Subnetze zum Grid-Netzwerk aktualisieren oder hinzufügen.

StorageGRID pflegt eine Liste der für die Kommunikation zwischen den Grid-Nodes im Grid-Netzwerk (eth0) verwendeten Subnetze. Zu diesen Einträgen gehören die Subnetze, die von jedem Standort im StorageGRID-System für das Grid-Netzwerk verwendet werden, sowie alle Subnetze, die für NTP, DNS, LDAP oder andere externe Server verwendet werden, auf die über das Grid-Netzwerk-Gateway zugegriffen wird.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Berechtigung für Wartung oder Root-Zugriff"](#).
- Sie haben die Provisionierungs-Passphrase.
- Sie haben die Netzwerkadressen in CIDR-Notation der Subnetze, die Sie konfigurieren möchten.

Über diese Aufgabe

Wenn einer der neuen Knoten eine Grid-Netzwerk-IP-Adresse in einem Subnetz hat, das zuvor nicht verwendet wurde, müssen Sie das neue Subnetz der Netzwerkkliste hinzufügen, bevor Sie die Erweiterung starten. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und den Vorgang erneut starten.

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > Grid-Netzwerk**.
2. Wählen Sie **Add another subnet**, um ein neues Subnetz in CIDR-Notation hinzuzufügen.

Geben Sie beispielsweise ein `10.96.104.0/22`.

3. Geben Sie die Provisionierungs-Passphrase 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 **Provisioning-Passphrase** ein.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können. Er wird auch zur Wiederherstellung des primären Admin-Knotens verwendet.

Die angegebenen Subnetze werden automatisch für Ihr StorageGRID System konfiguriert.

Neue Grid-Nodes implementieren

Die Schritte zur Implementierung neuer Grid-Nodes in einer Erweiterung entsprechen den Schritten, die bei der ersten Installation des Grid verwendet wurden. Sie müssen alle neuen Grid-Nodes implementieren, bevor Sie die Erweiterung durchführen können.

Wenn Sie das Raster erweitern, müssen die hinzugefügten Nodes nicht mit den vorhandenen Node-Typen übereinstimmen. VMware Nodes, Linux Container-basierte Nodes oder Appliance-Nodes lassen sich hinzufügen.

VMware: Grid-Nodes implementieren

Sie müssen für jeden VMware Node, den Sie der Erweiterung hinzufügen möchten, eine Virtual Machine in VMware vSphere implementieren.

Schritte

1. ["Implementieren Sie den neuen Node als Virtual Machine"](#) Und verbinden Sie sie mit einem oder mehreren StorageGRID-Netzwerken.

Bei der Implementierung des Node können Sie optional Node-Ports neu zuordnen oder CPU- oder Speichereinstellungen erhöhen.

2. Nachdem Sie alle neuen VMware-Nodes implementiert haben, ["Das Erweiterungsverfahren durchführen"](#).

Linux: Grid-Nodes implementieren

Die Grid-Nodes können auf neuen Linux-Hosts oder auf vorhandenen Linux-Hosts implementiert werden. Wenn Sie zusätzliche Linux-Hosts benötigen, um die CPU-, RAM- und Storage-Anforderungen der StorageGRID-Nodes, die Sie dem Grid hinzufügen möchten, zu unterstützen, bereiten Sie sie auf die gleiche Weise vor, wie Sie die Hosts bei der ersten Installation vorbereitet haben. Anschließend implementieren Sie die Erweiterungs-Nodes auf dieselbe Weise wie bei der Installation die Grid-Nodes.

Bevor Sie beginnen

- Sie haben Anweisungen zum Installieren von StorageGRID für Ihre Linux-Version und haben die Hardware- und Speicheranforderungen geprüft.
 - ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
 - ["Installieren Sie Ubuntu oder Debian"](#)
- Wenn Sie neue Grid-Nodes auf vorhandenen Hosts implementieren möchten, haben Sie bestätigt, dass die vorhandenen Hosts über genügend CPU-, RAM- und Storage-Kapazität für die zusätzlichen Nodes verfügen.
- Sie verfügen über einen Plan, um Ausfall-Domains zu minimieren. Beispielsweise sollten nicht alle Gateway-Nodes auf einem einzelnen physischen Host bereitgestellt werden.



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Storage Node auf einem einzelnen physischen oder virtuellen Host aus. Die Verwendung eines dedizierten Hosts für jeden Speicherknoten stellt eine isolierte Ausfalldomäne zur Verfügung.

- Wenn der StorageGRID-Node Storage verwendet, der einem NetApp ONTAP System zugewiesen ist, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.

Schritte

1. Wenn Sie neue Hosts hinzufügen, greifen Sie auf die Installationsanweisungen zur Implementierung von StorageGRID Nodes zu.
2. Befolgen Sie zum Bereitstellen der neuen Hosts die Anweisungen zur Vorbereitung der Hosts.
3. Befolgen Sie zum Erstellen von Node-Konfigurationsdateien und zum Validieren der StorageGRID-Konfiguration die Anweisungen für die Bereitstellung von Grid-Nodes.
4. Wenn Sie einem neuen Linux-Host Nodes hinzufügen, starten Sie den StorageGRID-Hostdienst.
5. Wenn Sie einem vorhandenen Linux-Host Nodes hinzufügen, starten Sie die neuen Nodes mithilfe der StorageGRID Host Service-CLI:`sudo storagegrid node start [<node name>]`

Nachdem Sie fertig sind

Nach der Implementierung aller neuen Grid-Nodes können Sie dies gerne nutzen ["Die Erweiterung durchführen"](#).

Appliances: Implementierung von Storage-, Gateway- oder nicht-primären Admin-Nodes

Um die StorageGRID-Software auf einem Appliance-Knoten zu installieren, verwenden Sie das Installationsprogramm für StorageGRID-Appliances, das in der Appliance enthalten ist. Jede Storage-Appliance arbeitet als einzelner Storage-Node in einer Erweiterung und jede Services-Appliance fungiert als einzelner Gateway-Node oder als nicht-primärer Admin-Node. Jede Appliance kann eine Verbindung zum Grid-Netzwerk, dem Admin-Netzwerk und dem Client-Netzwerk herstellen.

Bevor Sie beginnen

- Das Gerät wurde in einem Rack oder Schrank installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Sie haben den abgeschlossen ["Richten Sie die Hardware ein"](#) Schritte.

Zur Einrichtung der Appliance-Hardware gehören die erforderlichen Schritte zur Konfiguration von StorageGRID-Verbindungen (Netzwerkverbindungen und IP-Adressen) sowie die optionalen Schritte zur Aktivierung der Node-Verschlüsselung, zum Ändern des RAID-Modus und zur Neuzuweisung von Netzwerk-Ports.

- Alle Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte aufgeführt sind, wurden in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- Die StorageGRID Appliance Installer-Firmware auf der Ersatzanwendung ist mit der derzeit im Grid ausgeführten StorageGRID-Softwareversion kompatibel. Wenn die Versionen nicht kompatibel sind, müssen Sie die StorageGRID Appliance Installer-Firmware aktualisieren.
- Sie haben einen Service-Laptop mit einem ["Unterstützter Webbrowser"](#).
- Sie kennen eine der IP-Adressen, die dem Computing-Controller der Appliance zugewiesen sind. Sie können die IP-Adresse für jedes angeschlossene StorageGRID-Netzwerk verwenden.

Über diese Aufgabe

Die Installation von StorageGRID auf einem Appliance-Node erfolgt in folgenden Phasen:

- Sie geben die IP-Adresse des primären Admin-Knotens und den Namen des Appliance-Nodes an oder bestätigen sie.
- Sie starten die Installation und warten, bis Volumes konfiguriert und die Software installiert ist.

Die Installation wird durch Installationsaufgaben des Geräts gepartet. Um die Installation fortzusetzen, melden Sie sich beim Grid Manager an, genehmigen alle Grid-Nodes und schließen den StorageGRID-Installationsprozess ab.



Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess mithilfe des automatisierten `configure-sga.py` Installationskript für Appliances

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.

```
https://Controller_IP:8443
```

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Legen Sie im Abschnitt * Primary Admin Node* Connection fest, ob Sie die IP-Adresse für den primären Admin Node angeben müssen.

Wenn Sie zuvor andere Knoten in diesem Rechenzentrum installiert haben, kann der StorageGRID-Appliance-Installer diese IP-Adresse automatisch erkennen, vorausgesetzt, dass der primäre Admin-Knoten oder mindestens ein anderer Grid-Node mit ADMIN_IP konfiguriert ist, im selben Subnetz vorhanden ist.

3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	<ol style="list-style-type: none">a. Deaktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren.b. Geben Sie die IP-Adresse manuell ein.c. Klicken Sie Auf Speichern.d. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.

Option	Beschreibung
Automatische Erkennung aller verbundenen primären Admin-Nodes	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Warten Sie, bis die Liste der erkannten IP-Adressen angezeigt wird. c. Wählen Sie den primären Admin-Node für das Grid aus, in dem dieser Appliance-Speicher-Node bereitgestellt werden soll. d. Klicken Sie Auf Speichern. e. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.

4. Geben Sie im Feld **Knotenname** den Namen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und wählen Sie **Speichern**.

Der Node-Name wird diesem Appliance-Node im StorageGRID-System zugewiesen. Sie wird im Grid Manager auf der Seite Nodes (Registerkarte Übersicht) 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 *Node Name* in das Grid mit primärem Admin-Node *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-Installationsprogramms die Option **Installation starten**.

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Node name

Node name

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.

- Wenn Ihre Erweiterung mehrere Appliance-Nodes umfasst, wiederholen Sie die vorherigen Schritte für jede Appliance.



Wenn Sie mehrere Appliance Storage Nodes gleichzeitig bereitstellen müssen, können Sie den Installationsprozess mithilfe des Installationskripts für die configure-sga.py Appliance automatisieren.

- Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, wählen Sie in der Menüleiste die Option **Monitor-Installation** aus.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage Running		
Step	Progress	Status
Connect to storage controller	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete
Clear existing configuration	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete
Configure volumes	<div style="width: 30%; height: 10px; background-color: blue;"></div>	Creating volume StorageGRID-obj-00
Configure host settings	<div style="width: 0%; height: 10px; background-color: blue;"></div>	Pending

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt 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

In dieser Phase tritt eines der folgenden Prozesse auf:

- Bei einer Storage Appliance stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht alle vorhandenen Konfigurationen, kommuniziert mit SANtricity OS zum Konfigurieren von Volumes und konfiguriert die Host-Einstellungen.
- Bei einer Services-Appliance löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken im Compute-Controller und konfiguriert die Host-Einstellungen.

2. Installieren Sie das Betriebssystem

In dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID auf die Appliance.

10. Überwachen Sie den Installationsfortschritt, bis eine Meldung im Konsolenfenster angezeigt wird. Dazu werden Sie aufgefordert, den Knoten mit dem Grid Manager 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.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type#: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

Erweiterung durchführen

Wenn die Erweiterung durchgeführt wird, werden die neuen Grid-Nodes zu Ihrer bestehenden StorageGRID Implementierung hinzugefügt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Provisionierungs-Passphrase.
- Sie haben alle Grid-Nodes implementiert, die in dieser Erweiterung hinzugefügt werden.
- Sie haben die Berechtigung Wartung oder Stammzugriff.

- Beim Hinzufügen von Speicherknoten haben Sie bestätigt, dass alle Datenreparaturvorgänge im Rahmen einer Wiederherstellung abgeschlossen sind. Siehe "[Prüfen Sie die Reparatur von Daten](#)".
- Wenn Sie Storage-Nodes hinzufügen und diesen Knoten eine benutzerdefinierte Speicherklasse zuweisen möchten, haben Sie bereits "[Individuelle Storage-Klasse wurde erstellt](#)". Außerdem verfügen Sie entweder über die Root-Zugriffsberechtigung oder über die Wartungs- und ILM-Berechtigungen.
- Wenn Sie einen neuen Standort hinzufügen, haben Sie die ILM-Regeln geprüft und aktualisiert. Sie müssen sicherstellen, dass Objektkopien erst nach Abschluss der Erweiterung am neuen Standort gespeichert werden. Wenn beispielsweise eine Regel den Standardspeicherpool (**Alle Storage-Nodes**) verwendet, müssen Sie dies tun "[Erstellen Sie einen neuen Speicherpool](#)". Das nur die vorhandenen Storage-Nodes und enthält "[Aktualisieren Sie die ILM-Regeln](#)". Und die ILM-Richtlinie zur Verwendung dieses neuen Storage-Pools. Andernfalls werden Objekte auf den neuen Standort kopiert, sobald der erste Node an diesem Standort aktiv ist.

Über diese Aufgabe

Die Durchführung der Erweiterung umfasst folgende Hauptaufgaben:

1. Konfigurieren Sie die Erweiterung.
2. Starten Sie die Erweiterung.
3. Laden Sie eine neue Wiederherstellungspaket-Datei herunter.
4. Überwachen Sie die Erweiterungsschritte und -Stufen, bis alle neuen Knoten installiert und konfiguriert sind und alle Dienste gestartet sind.



Einige Erweiterungsschritte und -Phasen können eine erhebliche Zeit in Anspruch nehmen, um auf einem großen Grid ausgeführt zu werden. Das Streaming von Cassandra auf einen neuen Storage-Node kann beispielsweise nur wenige Minuten dauern, wenn die Cassandra-Datenbank leer ist. Wenn die Cassandra-Datenbank jedoch eine große Menge an Objekt-Metadaten enthält, kann diese Phase mehrere Stunden oder länger dauern. Starten Sie keine Storage-Nodes während der Phasen „erweitern des Cassandra-Clusters“ oder „Starten von Cassandra und Streaming-Daten“ neu.

Schritte

1. Wählen Sie **MAINTENANCE > Tasks > Expansion**.

Die Seite Rastererweiterung wird angezeigt. Im Abschnitt Ausstehende Knoten werden die Knoten aufgeführt, die zum Hinzufügen bereit sind.

Grid Expansion

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

[Configure Expansion](#)

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Search

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
<input type="radio"/> 00:50:56:a7:7a:c0	rleo-010-096-106-151	Storage Node	VMware VM	10.96.106.151/22
<input type="radio"/> 00:50:56:a7:0f:2e	rleo-010-096-106-156	API Gateway Node	VMware VM	10.96.106.156/22

2. Wählen Sie **Erweiterung Konfigurieren**.

Das Dialogfeld Standortauswahl wird angezeigt.

3. Wählen Sie den Erweiterungstyp aus, den Sie starten:

- Wenn Sie eine neue Site hinzufügen, wählen Sie **Neu**, und geben Sie den Namen der neuen Site ein.
- Wenn Sie einen oder mehrere Knoten zu einem bestehenden Standort hinzufügen, wählen Sie **existing** 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 den Cursor über die MAC-Adresse des **Grid Network** eines Knotens platzieren, um Details zu diesem Knoten anzuzeigen.

Pending Nodes

Grid nodes are listed as

Approve

Remove

Grid Network MA

00:50:56:a7:7a:c0

00:50:56:a7:0f:2e

leo-010-096-106-151

Storage Node

Network

Grid Network	10.96.106.151/22	10.96.104.1
Admin Network	Name	Type
Client Network		

Hardware

VMware VM

4 CPUs

8 GB RAM

Disks

55 GB

55 GB

55 GB

Approved Nodes



Wenn ein Node fehlt, vergewissern Sie sich, dass er erfolgreich bereitgestellt wurde.

6. Genehmigen Sie in der Liste der ausstehenden Knoten die Knoten, die Sie in dieser Erweiterung hinzufügen möchten.

- a. Aktivieren Sie das Optionsfeld neben dem ersten ausstehenden Rasterknoten, den Sie genehmigen möchten.
- b. Wählen Sie **Genehmigen**.

Das Konfigurationsformular für den Grid-Node wird angezeigt.

c. Ändern Sie bei Bedarf die allgemeinen Einstellungen:

Feld	Beschreibung
Standort	Der Name des Standorts, dem der Grid-Node zugeordnet wird. Wenn Sie mehrere Nodes hinzufügen, vergewissern Sie sich, dass Sie für jeden Node den korrekten Standort auswählen. Wenn Sie einen neuen Standort hinzufügen, werden alle Nodes zum neuen Standort hinzugefügt.
Name	Der Systemname für den Node. Systemnamen sind für interne StorageGRID-Vorgänge erforderlich und können nicht geändert werden.

Feld	Beschreibung
NTP-Rolle	<p>Die Rolle des Network Time Protocol (NTP) des Grid-Node:</p> <ul style="list-style-type: none"> • Wählen Sie automatisch (Standard), um dem Knoten automatisch die NTP-Rolle zuzuweisen. Die primäre Rolle wird Admin-Nodes, Storage-Nodes mit ADC-Diensten, Gateway-Nodes und allen Grid-Nodes mit nicht-statischen IP-Adressen zugewiesen. Die Clientrolle wird allen anderen Grid-Knoten zugewiesen. • Wählen Sie Primary, um dem Knoten die primäre NTP-Rolle manuell zuzuweisen. Mindestens zwei Knoten an jedem Standort sollten über die primäre Rolle verfügen, um einen redundanten Systemzugriff auf externe Zeitquellen zu ermöglichen. • Wählen Sie Client, um die Client-NTP-Rolle manuell dem Knoten zuzuweisen.
ADC-Service (nur Storage Nodes)	<p>Gibt an, ob dieser Storage Node den Dienst Administrative Domain Controller (ADC) ausführen soll. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten. Sie können den ADC-Dienst nicht zu einem Knoten hinzufügen, nachdem er bereitgestellt wurde.</p> <ul style="list-style-type: none"> • Wählen Sie Yes aus, wenn der zu ersetzende Speicher-Node den ADC-Dienst enthält. Da ein Storage Node nicht stillgelegt werden kann, wenn zu wenige ADC-Dienste verbleiben, wird dadurch sichergestellt, dass ein neuer ADC-Service verfügbar ist, bevor der alte Service entfernt wird. • Wählen Sie automatisch, damit das System bestimmen kann, ob dieser Knoten den ADC-Dienst benötigt. <p>Erfahren Sie mehr über die "ADC-Quorum".</p>
Storage-Klasse (nur Storage-Nodes)	<p>Verwenden Sie die Speicherklasse Default, oder wählen Sie die benutzerdefinierte Speicherklasse aus, die Sie diesem neuen Knoten zuweisen möchten.</p> <p>Storage-Grade werden von ILM-Speicherpools verwendet. Ihre Auswahl kann sich also darauf auswirken, welche Objekte auf dem Storage Node platziert werden.</p>

d. Ändern Sie bei 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 feststellen, dass Nodes doppelte IP-Adressen im Grid-Netzwerk aufweisen, während Sie Nodes genehmigen, müssen Sie die Erweiterung abbrechen, die Virtual Machines oder Appliances mit einer nicht doppelten IP neu bereitstellen und die Erweiterung neu starten.

- **Gateway:** Das Standard-Gateway des Grid-Knotens. Beispiel: 172.16.10.1
- **Subnetze (CIDR):** Ein oder mehrere Unternetzwerke für das Admin-Netzwerk.

e. Wählen Sie **Speichern**.

Der genehmigte Grid-Node wird in die Liste der genehmigten Nodes verschoben.

- Um die Eigenschaften eines genehmigten Grid-Knotens zu ändern, wählen Sie das entsprechende Optionsfeld aus, und wählen Sie **Bearbeiten**.
- Um einen genehmigten Rasterknoten zurück in die Liste ausstehender Knoten zu verschieben, wählen Sie dessen Optionsfeld aus und wählen Sie **Zurücksetzen**.
- Um einen genehmigten Grid-Node dauerhaft zu entfernen, schalten Sie den Node aus. Wählen Sie dann das entsprechende Optionsfeld aus, und wählen Sie **Entfernen**.

f. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.



Wenn möglich, sollten Sie alle ausstehenden Grid-Notizen genehmigen und eine einzelne Erweiterung durchführen. Wenn Sie mehrere kleine Erweiterungen durchführen, ist mehr Zeit erforderlich.

7. Wenn Sie alle Grid-Nodes genehmigt haben, geben Sie die **Provisioning-Passphrase** ein, und wählen Sie **Expand**.

Nach einigen Minuten wird diese Seite aktualisiert, um den Status des Erweiterungsverfahrens anzuzeigen. Wenn Aufgaben ausgeführt werden, die sich auf einzelne Grid-Knoten auswirken, wird im Abschnitt Grid Node Status der aktuelle Status für jeden Grid-Knoten aufgeführt.



Während des Schritts „Grid Nodes installieren“ für eine neue Appliance zeigt der StorageGRID-Appliance-Installer, wie die Installation von Phase 3 auf Phase 4 verschoben und abgeschlossen wird. Wenn Phase 4 abgeschlossen ist, wird der Controller neu gestartet.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing grid nodes								In Progress	
Grid Node Status									
Lists the installation and configuration status of each grid node included in the expansion.									
								Search <input type="text"/>	
Name	↑↓	Site	↑↓	Grid Network IPv4 Address	▼	Progress	↑↓	Stage	↑↓
rleo-010-096-106-151		Data Center 1		10.96.106.151/22		<div style="width: 50%;"></div>		Waiting for Dynamic IP Service peers	
rleo-010-096-106-156		Data Center 1		10.96.106.156/22		<div style="width: 50%;"></div>		Waiting for NTP to synchronize	
2. Initial configuration								Pending	
3. Distributing the new grid node's certificates to the StorageGRID system.								Pending	
4. Assigning Storage Nodes to storage grade								Pending	
5. Starting services on the new grid nodes								Pending	
6. Starting background process to clean up unused Cassandra keys								Pending	



Eine Standorterweiterung umfasst eine zusätzliche Aufgabe zur Konfiguration von Cassandra für den neuen Standort.

8. Sobald der Link **Download Recovery Package** angezeigt wird, laden Sie die Recovery Package Datei herunter.

Sie müssen eine aktualisierte Kopie der Wiederherstellungspaket-Datei so schnell wie möglich herunterladen, nachdem Grid-Topologieänderungen am StorageGRID-System vorgenommen wurden. Die Recovery Package-Datei ermöglicht es Ihnen, das System wiederherzustellen, wenn ein Fehler auftritt.

- a. Wählen Sie den Download-Link aus.
- b. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **Download starten**.
- c. Wenn der Download abgeschlossen ist, öffnen Sie das `.zip` und bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich `passwords.txt` Datei:
- d. Kopieren Sie die heruntergeladene Wiederherstellungspaket-Datei (`.zip`) an zwei sichere und getrennte Stellen.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

9. Wenn Sie Storage Nodes zu einem vorhandenen Standort hinzufügen oder einen Standort hinzufügen, überwachen Sie die Cassandra-Phasen, die beim Starten von Services auf den neuen Grid-Nodes auftreten.



Starten Sie keine Storage-Nodes während der Phasen „erweitern des Cassandra-Clusters“ oder „Starten von Cassandra und Streaming-Daten“ neu. Diese Phasen dauern möglicherweise für jeden neuen Storage Node viele Stunden, insbesondere dann, wenn vorhandene Storage-Nodes eine große Menge an Objekt-Metadaten enthalten.

Speicherknotten Werden Hinzugefügt

Wenn Sie Storage Nodes zu einem vorhandenen Standort hinzufügen, überprüfen Sie den Prozentsatz, der in der Statusmeldung „Starten von Cassandra und Streamen von Daten“ angezeigt wird.

5. Starting services on the new grid nodes In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

⚠ Do not reboot any Storage Nodes during Step 4. The "Starting Cassandra and streaming data" stage might take hours, especially if existing Storage Nodes contain a large amount of object metadata.

Search

Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22	<div style="width: 20%;"></div>	Starting Cassandra and streaming data (20.4% streamed)
rleo-010-096-106-156	Data Center 1	10.96.106.156/22	<div style="width: 20%;"></div>	Starting services

Dieser Prozentsatz schätzt, wie vollständig der Cassandra-Streaming-Vorgang ist, basierend auf der Gesamtmenge der verfügbaren Cassandra-Daten und der bereits auf den neuen Node geschriebenen Menge.

Site wird hinzugefügt

Wenn Sie einen neuen Standort hinzufügen, verwenden Sie `nodetool status` Den Fortschritt des Cassandra-Streamings zu überwachen und zu sehen, wie viele Metadaten während der Phase „Erweiterung des Cassandra-Clusters“ auf den neuen Standort kopiert wurden. Die gesamte Datenlast am neuen Standort sollte sich innerhalb von etwa 20 % der Gesamtmenge eines aktuellen Standorts befinden.

- Fahren Sie mit der Überwachung der Erweiterung fort, bis alle Aufgaben abgeschlossen sind und die Schaltfläche **Erweiterung konfigurieren** erneut angezeigt wird.

Nachdem Sie fertig sind

Je nachdem, welche Typen von Grid-Nodes Sie hinzugefügt haben, führen Sie weitere Integrations- und Konfigurationsschritte durch. Siehe "[Konfiguration Schritte nach Erweiterung](#)".

Erweitertes System konfigurieren

Konfiguration Schritte nach Erweiterung

Nach Abschluss einer Erweiterung müssen Sie weitere Integrations- und Konfigurationsschritte durchführen.

Über diese Aufgabe

Sie müssen die unten aufgeführten Konfigurationsaufgaben für die Grid-Nodes oder Standorte, die Sie in Ihrer Erweiterung hinzufügen, ausführen. Einige Aufgaben können optional sein, je nachdem, welche Optionen bei der Installation und Administration des Systems ausgewählt wurden und wie Sie die während der Erweiterung hinzugefügten Knoten und Standorte konfigurieren möchten.

Schritte

1. Wenn Sie eine Site hinzugefügt haben:

- ["Erstellen Sie einen Speicherpool"](#) Für den Standort und jede für die neuen Storage-Nodes ausgewählte Speicherklasse.
- Vergewissern Sie sich, dass die ILM-Richtlinie den neuen Anforderungen entspricht. Wenn Regeländerungen erforderlich sind, ["Erstellen Sie neue Regeln"](#) Und ["Aktualisieren Sie die ILM-Richtlinie"](#). Wenn die Regeln bereits korrekt sind, ["Aktivieren Sie eine neue Richtlinie"](#) Ohne Regeländerungen wird sichergestellt, dass StorageGRID die neuen Nodes verwendet.
- Vergewissern Sie sich, dass auf NTP-Server (Network Time Protocol) von diesem Standort aus zugegriffen werden kann. Siehe ["Managen von NTP-Servern"](#).



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

2. Wenn Sie einem vorhandenen Standort einen oder mehrere Storage-Nodes hinzugefügt haben:

- ["Zeigen Sie Details zum Speicherpool an"](#) Um zu bestätigen, dass jeder hinzugefügte Node in den erwarteten Speicherpools enthalten und in den erwarteten ILM-Regeln verwendet wird.
- Vergewissern Sie sich, dass die ILM-Richtlinie den neuen Anforderungen entspricht. Wenn Regeländerungen erforderlich sind, ["Erstellen Sie neue Regeln"](#) Und ["Aktualisieren Sie die ILM-Richtlinie"](#). Wenn die Regeln bereits korrekt sind, ["Aktivieren Sie eine neue Richtlinie"](#) Ohne Regeländerungen wird sichergestellt, dass StorageGRID die neuen Nodes verwendet.
- ["Vergewissern Sie sich, dass der Speicherknoten aktiv ist"](#) Und in der Lage, Objekte aufzunehmen.
- Wenn Sie die empfohlene Anzahl an Storage-Nodes nicht hinzufügen konnten, sollten Sie einen Ausgleich für Daten finden, die nach der Löschung codiert wurden. Siehe ["Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes"](#).

3. Wenn Sie einen Gateway-Node hinzugefügt haben:

- Wenn Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) für Client-Verbindungen verwendet werden, fügen Sie optional den Gateway-Node einer HA-Gruppe hinzu. Wählen Sie **CONFIGURATION > Network > High Availability groups**, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe ["Konfigurieren Sie Hochverfügbarkeitsgruppen"](#).

4. Wenn Sie einen Admin-Node hinzugefügt haben:

- a. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist, erstellen Sie für den neuen

Admin-Node eine Vertrauensbasis von einer Vertrauensbasis. Sie können sich erst beim Knoten anmelden, wenn Sie diese Vertrauensstellung von vertrauenswürdigen Parteien erstellt haben. Siehe ["Konfigurieren Sie Single Sign-On"](#).

- b. Wenn Sie den Load Balancer-Service auf Admin-Nodes verwenden möchten, fügen Sie optional den neuen Admin-Node einer HA-Gruppe hinzu. Wählen Sie **CONFIGURATION > Network > High Availability groups**, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe ["Konfigurieren Sie Hochverfügbarkeitsgruppen"](#).
 - c. Kopieren Sie optional die Admin-Node-Datenbank vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie das Attribut und die Audit-Informationen auf jedem Admin-Knoten konsistent halten möchten. Siehe ["Kopieren Sie die Admin-Knoten-Datenbank"](#).
 - d. Kopieren Sie optional die Prometheus-Datenbank vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie die historischen Metriken auf jedem Admin-Knoten konsistent halten möchten. Siehe ["Kopieren Sie die Prometheus-Kennzahlen"](#).
 - e. Kopieren Sie optional die vorhandenen Audit-Protokolle vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie die historischen Protokollinformationen auf jedem Admin-Knoten konsistent halten möchten. Siehe ["Prüfprotokolle kopieren"](#).
 - f. Optional können Sie den Zugriff auf das System für Überwachungszwecke über eine NFS-Dateifreigabe konfigurieren. Siehe ["Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS"](#).
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 vertrauenswürdiger oder vertrauenswürdiger ist, gehen Sie zu **CONFIGURATION > Security > Firewall Control**.

Wenn das Client-Netzwerk auf dem Erweiterungsknoten nicht vertrauenswürdiger ist, müssen Verbindungen zum Knoten im Client-Netzwerk über einen Load Balancer-Endpunkt hergestellt werden. Siehe ["Management der Firewall-Kontrollen"](#).

6. Konfigurieren Sie den DNS.

Wenn Sie für jeden Grid-Node DNS-Einstellungen separat angegeben haben, müssen Sie für die neuen Nodes benutzerdefinierte DNS-Einstellungen pro Node hinzufügen. Siehe ["Ändern der DNS-Konfiguration für einen einzelnen Grid-Node"](#).

Um einen ordnungsgemäßen Betrieb zu gewährleisten, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, können aufgrund bekannter Einschränkungen des Betriebssystems auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie dies tun ["Passen Sie die DNS-Serverliste an"](#) Für einzelne Knoten (in der Regel alle Knoten an einem Standort) einen anderen Satz von bis zu drei DNS-Servern verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein Inselstandort die FQDNs für externe Ziele auflösen kann.

Vergewissern Sie sich, dass der Speicherknoten aktiv ist

Nachdem ein Erweiterungsvorgang abgeschlossen ist, der neue Speicherknoten hinzugefügt hat, sollte das StorageGRID-System automatisch mit den neuen Speicherknoten beginnen. Sie müssen das StorageGRID-System verwenden, um sicherzustellen, dass der neue Speicherknoten aktiv ist.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).

2. Wählen Sie **NODES > Expansion Storage Node > Storage** aus.
3. Bewegen Sie den Cursor über die Grafik **verwendeter Speicher - Objektdaten**, um den Wert für **Used** anzuzeigen, der die Menge des gesamten nutzbaren Speicherplatzes ist, der für Objektdaten verwendet wurde.
4. Vergewissern Sie sich, dass der Wert von **verwendet** erhöht wird, wenn Sie den Cursor nach rechts auf dem Diagramm bewegen.

Admin-Knoten-Datenbank kopieren

Beim Hinzufügen von Admin-Nodes durch ein Erweiterungsverfahren können Sie optional die Datenbank vom primären Admin-Node zum neuen Admin-Node kopieren. Durch das Kopieren der Datenbank können Sie historische Informationen über Attribute, Warnmeldungen und Warnmeldungen aufbewahren.

Bevor Sie beginnen

- Sie haben die erforderlichen Erweiterungsschritte zum Hinzufügen eines Admin-Knotens abgeschlossen.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Der StorageGRID-Softwareaktivierungsprozess 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:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **SUPPORT > Tools > Grid Topology** verfügbar sind

Um sicherzustellen, dass die Admin-Node-Datenbank zwischen den Knoten konsistent ist, können Sie die Datenbank vom primären Admin-Node auf den Erweiterungs-Admin-Node kopieren.



Das Kopieren der Datenbank vom primären Admin-Node (der `__Source Admin-Node__`) zu einem Erweiterungs-Admin-Node kann bis zu mehrere Stunden dauern. In diesem Zeitraum ist der Grid Manager nicht zugänglich.

Führen Sie diese Schritte aus, um den MI-Dienst und den Management-API-Dienst sowohl auf dem primären Admin-Node als auch auf dem Erweiterungs-Admin-Node zu beenden, 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - b. Führen Sie den folgenden Befehl aus: `recover-access-points`
 - c. Geben Sie die Provisionierungs-Passphrase ein.
 - d. Beenden SIE DEN MI-Dienst: `service mi stop`
 - e. Beenden Sie den Management Application Program Interface (Management API) Service: `service mgmt-api stop`
2. Führen Sie die folgenden Schritte auf dem Erweiterungs-Admin-Knoten aus:
- a. Melden Sie sich beim Erweiterungs-Admin-Knoten an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - b. Beenden SIE DEN MI-Dienst: `service mi stop`
 - c. Beenden Sie den Management API-Service: `service mgmt-api stop`
 - d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`
 - e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
 - f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den Erweiterungs-Admin-Knoten:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die MI-Datenbank auf dem Erweiterungs-Admin-Node überschreiben möchten.
- Die Datenbank und ihre historischen Daten werden auf 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 vom SSH-Agent. Geben Sie Ein:`ssh-add -D`
3. Starten Sie die Dienste auf dem primären Admin-Knoten neu: `service servermanager start`

Kopieren Sie die Prometheus-Kennzahlen

Nach dem Hinzufügen eines neuen Admin-Knotens können Sie optional die historischen Metriken kopieren, die von Prometheus vom primären Admin-Node erhalten wurden, zum neuen Admin-Node. Durch das Kopieren der Metriken wird sichergestellt, dass historische Metriken zwischen Admin-Nodes konsistent sind.

Bevor Sie beginnen

- Der neue Admin-Node wird installiert und ausgeführt.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Wenn Sie einen Admin-Knoten hinzufügen, erstellt der Software-Installationsprozess eine neue Prometheus-

Datenbank. Sie können die historischen Kennzahlen zwischen den Knoten konsistent halten, indem Sie die Prometheus-Datenbank vom primären Admin-Node (den `_Source Admin-Node_`) auf den neuen Admin-Node kopieren.



Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

Schritte

1. Melden Sie sich beim Quell-Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- b. Stoppen Sie den Prometheus Service: `service prometheus stop`
- c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
- d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
- e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Node auf den neuen Admin-Node:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem neuen Admin-Knoten zerstören 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. Der folgende Status wird angezeigt:

```
Database cloned, starting services
```

- a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:

```
ssh-add -D
```

4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu.

```
service prometheus start
```

Prüfprotokolle kopieren

Wenn Sie einen neuen Admin-Node durch ein Erweiterungsverfahren hinzufügen, protokolliert sein AMS-Service nur Ereignisse und Aktionen, die nach dem Beitritt zum System auftreten. Nach Bedarf können Sie Audit-Protokolle von einem zuvor installierten Admin-Node auf den neuen Erweiterungs-Admin-Node kopieren, sodass er 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:

Über diese Aufgabe

Um historische Audit-Meldungen auf einem neuen Admin-Knoten verfügbar zu machen, müssen Sie die Audit-Log-Dateien manuell von einem vorhandenen Admin-Knoten in den Erweiterungs-Admin-Knoten kopieren.



Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn eine der folgenden Maßnahmen zutrifft:

- Sie haben einen externen Syslog-Server konfiguriert und Audit-Protokolle werden jetzt an den Syslog-Server anstatt an Admin-Knoten gesendet.
- Sie haben ausdrücklich angegeben, dass Audit-Meldungen nur auf den lokalen Knoten gespeichert werden sollten, die sie generiert haben.

Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)" Entsprechende Details.

Schritte

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@_primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Datei erstellt wird: `service ams stop`
3. Benennen Sie den um `audit.log` Datei um sicherzustellen, dass die Datei auf dem Erweiterungs-Admin-Knoten nicht überschrieben wird, in den Sie sie kopieren:

```
cd /var/local/audit/export
ls -l
mv audit.log new_name.txt
```

4. Kopieren Sie alle Audit-Log-Dateien in den Erweiterungs-Admin-Node:

```
scp -p * IP_address:/var/local/audit/export
```

5. Wenn Sie zur Eingabe der Passphrase für aufgefordert werden `/root/.ssh/id_rsa``Geben Sie das

SSH-Zugriffskennwort für den primären Admin-Node ein, der im aufgeführt ist
`Passwords.txt Datei:

6. Stellen Sie das Original wieder her `audit.log` Datei:

```
mv new_name.txt audit.log
```

7. AMS-Dienst starten:

```
service ams start
```

8. Melden Sie sich vom Server ab:

```
exit
```

9. Melden Sie sich beim Erweiterungs-Admin-Knoten an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@expansion_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

10. Benutzer- und Gruppeneinstellungen für die Audit-Log-Dateien aktualisieren:

```
cd /var/local/audit/export  
chown ams-user:bycast *
```

11. Melden Sie sich vom Server ab:

```
exit
```

Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes

Nachdem Sie Storage Nodes hinzugefügt haben, können Sie das EC-Ausgleichsverfahren verwenden, um Fragmente, die mit Löschvorgängen codiert wurden, auf die vorhandenen und neuen Storage-Nodes umzuverteilen.

Bevor Sie beginnen

- Sie haben die Erweiterungsschritte zum Hinzufügen der neuen Speicherknoten abgeschlossen.
- Sie haben die geprüft "[Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind](#)".
- Sie wissen, dass replizierte Objektdaten bei diesem Verfahren nicht verschoben werden und dass beim EC-Ausgleichsverfahren die replizierte Datennutzung auf jedem Storage Node nicht berücksichtigt wird, wenn festgestellt wird, wo Daten mit Erasure Coding verschoben werden.
- Sie haben die `Passwords.txt` Datei:

Was passiert, wenn dieses Verfahren ausgeführt wird

Beachten Sie vor dem Starten des Verfahrens Folgendes:

- Das EC-Ausgleichsverfahren startet nicht, wenn ein oder mehrere Volumes offline (unmounted) sind oder online (gemountet) sind, sondern sich in einem Fehlerzustand befinden.
- Das EG-Ausgleichsverfahren reserviert vorübergehend einen großen Speicher. Storage-Warnmeldungen werden möglicherweise ausgelöst, aber nach Abschluss des Ausgleichs werden sie gelöst. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt das EC-Ausgleichsverfahren fehl. Speicherreservierungen werden freigegeben, wenn der EC-Ausgleichsvorgang abgeschlossen ist, unabhängig davon, ob der Vorgang fehlgeschlagen oder erfolgreich war.
- Wenn ein Volume offline geschaltet wird oder ein Fehler auftritt, während ein EC-Neuausgleich ausgeführt wird, wird der Ausgleichsprozess zum Teil abgeschlossen und es gehen keine Daten verloren. Das EC-Ausgleichsverfahren kann an dem Punkt fortgesetzt werden, an dem es beendet wurde, wenn alle Volumes fehlerfrei online sind.
- Wenn das EC-Ausgleichsverfahren ausgeführt wird, kann die Performance von ILM-Vorgängen und S3- und Swift-Client-Operationen beeinträchtigt werden.



S3- und Swift-API-Operationen zum Hochladen von Objekten (oder Objektteilen) können während des EC-Ausgleichs fehlschlagen, wenn sie mehr als 24 Stunden benötigen. PUT-Vorgänge mit langer Dauer schlagen fehl, wenn die geltende ILM-Regel eine ausgewogene oder strikte Platzierung bei der Aufnahme verwendet. Der folgende Fehler wird gemeldet:
500 Internal Server Error.

Schritte

1. Überprüfen Sie die aktuellen Objekt-Storage-Details für den Standort, den Sie ausgleichen möchten.
 - a. Wählen Sie **KNOTEN**.
 - b. Wählen Sie den ersten Speicherknoten am Standort aus.
 - c. Wählen Sie die Registerkarte **Storage** aus.
 - d. Bewegen Sie den Mauszeiger über das Diagramm Speicher verwendet – Objektdaten, um die aktuelle Menge replizierter Daten und mit Lösungskodes versehene Daten auf dem Speicher-Node anzuzeigen.
 - e. Wiederholen Sie diese Schritte, um die anderen Speicherknoten am Standort anzuzeigen.
2. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

3. Starten Sie den Vorgang:

```
rebalance-data start --site "site-name"
```

Für "site-name" Geben Sie den ersten Standort an, an dem Sie neue Speicherknoten oder Knoten hinzugefügt haben. Umschließen `site-name` In Angeboten.

Der EC-Ausgleichsvorgang startet, und eine Job-ID wird zurückgegeben.

4. Kopieren Sie die Job-ID.

5. Überwachen Sie den Status des EC-Ausgleichs.

- So zeigen Sie den Status eines einzelnen EC-Ausgleichs an:

```
rebalance-data status --job-id job-id
```

Für ``job-id`` Geben Sie die ID an, die beim Start des Verfahrens zurückgegeben wurde.

- So zeigen Sie den Status des aktuellen EC-Ausgleichs und aller zuvor abgeschlossenen Verfahren an:

```
rebalance-data status
```



Hilfe zum Befehl zum Ausgleich von Daten erhalten:

```
rebalance-data --help
```

6. Führen Sie weitere Schritte aus, basierend auf dem zurückgegebenen Status:

- Wenn der Status lautet `In progress`, Der EC-Ausgleichsoperation läuft noch. Sie sollten das Verfahren regelmäßig überwachen, bis es abgeschlossen ist.

So zeigen Sie die geschätzte Zeit bis zum Abschluss und den Fertigstellungsgrad für den aktuellen Job an:

- Wählen Sie **SUPPORT > Tools > Metriken**.
 - Wählen Sie im Abschnitt Grafana **EC Übersicht**.
 - Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
- Wenn der Status lautet `Success`, Optional [Prüfen von Objekt-Storage](#) Um die aktualisierten Details für die Site anzuzeigen.

Daten mit Erasure-Coding-Verfahren sollten nun besser auf die Storage-Nodes am Standort abgestimmt sein.



Wenn die folgende Meldung angezeigt wird, führen Sie den EC-Ausgleichsvorgang erneut aus, bis alle mit der Löschung codierten Daten neu ausgeglichen wurden:

```
The moves in this rebalance job have been limited. To rebalance additional data, start EC rebalance again for the same site.
```

- Wenn der Status lautet `Failure`:
 - Vergewissern Sie sich, dass alle Speicherknoten am Standort mit dem Raster verbunden sind.
 - Überprüfen Sie, ob Warnmeldungen vorliegen, die sich auf diese Speicherknoten auswirken könnten, und beheben Sie sie.
 - Starten Sie das EC-Neuausgleich-Verfahren neu:

```
rebalance-data start --job-id job-id
```

- Wenn der Status des EC-Ausgleichs noch immer ist `Failure`, Wenden Sie sich an den

technischen Support.

7. Wenn das EC-Ausgleichsverfahren zu viel Last generiert (beispielsweise sind Ingest-Operationen betroffen), unterbrechen Sie den Vorgang.

```
rebalance-data pause --job-id job-id
```

8. Wenn Sie das EC-Ausgleichsverfahren beenden müssen (z. B. um ein StorageGRID-Software-Upgrade durchzuführen), geben Sie Folgendes ein:

```
rebalance-data terminate --job-id job-id
```



Wenn Sie ein EC-Ausgleichsverfahren beenden, verbleiben alle bereits verschobenen Datenfragmente am neuen Standort. Daten werden nicht zurück an den ursprünglichen Speicherort verschoben.

9. Wenn Sie Erasure Coding an mehreren Standorten verwenden, führen Sie dieses Verfahren für alle anderen betroffenen Standorte aus.

Wenden Sie sich an den technischen Support

Wenn während des Grid-Erweiterungsprozesses Fehler auftreten, die nicht behoben werden können, oder wenn eine Grid-Aufgabe fehlschlägt, wenden Sie sich an den technischen Support.

Über diese Aufgabe

Wenn Sie sich an den technischen Support wenden, müssen Sie die erforderlichen Protokolldateien bereitstellen, um bei der Fehlerbehebung der Fehler zu helfen, die auftreten.

Schritte

1. Stellen Sie eine Verbindung mit dem Erweiterungs-Node her, bei dem es zu Ausfällen kommt:

- a. Geben Sie den folgenden Befehl ein: `ssh -p 8022 admin@grid_node_IP`



Port 8022 ist der SSH-Port des Basis-OS, während Port 22 der SSH-Port der Container-Engine ist, auf der StorageGRID ausgeführt wird.

- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Sobald Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Je nach der erreichten Stufe der Installation können Sie eines der folgenden Protokolle abrufen, die auf dem Grid-Knoten verfügbar sind:

Plattform	Protokolle
VMware	<ul style="list-style-type: none"> • /var/log/daemon.log • /var/log/storagegrid/daemon.log • /var/log/storagegrid/nodes/<node-name>.log
Linux	<ul style="list-style-type: none"> • /var/log/storagegrid/daemon.log • /etc/storagegrid/nodes/<node-name>.conf (Für jeden ausgefallenen Node) • /var/log/storagegrid/nodes/<node-name>.log (Für jeden ausgefallenen Node; ist möglicherweise nicht vorhanden)

Stellen Sie Nodes wieder her und warten Sie das Grid

Recovery and Maintain: Übersicht

Verwenden Sie diese Anweisungen, um Ihr StorageGRID System zu warten und nach Ausfällen eine Wiederherstellung zu ermöglichen.

Informationen zu diesen Anweisungen

In diesen Anweisungen wird beschrieben, wie ein Software-Hotfix angewendet wird, Grid-Nodes wiederhergestellt, ein ausgefallener Standort wiederhergestellt, Grid-Nodes oder einen gesamten Standort ausmustern, Netzwerkwartung durchführen, Wartungsvorgänge auf Host- und Middleware-Ebene durchführen und Grid Node-Verfahren durchführen.



In diesen Anweisungen bezieht sich „Linux“ auf eine Bereitstellung von Red hat® Enterprise Linux®, Ubuntu®, CentOS oder Debian®. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool](#)" Um eine Liste der unterstützten Versionen zu erhalten.

Bevor Sie beginnen

- Sie verfügen über ein umfassendes Verständnis des StorageGRID Systems.
- Sie haben die Topologie Ihres StorageGRID Systems überprüft und sich mit der Grid-Konfiguration vertraut gemacht.
- Ihr versteht, dass ihr alle Anweisungen genau befolgen und alle Warnungen beachten müsst.
- Sie wissen, dass nicht beschriebene Wartungsverfahren nicht unterstützt werden oder eine Serviceerbringung erfordern.

Wartungsverfahren für Geräte

Hardwareprozeduren finden Sie in der Wartungsanleitung für Ihr StorageGRID-Gerät.

- "[SGF6112-Appliance warten](#)"
- "[Wartung von SG100 und SG1000 Appliances](#)"

- ["Warten Sie die SG6000-Appliance"](#)
- ["SG5700 Appliance warten"](#)

Recovery Package Herunterladen

Die Wiederherstellungspakedatei ermöglicht Ihnen die Wiederherstellung des StorageGRID-Systems bei einem Fehler.

Bevor Sie beginnen

- Vom primären Admin-Knoten aus sind Sie mit einem beim Grid-Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Provisionierungs-Passphrase.
- Das ist schon ["Bestimmte Zugriffsberechtigungen"](#).

Laden Sie die aktuelle Recovery Package-Datei herunter, bevor Sie Grid-Topologieänderungen am StorageGRID-System vornehmen oder bevor Sie Software aktualisieren. Laden Sie anschließend eine neue Kopie des Wiederherstellungspakets herunter, nachdem Sie Änderungen an der Grid-Topologie vorgenommen haben oder nachdem Sie die Software aktualisiert haben.

Schritte

1. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
2. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **Download starten**.

Der Download startet sofort.
3. Wenn der Download abgeschlossen ist, öffnen Sie das `.zip` Und bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich `Passwords.txt` Datei:
4. Kopieren Sie die heruntergeladene Wiederherstellungspaket-Datei (`.zip`) An zwei sichere und getrennte Stellen.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

StorageGRID Hotfix Verfahren

StorageGRID Hotfix Prozedur: Überblick

Möglicherweise müssen Sie einen Hotfix auf Ihr StorageGRID-System anwenden, wenn Probleme mit der Software zwischen Funktionsversionen erkannt und behoben werden.

StorageGRID Hotfixes enthalten Software-Änderungen, die außerhalb einer Feature- oder Patch-Freigabe verfügbar gemacht werden. Die gleichen Änderungen sind in einer zukünftigen Version enthalten. Darüber hinaus enthält jede Hotfix-Version eine Roll-up aller früheren Hotfixes innerhalb der Funktion oder Patch-Freigabe.

Überlegungen für die Anwendung eines Hotfix

Ein StorageGRID-Hotfix kann nicht angewendet werden, wenn ein anderer Wartungsvorgang ausgeführt wird.

Sie können beispielsweise keinen Hotfix anwenden, während eine Stilllegung, Erweiterung oder Wiederherstellung ausgeführt wird.



Wenn ein Knoten oder ein Standort stillgelegt wird, können Sie sicher einen Hotfix anwenden. Darüber hinaus können Sie in der Lage sein, einen Hotfix in den letzten Phasen eines StorageGRID-Upgrade-Verfahrens anzuwenden. Weitere Informationen finden Sie in der Anleitung zum Aktualisieren 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 Hotfix für die übrigen Knoten in Ihrem StorageGRID-System genehmigen.

Wenn ein Hotfix nicht auf einen oder mehrere Knoten angewendet wird, wird der Grund für den Fehler in der Spalte Details der Hotfix-Fortschrittstabelle angezeigt. Sie müssen alle Fehler beheben und den gesamten Prozess wiederholen. Knoten mit einer zuvor erfolgreichen Anwendung des Hotfix werden in nachfolgenden Anwendungen übersprungen. Sie können den Hotfix-Prozess so oft wie erforderlich sicher wiederholen, bis alle Knoten aktualisiert wurden. Der Hotfix muss erfolgreich auf allen Grid-Knoten installiert werden, damit die Anwendung abgeschlossen werden kann.

Während die Grid-Knoten mit der neuen Hotfix-Version aktualisiert werden, können die tatsächlichen Änderungen in einem Hotfix nur bestimmte Dienste auf bestimmte Node-Typen beeinflussen. Ein Hotfix wirkt sich beispielsweise nur auf den LDR-Service auf Storage Nodes aus.

Wie Hotfixes für die Wiederherstellung und Erweiterung eingesetzt werden

Nachdem ein Hotfix auf das Grid angewendet wurde, installiert der primäre Admin-Knoten automatisch die gleiche Hotfix-Version auf alle Knoten, die durch Wiederherstellungsvorgänge wiederhergestellt oder in einer Erweiterung hinzugefügt werden.

Wenn Sie jedoch den primären Admin-Knoten wiederherstellen müssen, müssen Sie manuell die richtige StorageGRID-Version installieren und dann den Hotfix anwenden. Die endgültige StorageGRID-Version des primären Admin-Knotens muss mit der Version der anderen Nodes im Raster übereinstimmen.

Das folgende Beispiel zeigt, wie ein Hotfix bei der Wiederherstellung des primären Admin-Knotens angewendet wird:

1. Angenommen, auf dem Grid wird eine StorageGRID 11.A.B-Version mit dem neuesten Hotfix ausgeführt. Die „GRID Version“ ist 11.A.B.y.
2. Der primäre Admin-Node schlägt fehl.
3. Sie stellen den primären Admin-Node mit StorageGRID 11.A.B neu bereit und führen das Recovery-Verfahren durch.



Wie zur Anpassung an die Grid-Version erforderlich, können Sie bei der Implementierung des Node eine untergeordnete Version verwenden. Sie müssen nicht zuerst die Hauptversion implementieren.

4. Anschließend wenden Sie Hotfix 11.A.B.y auf den primären Admin-Node an.

Weitere Informationen finden Sie unter ["Primären Ersatzadministrator-Knoten konfigurieren"](#).

Auswirkungen auf Ihr System beim Anwenden eines Hotfix

Wenn Sie einen Hotfix anwenden, müssen Sie verstehen, wie sich Ihr StorageGRID-

System auswirkt.

Bei Client-Applikationen kommt es unter Umständen zu kurzfristigen Unterbrechungen

Das StorageGRID System kann während des Hotfix-Prozesses Daten von Client-Applikationen aufnehmen und abrufen. Client-Verbindungen zu einzelnen Gateway-Nodes oder Storage-Nodes können jedoch vorübergehend unterbrochen werden, wenn der Hotfix Dienste auf diesen Knoten neu starten muss. Die Verbindung wird wiederhergestellt, sobald der Hotfix-Prozess abgeschlossen ist und die Dienste auf den einzelnen Knoten wieder aufgenommen werden.

Möglicherweise müssen Sie Ausfallzeiten planen, um einen Hotfix anzuwenden, wenn ein kurzfristiger Verlust der Verbindung nicht akzeptabel ist. Sie können eine selektive Genehmigung verwenden, um die Planung für die Aktualisierung bestimmter Knoten zu planen.



Dank mehrerer Gateways und Hochverfügbarkeitsgruppen (HA-Gruppen) lassen sich während des Hotfix-Prozesses automatische Failovers durchführen. Siehe Anweisungen für ["Konfigurieren von Hochverfügbarkeitsgruppen"](#).

Warnmeldungen und SNMP-Benachrichtigungen können ausgelöst werden

Warnmeldungen und SNMP-Benachrichtigungen können ausgelöst werden, wenn Dienste neu gestartet werden und das StorageGRID System als Umgebung mit gemischten Versionen funktioniert (einige Grid-Nodes mit einer früheren Version, 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 Hotfix auf StorageGRID:

- Nehmen Sie keine Änderungen an der Grid-Konfiguration vor (z. B. Festlegen von Netznetznetzen oder Genehmigen ausstehender Netzknoten), bis der Hotfix auf alle Knoten angewendet wurde.
- Aktualisieren Sie die ILM-Konfiguration erst, wenn der Hotfix auf alle Nodes angewendet wurde.

Beschaffung der erforderlichen Materialien für Hotfix

Bevor Sie einen Hotfix anwenden, müssen Sie alle erforderlichen Materialien erhalten.

Element	Hinweise
StorageGRID-Hotfix-Datei	Sie müssen die StorageGRID-Hotfix-Datei herunterladen.
<ul style="list-style-type: none">• Netzwerkport• "Unterstützter Webbrowser"• SSH-Client (z. B. PuTTY)	
Wiederherstellungspaket (.zip) Datei	Vor dem Anwenden eines Hotfix "Laden Sie die neueste Recovery Package-Datei herunter" Falls während des Hotfix Probleme auftreten, dann, nachdem der Hotfix angewendet wurde, laden Sie eine neue Kopie der Recovery Package-Datei herunter und speichern Sie sie an einem sicheren Ort. Mit der aktualisierten Wiederherstellungspaket-Datei können Sie das System wiederherstellen, wenn ein Fehler auftritt.

Element	Hinweise
Passwords.txt-Datei	Optional und nur verwendet, wenn Sie einen Hotfix manuell mit dem SSH-Client anwenden. Der <code>passwords.txt</code> Datei ist Teil des Wiederherstellungspakets <code>.zip</code> Datei:
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase wird im nicht aufgeführt <code>passwords.txt</code> Datei:
Zugehörige Dokumentation	<code>readme.txt</code> Datei für den Hotfix. Diese Datei ist auf der Download-Seite des Hotfix enthalten. Schauen Sie sich die an <code>readme</code> Vor dem Anwenden des Hotfix sorgfältig ablesen.

Hotfix-Datei herunterladen

Sie müssen die Hotfix-Datei herunterladen, bevor Sie den Hotfix anwenden können.

Schritte

1. Gehen Sie zu ["NetApp Downloads: StorageGRID"](#).
2. Wählen Sie den Pfeil nach unten unter **Verfügbare Software**, um eine Liste der Hotfixes anzuzeigen, die zum Herunterladen verfügbar sind.



Hotfix-Dateiversionen haben das Formular: 11.4.x.y.

3. Überprüfen Sie die Änderungen, die im Update enthalten sind.



Wenn Sie nur haben ["Primärer Admin-Node wiederhergestellt"](#) Und Sie müssen einen Hotfix anwenden, wählen Sie die gleiche Hotfix-Version, die auf den anderen Grid-Knoten installiert ist.

- a. Wählen Sie die Hotfix-Version, die Sie herunterladen möchten, und wählen Sie **Go**.
- b. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
- c. Lesen und akzeptieren Sie die Endnutzer-Lizenzvereinbarung.

Die Download-Seite für die ausgewählte Version wird angezeigt.

- d. Hotfix herunterladen `readme.txt` Datei zum Anzeigen einer Zusammenfassung der Änderungen, die im Hotfix enthalten sind.
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 gespeichert `.txt` Datei: Wenn dies der Fall ist, müssen Sie die Datei ohne umbenennen `.txt` Erweiterung.

5. Wählen Sie einen Speicherort für den Download aus, und wählen Sie **Speichern**.

Überprüfen Sie den Zustand des Systems, bevor Sie Hotfix anwenden

Sie müssen überprüfen, ob das System bereit ist, um den Hotfix aufzunehmen.

1. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).
2. Stellen Sie, falls möglich, sicher, dass das System ordnungsgemäß ausgeführt wird und dass alle Grid-Nodes mit dem Grid verbunden sind.

Verbundene Knoten weisen grüne Häkchen auf  Auf der Seite Knoten.

3. Überprüfen Sie, ob und beheben Sie alle aktuellen Warnmeldungen, wenn möglich.
4. Stellen Sie sicher, dass keine weiteren Wartungsverfahren wie Upgrades, Wiederherstellungen, Erweiterungen oder Stillstandsmaßnahmen ausgeführt werden.

Sie sollten warten, bis alle aktiven Wartungsvorgänge abgeschlossen sind, bevor Sie einen Hotfix anwenden.

Ein StorageGRID-Hotfix kann nicht angewendet werden, wenn ein anderer Wartungsvorgang ausgeführt wird. Sie können beispielsweise keinen Hotfix anwenden, während eine Stilllegung, Erweiterung oder Wiederherstellung ausgeführt wird.



Wenn ein Node oder Standort ["Die Stilllegungsvorgang wird angehalten"](#), Können Sie sicher einen Hotfix anwenden. Darüber hinaus können Sie in der Lage sein, einen Hotfix in den letzten Phasen eines StorageGRID-Upgrade-Verfahrens anzuwenden. Siehe Anweisungen für ["Aktualisieren von StorageGRID Software"](#).

Hotfix anwenden

Der Hotfix wird zuerst automatisch auf den primären Admin-Knoten angewendet. Anschließend müssen Sie die Anwendung des Hotfix für andere Grid-Knoten genehmigen, bis alle Knoten dieselbe Softwareversion ausführen. Sie können die Genehmigungssequenz anpassen, indem Sie auswählen, ob einzelne Grid-Nodes, Gruppen von Grid-Nodes oder alle Grid-Nodes genehmigt werden sollen.

Bevor Sie beginnen

- Sie haben die geprüft ["Überlegungen zur Anwendung eines Hotfix"](#).
- Sie haben die Provisionierungs-Passphrase.
- Sie haben Root-Zugriff oder die Berechtigung Maintenance.

Über diese Aufgabe

- Sie können die Anwendung eines Hotfix auf einen Knoten verzögern. Der Hotfix-Prozess ist jedoch erst abgeschlossen, wenn Sie den Hotfix auf alle Knoten anwenden.
- Sie können kein StorageGRID Software-Upgrade oder SANtricity OS-Update durchführen, bevor Sie den Hotfix-Prozess abgeschlossen haben.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).
2. Wählen Sie **WARTUNG > System > Software-Update**.

Die Seite Software-Aktualisierung wird angezeigt.

Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade	StorageGRID hotfix	SANtricity OS update
Upgrade to the next StorageGRID version and apply the latest hotfix for that version.	Apply a hotfix to your current StorageGRID software version.	Update the SANtricity OS software on your StorageGRID storage appliances.
Upgrade →	Apply hotfix →	Update →

3. Wählen Sie **Hotfix anwenden**.

Die Seite StorageGRID Hotfix wird angezeigt.

StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available. When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ?

Passphrase

Provisioning Passphrase ?

4. Wählen Sie die Hotfix-Datei aus, die Sie von der NetApp Support-Website heruntergeladen haben.

- Wählen Sie **Durchsuchen**.
- Suchen und wählen Sie die Datei aus.

`hotfix-install-version`

- Wählen Sie **Offen**.

Die Datei wurde hochgeladen. Nach Abschluss des Uploads wird der Dateiname im Feld Details

angezeigt.



Ändern Sie den Dateinamen nicht, da er Teil des Überprüfungsprozesses ist.

5. Geben Sie die Provisionierungs-Passphrase in das Textfeld ein.

Die Schaltfläche **Start** wird aktiviert.

6. Wählen Sie **Start**.

Eine Warnung wird angezeigt, dass die Verbindung Ihres Browsers vorübergehend unterbrochen wird, da Dienste auf dem primären Admin-Knoten neu gestartet werden.

7. Wählen Sie **OK**, um mit der Anwendung des Hotfix auf den primären Admin-Knoten zu beginnen.

Wenn der Hotfix beginnt:

a. Die Hotfix-Validierungen werden ausgeführt.



Wenn Fehler gemeldet werden, beheben Sie sie, laden Sie die Hotfix-Datei erneut hoch und wählen Sie erneut **Start** aus.

b. Die Tabelle mit dem Hotfix-Installationsfortschritt wird angezeigt.

Diese Tabelle zeigt alle Knoten in Ihrem Raster und die aktuelle Phase der Hotfix-Installation für jeden Knoten. Die Knoten in der Tabelle sind nach Typ gruppiert (Admin-Nodes, Gateway-Nodes, Storage-Nodes und Archive Nodes).

c. Der Fortschrittsbalken ist abgeschlossen, und der primäre Admin-Knoten wird als „Abschließen“ angezeigt.

Hotfix Installation Progress

Site	Name	Progress	Stage	Details	Action
Vancouver	VTC-ADM1-101-191	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete		

8. Sortieren Sie die Listen der Knoten in jeder Gruppierung in aufsteigender oder absteigender Reihenfolge nach **Site**, **Name**, **Progress**, **Stage** oder **Details**. Oder geben Sie einen Begriff in das Feld **Suche** ein, um nach bestimmten Knoten zu suchen.

9. Genehmigen Sie die Grid-Knoten, die aktualisiert werden können. Genehmigte Nodes desselben Typs werden nacheinander aktualisiert.



Genehmigen Sie den Hotfix für einen Knoten nur, wenn Sie sicher sind, dass der Knoten aktualisiert werden kann. Wenn der Hotfix auf einen Grid-Knoten angewendet wird, werden möglicherweise einige Dienste auf diesem Knoten neu gestartet. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren.

- Wählen Sie eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere einzelne Knoten zur Hotfix-Warteschlange hinzuzufügen.
- Wählen Sie in jeder Gruppierung die Schaltfläche **Alle genehmigen** aus, um alle Knoten desselben Typs der Hotfix-Warteschlange hinzuzufügen. Wenn Sie Suchkriterien im Feld **Suche** eingegeben haben, gilt die Schaltfläche **Alle genehmigen** für alle durch die Suchkriterien ausgewählten Knoten.



Die Schaltfläche **Alle genehmigen** oben auf der Seite genehmigt alle Knoten, die auf der Seite aufgeführt sind, während die Schaltfläche **Alle genehmigen** oben in einer Tabellengruppierung nur alle Knoten in dieser Gruppe genehmigt. Wenn die Reihenfolge, in der Knoten aktualisiert werden, wichtig ist, genehmigen Sie Knoten oder Gruppen von Knoten jeweils eins und warten Sie, bis das Upgrade auf jedem Knoten abgeschlossen ist, bevor Sie den nächsten Knoten genehmigen.

- Wählen Sie oben auf der Seite die Schaltfläche **Alle genehmigen** 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 Knoten oder alle Knoten aus der Hotfix-Warteschlange zu entfernen.

Wenn die Bühne über „Queued“ hinausgeht, wird die Schaltfläche **Entfernen** ausgeblendet und Sie können den Knoten nicht mehr aus dem Hotfix-Prozess entfernen.

Storage Nodes - 1 out of 9 completed							Approve All	Remove All
							Search	Q
Site	Name	Progress	Stage	Details	Action			
Raleigh	RAL-S1-101-196	<div style="width: 0%;"></div>	Queued		Remove			
Raleigh	RAL-S2-101-197	<div style="width: 100%;"></div>	Complete					
Raleigh	RAL-S3-101-198	<div style="width: 0%;"></div>	Queued		Remove			
Sunnyvale	SVL-S1-101-199	<div style="width: 0%;"></div>	Queued		Remove			
Sunnyvale	SVL-S2-101-93	<div style="width: 0%;"></div>	Waiting for you to approve		Approve			
Sunnyvale	SVL-S3-101-94	<div style="width: 0%;"></div>	Waiting for you to approve		Approve			
Vancouver	VTC-S1-101-193	<div style="width: 0%;"></div>	Waiting for you to approve		Approve			
Vancouver	VTC-S2-101-194	<div style="width: 0%;"></div>	Waiting for you to approve		Approve			
Vancouver	VTC-S3-101-195	<div style="width: 0%;"></div>	Waiting for you to approve		Approve			

10. Warten Sie, bis der Hotfix auf jeden genehmigten Grid-Knoten angewendet wird.

Wenn der Hotfix erfolgreich auf allen Knoten installiert wurde, wird die Fortschrittsabelle für die Hotfix-Installation geschlossen. Ein grünes Banner zeigt das Datum und die Uhrzeit an, zu der der Hotfix abgeschlossen wurde.

11. Wenn der Hotfix nicht auf alle 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 auf alle Knoten angewendet wurde. Sie können den Hotfix-Prozess so oft wie nötig wiederholen, bis er abgeschlossen ist.

Verfahren zur Recovery von Grid-Nodes

Verfahren zur Wiederherstellung von Grid Nodes: Übersicht

Wenn ein Grid-Node ausfällt, können Sie ihn wiederherstellen, indem Sie den fehlerhaften physischen oder virtuellen Server ersetzen, die StorageGRID Software neu installieren und wiederherstellbare Daten wiederherstellen.

Grid Nodes können ausfallen, wenn ein Hardware-, Virtualisierungs-, Betriebssystem- oder Softwarefehler den Node funktionsunfähig oder unzuverlässig macht. Es gibt viele Arten von Fehlern, die die Notwendigkeit zur Wiederherstellung eines Grid-Node auslösen können.

Die Schritte zur Wiederherstellung eines Grid-Node sind abhängig von der Plattform, auf der der Grid-Node gehostet wird, und vom Typ des Grid-Nodes. Jeder Grid-Node-Typ verfügt über eine bestimmte Recovery-Prozedur, die Sie genau befolgen müssen.

Im Allgemeinen versuchen Sie, soweit möglich Daten vom ausgefallenen Grid Node aufzubewahren, reparieren oder ersetzen den ausgefallenen Node, verwenden den Grid Manager zum Konfigurieren des Ersatz-Node und stellen die Daten des Node wieder her.



Wenn eine gesamte StorageGRID Site ausfällt, wenden Sie sich an den technischen Support. Der technische Support arbeitet mit Ihnen zusammen an der Entwicklung und Umsetzung eines Site Recovery-Plans, der die wiederherzustellende Datenmenge maximiert und Ihre Geschäftsziele erreicht. Siehe "[Durchführen der Standortwiederherstellung durch den technischen Support](#)".

Warnungen und Überlegungen für die Wiederherstellung von Grid Nodes

Wenn ein Grid-Node ausfällt, müssen Sie ihn so schnell wie möglich wiederherstellen. Bevor Sie beginnen, müssen Sie alle Warnungen und Überlegungen für die Node-Wiederherstellung prüfen.



StorageGRID ist ein verteiltes System, das aus mehreren Knoten besteht, die miteinander arbeiten. Verwenden Sie keine Festplatten-Snapshots, um Grid-Nodes wiederherzustellen. Beachten Sie stattdessen die Recovery- und Wartungsabläufe für jeden Node-Typ.

Einige der Gründe für die baldige Wiederherstellung eines ausgefallenen Grid-Node sind:

- Ein ausgefallener Grid-Node verringert die Redundanz von System- und Objektdaten, sodass Sie anfällig für dauerhaften Datenverlust sind, wenn ein anderer Node ausfällt.
- Ein ausgefallener Grid-Node kann sich auf die Effizienz des täglichen-bis-täglichen Betriebs auswirken.

- Ein ausgefallener Grid-Node kann die Überwachung des Systembetriebs verringern.
- Ein ausgefallener Grid-Node kann zu einem internen Serverfehler von 500 führen, wenn strenge ILM-Regeln vorhanden sind.
- Wenn ein Grid-Node nicht sofort wiederhergestellt wird, kann es zu einer Zunahme der Recovery-Zeiten kommen. So können sich beispielsweise Warteschlangen entwickeln, die vor Abschluss der Wiederherstellung gelöscht werden müssen.

Befolgen Sie immer das Recovery-Verfahren für den spezifischen Typ des Grid-Node, den Sie wiederherstellen. Die Wiederherstellungsverfahren variieren für primäre oder nicht primäre Admin-Nodes, Gateway-Nodes, Archiv-Nodes, Appliance-Nodes und Storage-Nodes.

Voraussetzungen für die Wiederherstellung von Grid-Nodes

Bei der Wiederherstellung der Grid-Nodes werden alle folgenden Bedingungen vorausgesetzt:

- Die fehlerhafte physische oder virtuelle Hardware wurde ersetzt und konfiguriert.
- Die StorageGRID-Appliance-Installationsversion auf der Ersatz-Appliance entspricht der Softwareversion Ihres StorageGRID-Systems, wie unter beschrieben "[Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance](#)".
- Wenn Sie einen anderen Grid-Node als den primären Admin-Node wiederherstellen, besteht die Verbindung zwischen dem wiederherzustellenden Grid-Node und dem primären Admin-Node.

Reihenfolge der Knotenwiederherstellung, wenn ein Server, der mehr als einen Grid-Knoten hostet, ausfällt

Wenn ein Server, der mehr als einen Grid-Node hostet, ausfällt, können Sie die Knoten in beliebiger Reihenfolge wiederherstellen. Wenn der ausgefallene Server jedoch den primären Admin-Node hostet, müssen Sie diesen Knoten zuerst wiederherstellen. Die Wiederherstellung des primären Admin-Knotens verhindert, dass andere Knoten-Wiederherstellungen angehalten werden, während sie warten, bis der primäre Admin-Node kontaktiert wird.

IP-Adressen für wiederhergestellte Knoten

Versuchen Sie nicht, einen Node mit einer IP-Adresse wiederherzustellen, die derzeit einem anderen Node zugewiesen ist. Wenn Sie den neuen Node implementieren, verwenden Sie die aktuelle IP-Adresse des ausgefallenen Nodes oder eine nicht genutzte IP-Adresse.

Wenn Sie für die Implementierung des neuen Knotens eine neue IP-Adresse verwenden und dann den Knoten wiederherstellen, wird die neue IP-Adresse für den wiederhergestellten Knoten weiterhin verwendet. Wenn Sie die ursprüngliche IP-Adresse wiederherstellen möchten, verwenden Sie nach Abschluss der Wiederherstellung das Tool IP ändern.

Sammeln der erforderlichen Materialien für die Grid Node Recovery

Bevor Sie Wartungsmaßnahmen durchführen, müssen Sie sicherstellen, dass die zur Wiederherstellung eines ausgefallenen Grid-Node erforderlichen Materialien vorhanden sind.

Element	Hinweise
StorageGRID Installationsarchiv	<p>Wenn Sie einen Grid-Node wiederherstellen müssen, müssen Sie dies tun Laden Sie die Installationsdateien von StorageGRID herunter Für Ihre Plattform.</p> <p>Hinweis: Sie müssen keine Dateien herunterladen, wenn Sie ausgefallene Speichervolumen auf einem Speickerknoten wiederherstellen.</p>
Service-Laptop	<p>Der Service-Laptop muss Folgendes haben:</p> <ul style="list-style-type: none"> • Netzwerkport • SSH-Client (z. B. PuTTY) • "Unterstützter Webbrowser"
Wiederherstellungspaket .zip Datei	<p>Erhalten Sie eine Kopie des aktuellsten Wiederherstellungspakets .zip Datei: <code>sgws-recovery-package-id-revision.zip</code></p> <p>Der Inhalt des .zip Die Datei wird jedes Mal aktualisiert, wenn das System geändert wird. Sie werden aufgefordert, die aktuellste Version des Wiederherstellungspakets nach dem Speichern dieser Änderungen an einem sicheren Ort zu speichern. Verwenden Sie die neueste Kopie, um nach Grid-Ausfällen eine Wiederherstellung durchzuführen.</p> <p>Wenn der primäre Admin-Node normal funktioniert, können Sie das Wiederherstellungspaket aus dem Grid Manager herunterladen. Wählen Sie WARTUNG > System > Wiederherstellungspaket.</p> <p>Wenn Sie nicht auf den Grid Manager zugreifen können, finden Sie verschlüsselte Kopien des Wiederherstellungspakets auf einigen Storage Nodes, die den ADC-Dienst enthalten. Untersuchen Sie auf jedem Speickerknoten diesen Speicherort für das Wiederherstellungspaket: <code>/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg</code> Verwenden Sie das Wiederherstellungspaket mit der höchsten Versionsnummer.</p>
Passwords.txt Datei	<p>Enthält die Passwörter, die für den Zugriff auf Grid-Nodes in der Befehlszeile erforderlich sind. Im Wiederherstellungspaket enthalten.</p>
Provisioning-Passphrase	<p>Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im Passwords.txt Datei:</p>
Aktuelle Dokumentation für Ihre Plattform	<p>Dokumentation finden Sie auf der Website des Plattformanbieters.</p> <p>Informationen zu den derzeit unterstützten Versionen Ihrer Plattform finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".</p>

Laden Sie StorageGRID-Installationsdateien herunter und extrahieren Sie sie

Laden Sie die Software herunter und extrahieren Sie die Dateien, sofern Sie nicht sind "[Wiederherstellen ausgefallener Speicher-Volumes auf einem Storage-Node](#)".

Sie müssen die Version von StorageGRID verwenden, die derzeit im Raster ausgeführt wird.

Schritte

1. Bestimmen Sie, welche Version der Software derzeit installiert ist. Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **über** aus.
2. Wechseln Sie zum "[NetApp Download-Seite für StorageGRID](#)".
3. Wählen Sie die Version von StorageGRID aus, die derzeit im Grid ausgeführt wird.

Die StorageGRID-Softwareversionen haben dieses Format: `11.x.y`.

4. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren** aus.
6. Wählen Sie in der Spalte **Install StorageGRID** der Download-Seite die aus `.tgz` Oder `.zip` Datei für Ihre Plattform.

Die in der Archivdatei der Installation angezeigte Version muss mit der Version der derzeit installierten Software übereinstimmen.

Verwenden Sie die `.zip` Datei, wenn Sie Windows ausführen.

Plattform	Installationsarchiv
Red hat Enterprise Linux oder CentOS	<code>StorageGRID-Webscale-version-RPM-uniqueID.zip</code> <code>StorageGRID-Webscale-version-RPM-uniqueID.tgz</code>
Ubuntu oder Debian oder Appliances	<code>StorageGRID-Webscale-version-DEB-uniqueID.zip</code> <code>StorageGRID-Webscale-version-DEB-uniqueID.tgz</code>
VMware	<code>StorageGRID-Webscale-version-VMware-uniqueID.zip</code> <code>StorageGRID-Webscale-version-VMware-uniqueID.tgz</code>

7. Laden Sie die Archivdatei herunter und extrahieren Sie sie.
8. Befolgen Sie den entsprechenden Schritt für Ihre Plattform und wählen Sie die Dateien aus, die Sie benötigen, basierend auf Ihrer Plattform und den Grid-Nodes, die Sie wiederherstellen müssen.

Die im Schritt für jede Plattform aufgeführten Pfade beziehen sich auf das von der Archivdatei installierte Verzeichnis auf der obersten Ebene.

9. Wenn Sie ein wiederherstellen "[Red hat Enterprise Linux oder CentOS System](#)", Wählen Sie die entsprechenden Dateien.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	RPM Paket für die Installation der StorageGRID Node Images auf Ihren RHEL- oder CentOS-Hosts.
	RPM Paket für die Installation des StorageGRID Host Service auf Ihren RHEL- oder CentOS-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können. Sie können dieses Skript auch für Ping Federate verwenden.
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel für die Ansible-Rolle und das Playbook zur Konfiguration von RHEL- oder CentOS-Hosts für die Implementierung von StorageGRID Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure

Pfad und Dateiname	Beschreibung
	<p>API-Schemata für StorageGRID:</p> <p>Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.</p>

1. Wenn Sie ein wiederherstellen "[Ubuntu oder Debian-System](#)", Wählen Sie die entsprechenden Dateien.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine NetApp Lizenzdatei, die nicht in der Produktionsumgebung enthalten ist und für Tests und Proof of Concept-Implementierungen genutzt werden kann
	DEB-Paket zum Installieren der StorageGRID-Knoten-Images auf Ubuntu oder Debian-Hosts.
	MD5-Prüfsumme für die Datei <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	DEB-Paket zur Installation des StorageGRID-Hostdienstes auf Ubuntu oder Debian-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können. Sie können dieses Skript auch für Ping Federate verwenden.

Pfad und Dateiname	Beschreibung
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel-Rolle und Playbook für Ansible zur Konfiguration von Ubuntu oder Debian-Hosts für die Implementierung von StorageGRID-Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.

1. Wenn Sie ein wiederherstellen "[VMware System](#)", Wählen Sie die entsprechenden Dateien.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	Die Festplattendatei für Virtual Machines, die als Vorlage für die Erstellung von Grid-Node-Virtual Machines verwendet wird.

Pfad und Dateiname	Beschreibung
	Die Vorlagendatei „Open Virtualization Format“ (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung des primären Admin-Knotens.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von nicht-primären Admin-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Archiv-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Gateway-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Zur Bereitstellung von virtuellen Maschinen-basierten Speicher-knoten.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Bash Shell-Skript, das zur Automatisierung der Implementierung virtueller Grid-Nodes verwendet wird.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>deploy-vsphere-ovftool.sh</code> Skript:
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) aktiviert ist. Sie können dieses Skript auch für Ping Federate verwenden.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:

Pfad und Dateiname	Beschreibung
	Ein Beispiel für ein Python-Skript, mit dem Sie sich bei der Grid Management API anmelden können, wenn Single Sign-On (SSO) mithilfe von Active Directory oder Ping Federate aktiviert ist.
	Ein Hilfskript, das vom Begleiter aufgerufen wird <code>storagegrid-ssoauth-azure.py</code> Python-Skript zur Durchführung von SSO-Interaktionen mit Azure
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie diese Schemas verwenden, um zu bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung für Upgrade-Kompatibilitätstests haben.

1. Wenn Sie ein Appliance-basiertes StorageGRID-System wiederherstellen, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	DEB-Paket zum Installieren der StorageGRID Node Images auf den Geräten.
	MD5-Prüfsumme für die Datei <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .



Für die Installation der Appliance sind diese Dateien nur erforderlich, wenn Sie den Netzwerkverkehr vermeiden müssen. Die Appliance kann die erforderlichen Dateien vom primären Admin-Knoten herunterladen.

Wählen Sie die Knotenwiederherstellung aus

Sie müssen den korrekten Wiederherstellungsvorgang für den Typ des fehlgeschlagenen Knotens auswählen.

Grid-Node	Wiederherstellungsvorgang
Mehr als ein Storage-Node	Wenden Sie sich an den technischen Support. Wenn mehrere Storage-Nodes ausgefallen sind, muss der technische Support bei der Recovery Unterstützung leisten, um Inkonsistenzen zu Datenbanken zu vermeiden, die zu Datenverlusten führen können. Möglicherweise ist ein Wiederherstellungsverfahren für Standorte erforderlich. "Durchführen der Standortwiederherstellung durch den technischen Support"
Ein einzelner Storage-Node	Das Speicherknoten-Wiederherstellungsverfahren hängt vom Typ und der Dauer des Ausfalls ab. "Wiederherstellung nach Ausfällen der Storage-Nodes"
Admin-Node	Das Verfahren Admin-Knoten hängt davon ab, ob Sie den primären Admin-Knoten oder einen nicht-primären Admin-Knoten wiederherstellen müssen. "Wiederherstellung bei Ausfällen des Admin-Nodes"
Gateway-Node	"Wiederherstellung nach Gateway-Node-Ausfällen" .
Archiv-Node	"Wiederherstellung nach Ausfällen des Archivierungs-Nodes" .



Wenn ein Server, der mehr als einen Grid-Node hostet, ausfällt, können Sie die Knoten in beliebiger Reihenfolge wiederherstellen. Wenn der ausgefallene Server jedoch den primären Admin-Node hostet, müssen Sie diesen Knoten zuerst wiederherstellen. Die Wiederherstellung des primären Admin-Knotens verhindert, dass andere Knoten-Wiederherstellungen angehalten werden, während sie warten, bis der primäre Admin-Node kontaktiert wird.

Wiederherstellung nach Ausfällen der Storage-Nodes

Recovery von Storage-Node-Ausfällen: Übersicht

Das Verfahren zur Wiederherstellung eines fehlgeschlagenen Speicherknoten hängt von der Art des Fehlers und dem Typ des fehlgeschlagenen Speicherknoten ab.

Verwenden Sie diese Tabelle, um das Wiederherstellungsverfahren für einen fehlgeschlagenen Speicherknoten auszuwählen.

Problem	Aktion	Hinweise
<ul style="list-style-type: none"> • Mehr als ein Speicherknoten ist ausgefallen. • Ein zweiter Speicherknoten ist weniger als 15 Tage nach Ausfall oder Wiederherstellung eines Speicherknotens ausgefallen. <p>Dies schließt den Fall ein, dass ein Speicherknoten während der Wiederherstellung eines anderen Speicherknoten noch in Arbeit ist.</p>	<p>Wenden Sie sich an den technischen Support.</p>	<p>Die Wiederherstellung von mehr als einem Storage-Node (oder mehr als einem Storage-Node innerhalb von 15 Tagen) kann die Integrität der Cassandra-Datenbank beeinträchtigen, was zu Datenverlust führen kann.</p> <p>Der technische Support kann bestimmen, wann die Wiederherstellung eines zweiten Storage Node sicher gestartet werden kann.</p> <p>Hinweis: Wenn mehr als ein Speicherknoten, der den ADC-Dienst enthält, an einem Standort ausfällt, verlieren Sie alle ausstehenden Plattformdienstanfragen für diesen Standort.</p>
<p>Mehr als ein Speicher-Node an einem Standort ist ausgefallen oder ein ganzer Standort ist ausgefallen.</p>	<p>Wenden Sie sich an den technischen Support. Möglicherweise ist eine Standortwiederherstellung erforderlich.</p>	<p>Der technische Support prüft Ihre Situation und erstellt einen Recovery-Plan. Siehe "Durchführen der Standortwiederherstellung durch den technischen Support".</p>
<p>Ein Speicherknoten ist seit mehr als 15 Tagen offline.</p>	<p>"Stellen Sie Storage Node länger als 15 Tage wieder her"</p>	<p>Dieses Verfahren ist erforderlich, um die Integrität der Cassandra-Datenbank sicherzustellen.</p>
<p>Ein Appliance-Speicherknoten ist fehlgeschlagen.</p>	<p>"Appliance Storage Node wiederherstellen"</p>	<p>Das Wiederstellungsverfahren für Appliance Storage Nodes ist bei allen Ausfällen gleich.</p>
<p>Ein oder mehrere Storage-Volumes sind ausgefallen, das Systemlaufwerk ist jedoch intakt</p>	<p>"Wiederherstellung nach einem Storage-Volume-Ausfall bei intaktem Systemlaufwerk"</p>	<p>Dieses Verfahren wird für softwarebasierte Speicherknoten verwendet.</p>
<p>Das Systemlaufwerk ist ausgefallen.</p>	<p>"Wiederherstellung nach einem Laufwerksausfall"</p>	<p>Das Verfahren zum Austausch der Nodes hängt von der Implementierungsplattform ab und ob auch Storage Volumes ausgefallen sind.</p>



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

Stellen Sie Storage Node länger als 15 Tage wieder her

Wenn ein einzelner Storage-Node länger als 15 Tage offline war und nicht mit anderen Storage-Nodes verbunden ist, müssen Sie Cassandra auf dem Node neu aufbauen.

Bevor Sie beginnen

- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Decommission.**)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Expansion.**)

Über diese Aufgabe

Storage-Nodes verfügen über eine Cassandra Datenbank mit Objekt-Metadaten. Wenn ein Storage-Node seit mehr als 15 Tagen nicht mit anderen Storage-Nodes kommunizieren kann, geht StorageGRID davon aus, dass die Cassandra-Datenbank des Node veraltet ist. Der Speicher-Node kann erst wieder dem Grid beitreten, wenn Cassandra mithilfe von Informationen aus anderen Speicher-Nodes neu erstellt wurde.

Verwenden Sie dieses Verfahren, um Cassandra nur dann neu aufzubauen, wenn ein einzelner Storage-Node ausfällt. Wenden Sie sich an den technischen Support, wenn weitere Storage-Nodes offline sind oder wenn Cassandra innerhalb der letzten 15 Tage auf einem anderen Storage-Node neu erstellt wurde. Dazu gehört beispielsweise das Verfahren zur Wiederherstellung ausgefallener Storage-Volumes oder zur Wiederherstellung eines ausgefallenen Storage-Nodes.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es kann zu Datenverlusten kommen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Siehe "[Durchführen der Standortwiederherstellung durch den technischen Support](#)".

Schritte

1. Schalten Sie ggf. den Storage-Node ein, der wiederhergestellt werden muss.
2. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#.+`



Wenn Sie sich beim Grid-Node nicht anmelden können, ist die Systemfestplatte möglicherweise nicht intakt. Gehen Sie zum Verfahren für "[Wiederherstellung nach einem Systemausfall](#)".

3. Führen Sie die folgenden Prüfungen auf dem Speicherknoten durch:

- a. Geben Sie diesen Befehl ein: `nodetool status`

Die Ausgabe sollte sein `Connection refused`

- b. Wählen Sie im Grid Manager **SUPPORT > Tools > Grid-Topologie** aus.
- c. Wählen Sie **Site > Storage Node > SSM > Services**. Vergewissern Sie sich, dass der Cassandra-Service angezeigt wird `Not Running`.
- d. Wählen Sie **Storage Node > SSM > Resources**. Vergewissern Sie sich, dass im Abschnitt `Volumes` kein Fehlerstatus vorhanden ist.
- e. Geben Sie diesen Befehl ein: `grep -i Cassandra /var/local/log/servermanager.log`

Die folgende Meldung sollte in der Ausgabe angezeigt werden:

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

4. Geben Sie diesen Befehl ein, und überwachen Sie die Skriptausgabe: `check-cassandra-rebuild`

- Wenn der Cassandra-Service, abhängig von Volume 0, ausgeführt wird, werden Sie aufgefordert, ihn zu beenden. Geben Sie ein: **Y**



Wenn der Cassandra-Dienst bereits angehalten wurde, werden Sie nicht dazu aufgefordert. Der Cassandra-Service wird nur für Volume 0 angehalten.

- Überprüfen Sie die Warnungen im Skript. Wenn keine dieser Möglichkeiten gelten, bestätigen Sie, dass Sie Cassandra neu aufbauen möchten. Geben Sie ein: **Y**



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

5. Führen Sie nach Abschluss der Neuerstellung die folgenden Prüfungen durch:

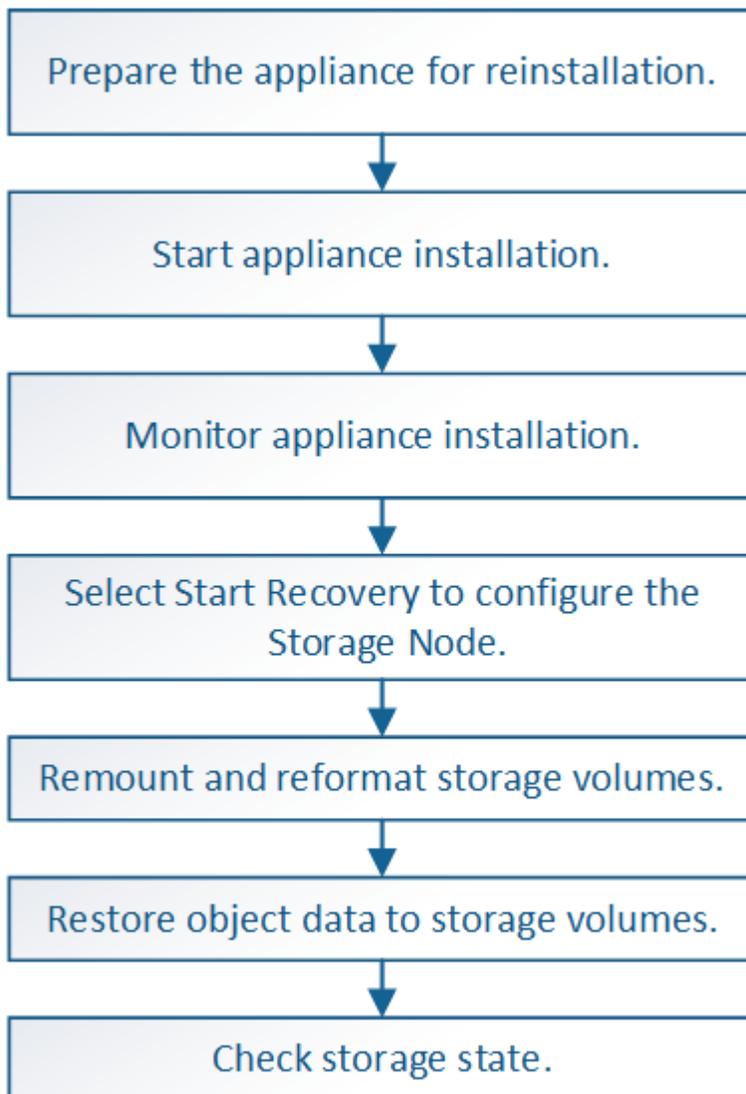
- a. Wählen Sie im Grid Manager **SUPPORT > Tools > Grid-Topologie** aus.
- b. Wählen Sie **Site > Recovered Storage Node > SSM > Services**.
- c. Vergewissern Sie sich, dass alle Dienste ausgeführt werden.
- d. Wählen Sie **DDS > Data Store**.
- e. Bestätigen Sie, dass der **Data Store Status** „up“ und der **Data Store State** „normal“ lautet.

Appliance Storage Node wiederherstellen

Wiederherstellen des Appliance Storage Node: Workflow

Das Verfahren zur Wiederherstellung eines fehlerhaften StorageGRID-Appliance-Speicherknoten ist dieselbe, egal ob Sie eine Wiederherstellung nach dem Verlust des Systemlaufwerks oder nach dem Verlust von Storage-Volumen durchführen.

Wie im Workflow-Diagramm gezeigt, müssen Sie die Appliance vorbereiten und die Software neu installieren, den Knoten so konfigurieren, dass er wieder in das Raster eingebunden wird, den Speicher neu formatieren und Objektdaten wiederherstellen.



Vorsichtsmaßnahmen und Hinweise zur Wiederherstellung von Appliance-Storage-Nodes



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen kann zu Datenverlust führen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Siehe "[Durchführen der Standortwiederherstellung durch den technischen Support](#)".



Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und sich die Kopie auf einem ausgefallenen Storage Volume befindet, können Sie das Objekt nicht wiederherstellen.



Wenn während der Wiederherstellung ein Alarm „Services: Status – Cassandra (SVST)“ (Services: Status – Cassandra (SVST)) angezeigt wird, siehe "[Recovery ausgefallener Storage-Volumes und Wiederherstellung der Cassandra-Datenbank](#)". Nach dem Wiederaufbau von Cassandra sollten die Alarme gelöscht werden. Wenn die Alarme nicht gelöscht werden, wenden Sie sich an den technischen Support.

Informationen zu Hardware-Wartungsverfahren, z. B. Anweisungen zum Austauschen eines Controllers oder zum Neuinstallieren von SANtricity OS, finden Sie in der Wartungsanleitung für Ihre Speichergerät.



- "[SGF6112 Storage Appliances](#)"
- "[SG6000 Storage-Appliances](#)"
- "[SG5700 Storage-Appliances](#)"

Appliance-Speicherknoten für die Neuinstallation vorbereiten

Wenn Sie einen Appliance-Speicherknoten wiederherstellen, müssen Sie zuerst die Appliance für die Neuinstallation der StorageGRID-Software vorbereiten.

Schritte

1. Melden Sie sich beim fehlgeschlagenen Speicherknoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Bereiten Sie den Appliance-Speicherknoten für die Installation der StorageGRID-Software vor.

`sgareinstall`

3. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie Folgendes ein: `y`

Die Appliance wird neu gestartet, und Ihre SSH-Sitzung wird beendet. In der Regel dauert es etwa 5 Minuten, bis das Installationsprogramm für StorageGRID-Appliances verfügbar ist, obwohl in einigen Fällen Sie möglicherweise bis zu 30 Minuten warten müssen.



Versuchen Sie nicht, den Neustart zu beschleunigen, indem Sie das Gerät aus- und wieder einschalten oder anderweitig zurücksetzen. Sie können automatische BIOS-, BMC- oder andere Firmware-Upgrades unterbrechen.

Der Speicherknoten der StorageGRID-Appliance wird zurückgesetzt, und die Daten auf dem Speicherknoten sind nicht mehr zugänglich. Die während der ursprünglichen Installation konfigurierten IP-Adressen sollten intakt bleiben. Nach Abschluss des Vorgangs wird jedoch empfohlen, dies zu bestätigen.

Nach Ausführung des `sgareinstall` Der Befehl entfernt alle über StorageGRID bereitgestellten Konten, Passwörter und SSH-Schlüssel und generiert neue Host-Schlüssel.

Starten Sie die Installation der StorageGRID Appliance

Um StorageGRID auf einem Appliance-Speicherknoten zu installieren, verwenden Sie das StorageGRID-Appliance-Installationsprogramm, das in der Appliance enthalten ist.

Bevor Sie beginnen

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des StorageGRID Appliance Installer wurden Netzwerkverbindungen und IP-Adressen für die Appliance konfiguriert.
- Sie kennen die IP-Adresse des primären Admin-Knotens für das StorageGRID-Raster.
- Alle Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte aufgeführt sind, wurden in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- Sie haben diese vorausgesetzten Aufgaben ausgeführt, indem Sie die Installationsanweisungen für Ihre Speicher-Appliance befolgen. Siehe "[Schnellstart für die Hardwareinstallation](#)".
- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Sie kennen eine der IP-Adressen, die dem Computing-Controller in der Appliance zugewiesen sind. Sie können die IP-Adresse für das Admin-Netzwerk (Management-Port 1 auf dem Controller), das Grid-Netzwerk oder das Client-Netzwerk verwenden.

Über diese Aufgabe

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 ihn.
- Sie starten die Installation und warten, bis Volumes konfiguriert und die Software installiert ist.
- Durch den Prozess partway, die Installation pausiert. Um die Installation fortzusetzen, müssen Sie sich beim Grid Manager anmelden und den ausstehenden Speicherknoten als Ersatz für den ausgefallenen Node konfigurieren.

- Nachdem Sie den Node konfiguriert haben, wird die Installation der Appliance abgeschlossen und die Appliance wird neu gestartet.

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Compute-Controller in der Appliance ein.

`https://Controller_IP:8443`

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Legen Sie im Abschnitt primäre Administratorknoten-Verbindung fest, ob Sie die IP-Adresse für den primären Admin-Node angeben müssen.

Das Installationsprogramm der StorageGRID-Appliance kann diese IP-Adresse automatisch erkennen, wenn der primäre Admin-Node oder mindestens ein anderer Grid-Node mit Admin_IP konfiguriert ist, sich im selben Subnetz befindet.

3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Schritte
Manuelle IP-Eingabe	<ol style="list-style-type: none"> a. Deaktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie Auf Speichern. d. Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.
Automatische Erkennung aller verbundenen primären Admin-Nodes	<ol style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Wählen Sie aus der Liste der ermittelten IP-Adressen den primären Admin-Node für das Grid aus, in dem dieser Appliance-Speicher-Node bereitgestellt wird. c. Klicken Sie Auf Speichern. d. Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.

4. Geben Sie im Feld **Node Name** den gleichen Hostnamen (Systemnamen) ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Save**.
5. Vergewissern Sie sich im Abschnitt Installation, dass der aktuelle Status „bereit ist, die Installation von zu starten `node name Into Grid mit Primary Admin Node `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-Installationsprogramms auf **Installation starten**.

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Node name

Node name

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.



Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, klicken Sie in der Menüleiste auf **Monitor-Installation**. Siehe "[Überwachen Sie die Appliance-Installation](#)".

Überwachen Sie die Installation der StorageGRID Appliance

Das Installationsprogramm der StorageGRID Appliance stellt den Status bereit, bis die Installation abgeschlossen ist. Nach Abschluss der Softwareinstallation wird die Appliance neu gestartet.

Schritte

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage		Running
Step	Progress	Status
Connect to storage controller		Complete
Clear existing configuration		Complete
Configure volumes		Creating volume StorageGRID-obj-00
Configure host settings		Pending

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt 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 Storage Controller her, löscht alle vorhandenen Konfigurationen, kommuniziert mit SANtricity OS, um Volumes zu konfigurieren, und konfiguriert die Host-Einstellungen.

- **2. Installieren Sie das Betriebssystem**

In dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID auf die Appliance.

3. Überwachen Sie den Installationsfortschritt weiter, bis die Phase **StorageGRID installieren** angehalten wird. Auf der eingebetteten Konsole wird eine Meldung angezeigt, in der Sie aufgefordert werden, diesen Knoten auf dem Admin-Knoten mithilfe des Grid-Managers zu genehmigen.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Gehen Sie zu "Wählen Sie Wiederherstellung starten, um Appliance Storage Node zu konfigurieren".

Wählen Sie Wiederherstellung starten, um Appliance Storage Node zu konfigurieren

Sie müssen im Grid Manager die Option Wiederherstellung starten auswählen, um einen Appliance-Speicherknoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben die Provisionierungs-Passphrase.

- Sie haben einen Storage Node für die Recovery-Appliance bereitgestellt.
- Sie haben das Startdatum aller Reparaturaufträge für Daten, die mit dem Verfahren zur Fehlerkorrektur codiert wurden.
- Sie haben überprüft, ob der Speicher-Node innerhalb der letzten 15 Tage nicht neu erstellt wurde.

Schritte

1. Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden in der Liste angezeigt, wenn sie fehlschlagen. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und für die Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netznoten wiederherstellen“.

Wenn der Grid-Knoten die Stufe „Warten auf manuelle Schritte“ erreicht, gehen Sie zum nächsten Thema und führen Sie die manuellen Schritte durch, um Appliance-Storage-Volumes neu zu mounten und neu zu formatieren.



An jedem Punkt während der Wiederherstellung können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das anzeigt, dass der Knoten in einem unbestimmten Zustand bleibt, wenn Sie das Verfahren zurücksetzen.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Vorgangs erneut versuchen möchten, müssen Sie den Appliance-Knoten durch Ausführen auf einen vorinstallierten Status wiederherstellen `sgareinstall` Auf dem Node.

Appliance-Storage-Volumes neu einbinden und formatieren (manuelle Schritte)

Führen Sie manuell zwei Skripte aus, um noch intakte Storage-Volumes neu mounten und ausgefallene Storage Volumes neu formatieren zu können. Das erste Skript bindet Volumes wieder ein, die ordnungsgemäß als StorageGRID-Storage-Volumes formatiert sind. Das zweite Skript formatiert alle nicht abgehängt Volumes neu, stellt die Cassandra-Datenbank bei Bedarf wieder her und startet Services.

Bevor Sie beginnen

- Sie haben bereits die Hardware für alle ausgefallenen Storage Volumes ausgetauscht, die ausgetauscht werden müssen.

Ausführen des `sn-remount-volumes` Skript kann Ihnen helfen, zusätzliche ausgefallene Storage-Volumes zu identifizieren.

- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Decommission.**)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Expansion.**)



Wenden Sie sich an den technischen Support, wenn mehr als ein Speicherknoten offline ist oder wenn ein Speicherknoten in diesem Grid in den letzten 15 Tagen neu aufgebaut wurde. Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript: Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen voneinander kann zu Datenverlust führen.

Über diese Aufgabe

Zum Abschluss dieses Vorgangs führen Sie die folgenden grundlegenden Aufgaben aus:

- Melden Sie sich beim wiederhergestellten Speicherknoten an.
- Führen Sie die aus `sn-remount-volumes` Skript zum Neumounten ordnungsgemäß formatierter Speicher-Volumes. Wenn dieses Skript ausgeführt wird, führt es Folgendes aus:
 - Hängt jedes Storage-Volume an und ab, um das XFS-Journal wiederzugeben.
 - Führt eine Konsistenzprüfung der XFS-Datei durch.
 - Wenn das Dateisystem konsistent ist, bestimmt, ob das Storage Volume ein ordnungsgemäß formatiertes StorageGRID Storage Volume ist.
 - Wenn das Storage Volume ordnungsgemäß formatiert ist, wird das Storage-Volume wieder gemountet. Alle bestehenden Daten auf dem Volume bleiben erhalten.
- Prüfen Sie die Skriptausgabe und beheben Sie etwaige Probleme.
- Führen Sie die aus `sn-recovery-postinstall.sh` Skript: Wenn dieses Skript ausgeführt wird, führt es Folgendes aus.



Starten Sie einen Storage-Node vor der Ausführung nicht während der Wiederherstellung neu `sn-recovery-postinstall.sh` (Schritt 4) zum Neuformatieren der ausgefallenen Storage Volumes und zum Wiederherstellen von Objekt-Metadaten. Vor dem Neubooten des Speicherknoten `sn-recovery-postinstall.sh` Durch das Abschließen werden Fehler bei Diensten verursacht, die zu starten versuchen, und die Knoten der StorageGRID-Appliance den Wartungsmodus beenden.

- Umformatiert alle Storage-Volumes, die von der `sn-remount-volumes` Das Skript konnte nicht gemountet werden oder es wurde festgestellt, dass es nicht ordnungsgemäß formatiert wurde.



Wenn ein Speicher-Volume neu formatiert wird, gehen alle Daten auf diesem Volume verloren. Sie müssen ein zusätzliches Verfahren durchführen, um Objektdaten von anderen Standorten im Grid wiederherzustellen, vorausgesetzt, dass ILM-Regeln für die Speicherung von mehr als einer Objektkopie konfiguriert wurden.

- Stellt die Cassandra-Datenbank bei Bedarf auf dem Node wieder her.
- Startet die Dienste auf dem Speicherknoten.

Schritte

1. Melden Sie sich beim wiederhergestellten Speicherknoten an:

- Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Führen Sie das erste Skript aus, um alle ordnungsgemäß formatierten Speicher-Volumes neu zu mounten.



Wenn alle Speicher-Volumes neu sind und formatiert werden müssen, oder wenn alle Speicher-Volumes ausgefallen sind, können Sie diesen Schritt überspringen und das zweite Skript ausführen, um alle nicht abgehängt Speicher-Volumes neu zu formatieren.

a. Führen Sie das Skript aus: `sn-remount-volumes`

Dieses Skript kann Stunden dauern, bis es auf Storage-Volumes ausgeführt wird, die Daten enthalten.

b. Überprüfen Sie die Ausgabe, während das Skript ausgeführt wird, und beantworten Sie alle Eingabeaufforderungen.



Nach Bedarf können Sie die verwenden `tail -f` Befehl zum Überwachen des Inhalts der Protokolldatei des Skripts (`/var/local/log/sn-remount-volumes.log`). Die Protokolldatei enthält ausführlichere Informationen als die Befehlsausgabe der Befehlszeile.

```
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 Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

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 Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

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 Storage-Volume erfolgreich neu eingebunden und drei Storage-Volumes wiesen Fehler auf.

- /dev/sdb Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und hatte eine gültige Volume-Struktur, so dass es erfolgreich neu eingebunden wurde. Daten auf Geräten, die vom Skript neu eingebunden 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 Speichervolumen nicht mounten kann, werden Sie gefragt, ob Sie die Konsistenzprüfung des Dateisystems ausführen möchten.
 - Wenn das Speichervolumen an eine neue Festplatte angeschlossen ist, beantworten Sie **N** mit der Eingabeaufforderung. Sie müssen das Dateisystem auf einer neuen Festplatte nicht überprüfen.
 - Wenn das Speichervolumen an eine vorhandene Festplatte angeschlossen ist, beantworten Sie **Y** mit der Eingabeaufforderung. Sie können die Ergebnisse der Dateisystemüberprüfung verwenden, um die Quelle der Beschädigung zu bestimmen. Die Ergebnisse werden im gespeichert `/var/local/log/sn-remount-volumes.log` Protokolldatei.
- `/dev/sde` Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und eine gültige Volume-Struktur hatte; die LDR-Knoten-ID befindet sich jedoch im `valid` Die Datei stimmt nicht mit der ID für diesen Speicher-knoten überein (der `configured LDR noid` Oben angezeigt). Diese Meldung gibt an, dass dieses Volume zu einem anderen Speicher-knoten gehört.

3. Prüfen Sie die Skriptausgabe und beheben Sie etwaige Probleme.



Wenn ein Speichervolumen die Konsistenzprüfung des XFS-Dateisystems fehlgeschlagen ist oder nicht gemountet werden konnte, überprüfen Sie sorgfältig die Fehlermeldungen in der Ausgabe. Sie müssen die Auswirkungen der Ausführung des verstehen `sn-recovery-postinstall.sh` Skript auf diesen Volumen.

- a. Überprüfen Sie, ob die Ergebnisse einen Eintrag für alle Volumes enthalten, die Sie erwartet haben. Wenn keine Volumes aufgeführt sind, führen Sie das Skript erneut aus.
- b. Überprüfen Sie die Meldungen für alle angeschlossenen Geräte. Stellen Sie sicher, dass keine Fehler vorliegen, die darauf hinweisen, dass ein Speichervolumen nicht zu diesem Speicher-knoten 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 Storage-Volume gemeldet wird, das zu einem anderen Storage Node gehört, wenden Sie sich an den technischen Support. Wenn Sie den ausführen `sn-recovery-postinstall.sh` Skript: Das Speichervolumen wird neu formatiert, was zu Datenverlust führen kann.

- c. Wenn keine Speichergeräte montiert werden konnten, notieren Sie sich den Gerätenamen und reparieren oder ersetzen Sie das Gerät.



Sie müssen Speichergeräte reparieren oder ersetzen, die nicht montiert werden können.

Sie verwenden den Gerätenamen, um die Volume-ID zu suchen. Dies ist erforderlich, wenn Sie den ausführen `repair-data` Skript zum Wiederherstellen von Objektdaten auf dem Volume (beim nächsten Verfahren).

- d. Führen Sie nach der Reparatur oder dem Austausch aller nicht montierbaren Geräte den aus `sn-remount-volumes` Skript erneut, um zu bestätigen, dass alle Speicher-Volumes, die neu gemountet werden können, neu eingebunden wurden.



Wenn ein Storage-Volume nicht gemountet oder nicht ordnungsgemäß formatiert werden kann und Sie mit dem nächsten Schritt fortfahren, werden das Volume und sämtliche Daten auf dem Volume gelöscht. Falls Sie zwei Kopien von Objektdaten hatten, ist nur eine einzige Kopie verfügbar, bis Sie das nächste Verfahren (Wiederherstellen von Objektdaten) abgeschlossen haben.



Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript, wenn Sie glauben, dass die auf einem ausgefallenen Storage-Volume verbleibenden Daten nicht von einer anderen Stelle im Raster neu erstellt werden können (Beispiel: Wenn Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie erstellt, oder wenn Volumes auf mehreren Nodes ausgefallen sind). Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, wie Sie Ihre Daten wiederherstellen können.

4. Führen Sie die aus `sn-recovery-postinstall.sh` Skript: `sn-recovery-postinstall.sh`

Dieses Skript formatiert alle Storage-Volumes, die nicht gemountet werden konnten oder die sich als falsch formatiert herausfanden. Darüber hinaus wird die Cassandra-Datenbank bei Bedarf auf dem Node wiederhergestellt und die Services auf dem Storage-Node gestartet.

Beachten Sie Folgendes:

- Das Skript kann Stunden in Anspruch nehmen.
- Im Allgemeinen sollten Sie die SSH-Sitzung allein 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 Netzwerkunterbrechung auftritt und die SSH-Sitzung beendet wird. Sie können jedoch den Fortschritt auf der Seite Wiederherstellung anzeigen.
- Wenn der Storage-Node den RSM-Service verwendet, wird das Skript möglicherweise 5 Minuten lang blockiert, während die Node-Services neu gestartet werden. Diese 5-minütige Verzögerung wird erwartet, wenn der RSM-Dienst zum ersten Mal startet.



Der RSM-Dienst ist auf Speicherknoten vorhanden, die den ADC-Service enthalten.



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

5. Als der `sn-recovery-postinstall.sh` Skript wird ausgeführt, überwachen Sie die Wiederherstellungsseite im Grid Manager.

Die Fortschrittsanzeige und die Spalte Phase auf der Seite Wiederherstellung geben einen allgemeinen Status des an `sn-recovery-postinstall.sh` Skript:

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
No results found.			

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT	<div style="width: 100%; height: 10px; background-color: #0070C0;"></div>	Recovering Cassandra

6. Nach dem `sn-recovery-postinstall.sh` Das Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speichervolumen wiederherstellen, die mit dem Skript formatiert wurden.

Das Skript fragt Sie, ob Sie Objektdaten manuell wiederherstellen möchten.

- In den meisten Fällen sollten Sie ["Stellen Sie Objektdaten mithilfe von Grid Manager wieder her"](#). Antwort `n` Um den Grid-Manager zu verwenden.
- In seltenen Fällen, z. B. wenn Sie vom technischen Support angewiesen werden oder wenn Sie wissen, dass für den Ersatz-Node weniger verfügbare Volumes für Objekt-Storage als der ursprüngliche Node verfügbar sind, müssen Sie dies tun ["Manuelles Wiederherstellen von Objektdaten"](#) Verwenden der `repair-data` Skript: Wenn einer dieser Fälle zutrifft, antworten Sie `y`.



Wenn Sie antworten `y` So stellen Sie Objektdaten manuell wieder her:

- Objektdaten können mit Grid Manager nicht wiederhergestellt werden.
- Sie können den Fortschritt manueller Wiederherstellungsaufträge mit Grid Manager überwachen.

Wiederherstellung von Objektdaten auf Storage Volumes für die Appliance

Nach der Wiederherstellung von Speicher-Volumen für den Appliance-Storage-Node können Sie die replizierten oder Erasure-Coded-Objektdaten wiederherstellen, die bei einem Ausfall des Storage-Node verloren gingen.

Welches Verfahren sollte ich verwenden?

Stellen Sie nach Möglichkeit Objektdaten mithilfe der Seite **Volume-Wiederherstellung** im Grid Manager wieder her.

- Wenn die Volumes unter **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Knoten** aufgeführt sind, stellen Sie Objektdaten mithilfe des wieder her ["Seite zur Volume-Wiederherstellung im Grid Manager"](#).
- Wenn die Volumes nicht unter **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Knoten** aufgeführt sind, befolgen Sie die nachstehenden Schritte zur Verwendung des `repair-data` Skript zur Wiederherstellung von Objektdaten.

Wenn der wiederhergestellte Speicher-Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie den verwenden `repair-data` Skript:

Verwenden Sie die `repair-data` Skript zur Wiederherstellung von Objektdaten

Bevor Sie beginnen

- Sie müssen bestätigt haben, dass der wiederhergestellte Speicherknoten einen Verbindungsstatus von **verbunden** hat  Auf der Registerkarte **NODES > Übersicht** im Grid Manager.

Über diese Aufgabe

Objektdaten können von anderen Storage-Nodes, einem Archiv-Node oder einem Cloud Storage-Pool wiederhergestellt werden, wenn die ILM-Regeln des Grid so konfiguriert wurden, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und sich diese Kopie auf einem ausgefallenen Storage Volume befand, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, muss StorageGRID mehrere Anfragen an den Cloud Storage Pool Endpunkt stellen, um Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Recovery-Zeitrahmens und der damit verbundenen Kosten zu erhalten.
- Wenn sich die einzige verbleibende Kopie eines Objekts auf einem Archiv-Node befindet, werden Objektdaten vom Archiv-Node abgerufen. Das Wiederherstellen von Objektdaten auf einem Storage-Node aus einem Archiv-Node dauert länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes, da die Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen zu einer Verzögerung führt.

Informationen zum `repair-data` Skript

Zum Wiederherstellen von Objektdaten führen Sie den aus `repair-data` Skript: Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans zusammen, um sicherzustellen, dass ILM-Regeln eingehalten werden.

Wählen Sie unten **replizierte Daten** oder **Erasur-codierte (EC) Daten** aus, um die verschiedenen Optionen für das zu erfahren `repair-data` Skript erstellen, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding-Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssets ausführen.



Weitere Informationen zum `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile des primären Admin-Knotens.

Replizierte Daten

Zwei Befehle sind zum Wiederherstellen replizierter Daten verfügbar, unabhängig davon, ob Sie den gesamten Node oder nur bestimmte Volumes auf dem Node 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
```

EC-Daten (Erasure Coding)

Zwei Befehle sind zum Wiederherstellen von Erasure-codierten Daten verfügbar. Dabei basiert es darauf, ob Sie den gesamten Node reparieren müssen oder nur bestimmte Volumes auf dem Node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Sie können Reparaturen von Daten, die auf Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Wenn jedoch nicht alle mit Löschkode gekennzeichneten Daten berücksichtigt werden können, kann die Reparatur nicht abgeschlossen werden. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.



Der EC-Reparaturauftrag reserviert vorübergehend eine große Menge an Lagerung. Storage-Warnmeldungen können zwar ausgelöst werden, werden aber nach Abschluss der Reparatur behoben. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturauftrag abgeschlossen wurde, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Suchen Sie nach Hostnamen für Speicherknoten

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die

wiederhergestellten Speicher-Volumen zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`.

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. Befolgen Sie die Anweisungen für **replizierte Daten, Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn nur einige Volumes gescheitert sind, gehen Sie zu [wenn nur einige Volumes ausgefallen sind](#).



Du kannst nicht laufen `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

Replizierte Daten

Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option, wo `--nodes` ist der Hostname (Systemname), um den gesamten Speicher-Node zu reparieren.

Mit diesem Befehl werden die replizierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Bei der Wiederherstellung von Objektdaten wird die Warnmeldung **Objektverlust** ausgelöst, wenn das StorageGRID-System keine replizierten Objektdaten finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Siehe "[Untersuchen Sie verlorene Objekte](#)".

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option, wo `--nodes` ist der Hostname (Systemname), um den gesamten Speicher-Node zu reparieren.

Mit diesem Befehl werden die Erasure-codierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasur-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zu [wenn alle Volumes ausgefallen sind](#).

Geben Sie die Volume-IDs in hexadezimal ein. Beispiel: 0000 ist der erste Band und 000F ist der sechzehnte Band. Sie können ein Volume, einen Bereich von Volumes oder mehrere Volumes angeben, die sich nicht in einer Sequenz befinden.

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 das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wobei `--nodes` Ist der Hostname des Node). Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf das Volume wieder her 0002 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf alle Volumes im Bereich wieder her 0003 Bis 0009 Auf einem Storage-Node mit dem Namen 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 in Volumes wieder her 0001, 0005, und 0008 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Bei der Wiederherstellung von Objektdaten wird die Warnmeldung **Objektverlust** ausgelöst, wenn das StorageGRID-System keine replizierten Objektdaten finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Notieren Sie sich die Beschreibung der Warnmeldung und die empfohlenen Maßnahmen, um die Ursache des Verlusts zu ermitteln und zu ermitteln, ob eine Wiederherstellung möglich ist.

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wobei `--nodes` Ist der Hostname des Node). Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt die mit dem Löschen kodierte Daten auf das Volume wieder her 0007 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt Daten mit Lösungscode auf alle Volumes im Bereich wieder her 0004 Bis 0006 Auf einem Storage-Node mit dem Namen 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 Erasure-codierte Daten auf Volumes wieder her 000A, 000C, und 000E Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies

`repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Überwachen Sie Reparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beides verwenden.

Sie können auch den Status der in Verarbeitung beendeten Volume-Wiederherstellungsaufträge überwachen und einen Verlauf der in abgeschlossenen Wiederherstellungsaufträge anzeigen "[Grid Manager](#)".

Replizierte Daten

- Um einen geschätzten Fertigstellungsgrad für die replizierte Reparatur zu erhalten, fügen Sie die hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES > Storage Node wird repariert > ILM**.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle 0** Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid > Storage Node wird repariert > LDR > Data Store**.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra-Inkonsistenzen sind möglicherweise vorhanden, und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM)**: Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:
 - Wählen Sie **SUPPORT > Tools > Metrics**, um die geschätzte Zeit bis zum Abschluss und den Fertigstellungsgrad für den aktuellen Job anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
 - Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data`

Betriebliche Gründe:

```
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 enthält Informationen, einschließlich `repair ID`, für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung des Appliance-Speicherknoten

Nach der Wiederherstellung eines Appliance Storage Node müssen Sie überprüfen, ob der gewünschte Status des Appliance Storage Node auf „Online“ gesetzt ist, und vergewissern Sie sich, dass der Status bei jedem Neustart des Storage Node-Servers standardmäßig online ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten > LDR > Storage > Speicherzustand — gewünscht** und **Speicherstatus — Strom**.

Der Wert beider Attribute sollte Online sein.

3. Wenn der 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 **Storage State — gewünschte** die Option **Online** aus.
 - c. Klicken Sie auf **Änderungen Übernehmen**.
 - d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherzustand — gewünscht** und **Speicherzustand — Aktuell** auf Online aktualisiert werden.

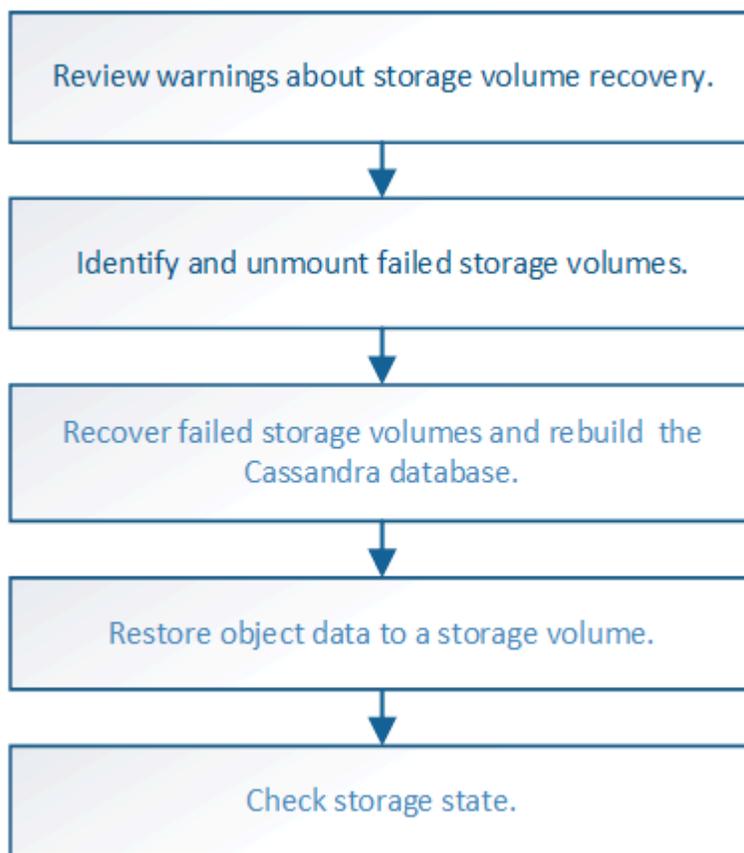
Wiederherstellung nach einem Ausfall des Speichervolumens, wenn das Systemlaufwerk intakt ist: Workflow

Sie müssen eine Reihe von Aufgaben durchführen, um einen softwarebasierten Storage Node wiederherzustellen, bei dem ein oder mehrere Storage-Volumes auf dem Storage-Node ausgefallen sind, das Systemlaufwerk jedoch intakt ist. Wenn nur Speichervolumen ausgefallen sind, steht der Speicherknoten dem StorageGRID-System weiterhin zur Verfügung.



Dieses Wiederstellungsverfahren gilt nur für softwarebasierte Speicherknoten. Wenn Speicher-Volumes auf einem Appliance Storage Node ausgefallen sind, verwenden Sie stattdessen das Verfahren der Appliance: "[Appliance Storage Node wiederherstellen](#)".

Wie im Workflow-Diagramm gezeigt, müssen Sie fehlerhafte Speicher-Volumes identifizieren und abmounten, die Volumes wiederherstellen, die Cassandra-Datenbank neu erstellen und Objektdaten wiederherstellen.



Prüfen Sie Warnungen zur Wiederherstellung des Speichervolumens

Bevor Sie fehlgeschlagene Speicher-Volumes für einen Speicherknoten wiederherstellen, müssen Sie die folgenden Warnungen überprüfen.

Die Storage-Volumes (oder Rangedbs) in einem Storage-Node werden durch eine hexadezimale Zahl identifiziert, die als Volume-ID bezeichnet wird. Zum Beispiel ist 0000 das erste Volumen und 000F das sechzehnte Volumen. Der erste Objektspeicher (Volume 0) auf jedem Storage-Node belegt bis zu 4 TB Speicherplatz für Objekt-Metadaten und Cassandra-Datenbankvorgänge. Für Objektdaten werden der

verbleibende Speicherplatz auf diesem Volume verwendet. Alle anderen Storage Volumes werden ausschließlich für Objektdaten verwendet.

Falls Volume 0 ausfällt und wiederhergestellt werden muss, kann die Cassandra-Datenbank im Rahmen des Volume-Recovery-Verfahrens neu erstellt werden. Cassandra kann unter folgenden Umständen auch wieder aufgebaut werden:

- Ein Storage-Node wird nach mehr als 15 Tagen offline wieder online geschaltet.
- Das Systemlaufwerk und ein oder mehrere Storage-Volumes ausfallen und werden wiederhergestellt.

Nach dem Rebuilt von Cassandra verwendet das System Informationen von anderen Speicherknoten. Wenn zu viele Storage-Nodes offline sind, sind einige Cassandra-Daten möglicherweise nicht verfügbar. Falls Cassandra vor Kurzem neu aufgebaut wurde, sind Cassandra-Daten möglicherweise noch nicht konsistent im gesamten Grid. Datenverluste können auftreten, wenn Cassandra neu aufgebaut wird, wenn zu viele Storage-Nodes offline sind oder wenn zwei oder mehr Storage-Nodes innerhalb von 15 Tagen neu erstellt werden.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen kann zu Datenverlust führen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Siehe "[Durchführen der Standortwiederherstellung durch den technischen Support](#)".



Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und sich die Kopie auf einem ausgefallenen Storage Volume befindet, können Sie das Objekt nicht wiederherstellen.



Wenn während der Wiederherstellung ein Alarm „Services: Status – Cassandra (SVST)“ (Services: Status – Cassandra (SVST)) angezeigt wird, siehe "[Recovery ausgefallener Storage-Volumes und Wiederherstellung der Cassandra-Datenbank](#)". Nach dem Wiederaufbau von Cassandra sollten die Alarme gelöscht werden. Wenn die Alarme nicht gelöscht werden, wenden Sie sich an den technischen Support.

Verwandte Informationen

["Warnungen und Überlegungen für die Wiederherstellung von Grid Nodes"](#)

Ermitteln und Aufheben fehlgeschlagener Storage Volumes

Bei der Wiederherstellung eines Storage-Nodes mit ausgefallenen Storage-Volumes müssen Sie die ausgefallenen Volumes identifizieren und deren Bereitstellung aufheben. Sie müssen überprüfen, ob nur die fehlgeschlagenen Speicher-Volumes im Rahmen der Wiederherstellungsverfahren neu formatiert werden.

Bevor Sie beginnen

Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

Sie sollten ausgefallene Storage Volumes so bald wie möglich wiederherstellen.

Der erste Schritt des Wiederherstellungsprozesses besteht darin, Volumes zu erkennen, die entfernt wurden, abgehängt werden müssen oder I/O-Fehler haben. Wenn weiterhin fehlgeschlagene Volumes angehängt sind, aber ein zufällig beschädigtes Dateisystem vorhanden ist, erkennt das System möglicherweise keine Beschädigung in nicht verwendeten oder nicht zugewiesenen Teilen der Festplatte.



Sie müssen dieses Verfahren abschließen, bevor Sie manuelle Schritte zur Wiederherstellung von Volumes durchführen, z. B. das Hinzufügen oder erneutes Anschließen von Festplatten, das Anhalten des Node, Starten des Node oder Neustarten. Andernfalls, wenn Sie den ausführen `reformat_storage_block_devices.rb` Skript, möglicherweise tritt ein Dateisystemfehler auf, der zum Aufhängen oder Fehlschlagen des Skripts führt.



Reparieren Sie die Hardware und schließen Sie die Festplatten ordnungsgemäß an, bevor Sie den ausführen `reboot` Befehl.



Fehlerhafte Storage-Volumes sorgfältig ermitteln Anhand dieser Informationen können Sie überprüfen, welche Volumes neu formatiert werden müssen. Sobald ein Volume neu formatiert wurde, können Daten auf dem Volume nicht wiederhergestellt werden.

Um fehlgeschlagene Speicher-Volumes korrekt wiederherzustellen, müssen Sie sowohl die Gerätenamen der ausgefallenen Speicher-Volumes als auch die zugehörigen Volume-IDs kennen.

Bei der Installation wird jedem Storage-Gerät eine UUID (Universal Unique Identifier) des Filesystems zugewiesen und über die zugewiesene Filesystem-UUID in ein `rangedb`-Verzeichnis auf dem Storage Node gemountet. Die UUID des Dateisystems und das Verzeichnis „`rangedb`“ sind im aufgeführt `/etc/fstab` Datei: Der Gerätename, das `rankgedb`-Verzeichnis und die Größe des gemounteten Volumes werden im Grid Manager angezeigt.

Im folgenden Beispiel ist das Gerät `/dev/sdc` Hat eine Volume-Größe von 4 TB, wird angehängt auf `/var/local/rangedb/0`, Verwenden des Gerätenamens `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` Im `/etc/fstab` Datei:

The diagram illustrates the storage configuration for the /var directory. It shows a tree view of /var with subdirectories like local and rangedb. The /etc/fstab file contains entries for /dev/sdc, /dev/sdd, /dev/sde, /dev/sde, /dev/tt0, /dev/cdrom, /dev/disk/by-uuid, and /dev/mapper. The 'Volumes' table provides details on the mount points, devices, status, size, space available, total entries, entries available, and write cache for each volume.

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	root	Online	10.4 GB	4.53 GB	655,360	559,513	Unknown
/var/local	cvloc	Online	96.6 GB	92.8 GB	94,369,792	94,369,445	Unknown
/var/local/rangedb/0	sdc	Online	4,396 GB	4,379 GB	858,993,408	858,983,455	Unavailable
/var/local/rangedb/1	sdd	Online	4,396 GB	4,362 GB	858,993,408	858,973,530	Unavailable
/var/local/rangedb/2	sde	Online	4,396 GB	4,370 GB	858,993,408	858,982,305	Unavailable

Schritte

1. Führen Sie die folgenden Schritte durch, um die fehlgeschlagenen Speicher-Volumes und deren Gerätenamen aufzunehmen:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Standort > fehlgeschlagener Speicherknoten > LDR > Storage > 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 **Standort > fehlgeschlagener Speicherknoten > SSM > Ressourcen > Übersicht > Haupt**. Ermitteln Sie den Mount-Punkt und die Volume-Größe jedes im vorherigen Schritt identifizierten ausgefallenen Storage-Volumes.

Objektspeichern werden in Hex-Notation nummeriert. Zum Beispiel ist 0000 das erste Volumen und 000F das sechzehnte Volumen. 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
/	root	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 fehlgeschlagenen Speicherknoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als `root` angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Führen Sie das folgende Skript aus, um die Bereitstellung eines ausgefallenen Speichervolume aufzuheben:

```
sn-unmount-volume object_store_ID
```

Der `object_store_ID` ist die ID des ausgefallenen Speicher-Volumes. Geben Sie beispielsweise an `0`. Im Befehl für einen Objektspeicher mit der ID `0000`.

4. Wenn Sie dazu aufgefordert werden, drücken Sie `y`, um den Cassandra-Service abhängig von Speichervolume `0` zu beenden.



Wenn der Cassandra-Dienst bereits angehalten wurde, werden Sie nicht dazu aufgefordert. Der Cassandra-Service wird nur für Volume `0` angehalten.

```
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.
```

In einigen Sekunden wird das Volume abgehängt. Die Meldungen werden angezeigt, die jeden Schritt des Prozesses angeben. Die letzte Meldung gibt an, dass das Volume abgehängt wurde.

5. Wenn das Unmounten fehlschlägt, weil das Volume ausgelastet ist, können Sie das Unmounten mithilfe des erzwingen `--use-umountof` Option:



Erzwingen eines Unmounting mithilfe des `--use-umountof` Die Option kann dazu führen, dass sich Prozesse oder Dienste, die das Volume verwenden, 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
```

Recovery ausgefallener Storage-Volumes und Wiederherstellung der Cassandra-Datenbank

Sie müssen ein Skript ausführen, das den Speicher auf ausgefallenen Storage-Volumes neu formatiert und neu einbindet, und die Cassandra-Datenbank auf dem Storage-Node neu erstellen, falls das System den Bedarf ermittelt.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei:
- Die Systemlaufwerke auf dem Server sind intakt.
- Die Fehlerursache wurde erkannt und ggf. Ersatz-Storage-Hardware bereits angeschafft.
- Die Gesamtgröße des Ersatzspeichers ist mit dem Original identisch.
- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Decommission.**)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Expansion.**)
- Das ist schon "[Die Warnungen zur Wiederherstellung des Speichervolumens wurden überprüft](#)".

Schritte

1. Ersetzen Sie bei Bedarf den fehlerhaften physischen oder virtuellen Speicher, der mit den fehlerhaften Speicher-Volumes verbunden ist, die Sie zuvor ermittelt und abgehängt haben.

Volumes sollten in diesem Schritt nicht erneut bereitgestellt werden. Der Speicher wird neu eingebunden und hinzugefügt `/etc/fstab` In einem späteren Schritt.

2. Gehen Sie im Grid Manager zu **NODES > appliance Storage Node > Hardware**. Überprüfen Sie im Abschnitt StorageGRID-Gerät auf der Seite, ob der Speicher-RAID-Modus ordnungsgemäß funktioniert.
3. Melden Sie sich beim fehlgeschlagenen Speicherknoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

4. Verwenden Sie einen Texteditor (`vi` oder `vim`), um fehlgeschlagene Volumes aus dem zu löschen `/etc/fstab` Datei und dann speichern Sie die Datei.



Kommentieren eines ausgefallenen Volumes in `/etc/fstab` Datei reicht nicht aus. Das Volume muss aus gelöscht werden `fstab` Während der Wiederherstellungsvorgang überprüft, ob alle Leitungen im vorhanden sind `fstab` Die Datei stimmt mit den gemounteten Dateisystemen überein.

5. Formatieren Sie alle ausgefallenen Storage-Volumes neu und stellen Sie ggf. die Cassandra-Datenbank wieder her. Geben Sie Ein: `reformat_storage_block_devices.rb`
 - Wenn Speicher-Volume 0 abgehängt ist, werden Eingabeaufforderungen und Meldungen darauf

hinweisen, dass der Cassandra-Dienst angehalten wird.

- Sie werden aufgefordert, die Cassandra-Datenbank bei Bedarf neu aufzubauen.
 - Überprüfen Sie die Warnungen. Falls keines dieser Beispiele zutreffend ist, bauen Sie die Cassandra-Datenbank neu aus. Geben Sie ein: **Y**
 - Wenn mehr als ein Speicherknoten offline ist oder wenn ein anderer Speicherknoten in den letzten 15 Tagen wieder aufgebaut wurde. Geben Sie: **N** ein

Das Skript wird beendet, ohne dass Cassandra neu aufgebaut werden muss. Wenden Sie sich an den technischen Support.

- Wenn Sie nach jedem Rangedb-Laufwerk auf dem Storage-Node 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 neu zu formatieren, das Fehler hatte. Dadurch wird das Speichervolumen neu formatiert und das neu formatierte Speichervolumen wird hinzugefügt `/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 montieren Sie das Laufwerk (wenn Sie denken, dass die Daten auf dem Laufwerk beibehalten werden sollten und das Laufwerk fehlerhaft abgehängt wurde) oder entfernen Sie das Laufwerk. Führen Sie dann die aus `reformat_storage_block_devices.rb` Befehl erneut.



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

Im folgenden Beispiel wird das Laufwerk ausgegeben `/dev/sdf` Muss neu formatiert werden, und Cassandra musste nicht neu aufgebaut 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 Speicher-Volumes neu formatiert und neu gemountet wurden und die erforderlichen Cassandra-Vorgänge abgeschlossen sind, können Sie dies tun ["Stellen Sie Objektdaten mithilfe von Grid Manager wieder her"](#).

Wiederherstellung von Objektdaten auf dem Storage Volume, auf dem das Systemlaufwerk intakt ist

Nach der Wiederherstellung eines Speicher-Volumes auf einem Speicher-Node, auf dem das Systemlaufwerk intakt ist, können Sie die replizierten oder mit Löschungen codierten Objektdaten wiederherstellen, die beim Ausfall des Speicher-Volumes verloren gingen.

Welches Verfahren sollte ich verwenden?

Stellen Sie nach Möglichkeit Objektdaten mithilfe der Seite **Volume-Wiederherstellung** im Grid Manager wieder her.

- Wenn die Volumes unter **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Knoten** aufgeführt sind, stellen Sie Objektdaten mithilfe des wieder her ["Seite zur Volume-Wiederherstellung im Grid Manager"](#).
- Wenn die Volumes nicht unter **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Knoten** aufgeführt sind, befolgen Sie die nachstehenden Schritte zur Verwendung des `repair-data` Skript zur Wiederherstellung von Objektdaten.

Wenn der wiederhergestellte Speicher-Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie den verwenden `repair-data` Skript:

Verwenden Sie die `repair-data` Skript zur Wiederherstellung von Objektdaten

Bevor Sie beginnen

- Sie müssen bestätigt haben, dass der wiederhergestellte Speicherknoten einen Verbindungsstatus von **verbunden** hat  Auf der Registerkarte **NODES > Übersicht** im Grid Manager.

Über diese Aufgabe

Objektdaten können von anderen Storage-Nodes, einem Archiv-Node oder einem Cloud Storage-Pool wiederhergestellt werden, wenn die ILM-Regeln des Grid so konfiguriert wurden, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und sich diese Kopie auf einem ausgefallenen Storage Volume befand, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, muss StorageGRID mehrere Anfragen an den Cloud Storage Pool Endpunkt stellen, um Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Recovery-Zeitrahmens und der damit verbundenen Kosten zu erhalten.
- Wenn sich die einzige verbleibende Kopie eines Objekts auf einem Archiv-Node befindet, werden Objektdaten vom Archiv-Node abgerufen. Das Wiederherstellen von Objektdaten auf einem Storage-Node aus einem Archiv-Node dauert länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes, da die Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen zu einer Verzögerung führt.

Informationen zum `repair-data` Skript

Zum Wiederherstellen von Objektdaten führen Sie den aus `repair-data` Skript: Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans zusammen, um sicherzustellen, dass ILM-Regeln eingehalten werden.

Wählen Sie unten **replizierte Daten** oder **Erasur-codierte (EC) Daten** aus, um die verschiedenen Optionen für das zu erfahrene `repair-data` Skript erstellen, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding-Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssets ausführen.



Weitere Informationen zum `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile des primären Admin-Knotens.

Replizierte Daten

Zwei Befehle sind zum Wiederherstellen replizierter Daten verfügbar, unabhängig davon, ob Sie den gesamten Node oder nur bestimmte Volumes auf dem Node 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
```

EC-Daten (Erasure Coding)

Zwei Befehle sind zum Wiederherstellen von Erasure-codierten Daten verfügbar. Dabei basiert es darauf, ob Sie den gesamten Node reparieren müssen oder nur bestimmte Volumes auf dem Node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Sie können Reparaturen von Daten, die auf Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Wenn jedoch nicht alle mit Löschkode gekennzeichneten Daten berücksichtigt werden können, kann die Reparatur nicht abgeschlossen werden. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.



Der EC-Reparaturauftrag reserviert vorübergehend eine große Menge an Lagerung. Storage-Warnmeldungen können zwar ausgelöst werden, werden aber nach Abschluss der Reparatur behoben. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturauftrag abgeschlossen wurde, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Suchen Sie nach Hostnamen für Speicherknoten

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die

wiederhergestellten Speicher-Volumen zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`.

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn nur einige Volumes gescheitert sind, gehen Sie zu [wenn nur einige Volumes ausgefallen sind](#).



Du kannst nicht laufen `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

Replizierte Daten

Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option, wo `--nodes` ist der Hostname (Systemname), um den gesamten Speicher-Node zu reparieren.

Mit diesem Befehl werden die replizierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Bei der Wiederherstellung von Objektdaten wird die Warnmeldung **Objektverlust** ausgelöst, wenn das StorageGRID-System keine replizierten Objektdaten finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Siehe "[Untersuchen Sie verlorene Objekte](#)".

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option, wo `--nodes` ist der Hostname (Systemname), um den gesamten Speicher-Node zu reparieren.

Mit diesem Befehl werden die Erasure-codierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasur-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zu [wenn alle Volumes ausgefallen sind](#).

Geben Sie die Volume-IDs in hexadezimal ein. Beispiel: 0000 ist der erste Band und 000F ist der sechzehnte Band. Sie können ein Volume, einen Bereich von Volumes oder mehrere Volumes angeben, die sich nicht in einer Sequenz befinden.

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 das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wobei `--nodes` Ist der Hostname des Node). Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf das Volume wieder her 0002 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf alle Volumes im Bereich wieder her 0003 Bis 0009 Auf einem Storage-Node mit dem Namen 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 in Volumes wieder her 0001, 0005, und 0008 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Bei der Wiederherstellung von Objektdaten wird die Warnmeldung **Objektverlust** ausgelöst, wenn das StorageGRID-System keine replizierten Objektdaten finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Notieren Sie sich die Beschreibung der Warnmeldung und die empfohlenen Maßnahmen, um die Ursache des Verlusts zu ermitteln und zu ermitteln, ob eine Wiederherstellung möglich ist.

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wobei `--nodes` Ist der Hostname des Node). Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt die mit dem Löschen kodierte Daten auf das Volume wieder her 0007 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt Daten mit Lösungscode auf alle Volumes im Bereich wieder her 0004 Bis 0006 Auf einem Storage-Node mit dem Namen 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 Erasure-codierte Daten auf Volumes wieder her 000A, 000C, und 000E Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies

`repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Überwachen Sie Reparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beides verwenden.

Sie können auch den Status der in Verarbeitung beendeten Volume-Wiederherstellungsaufträge überwachen und einen Verlauf der in abgeschlossenen Wiederherstellungsaufträge anzeigen "[Grid Manager](#)".

Replizierte Daten

- Um einen geschätzten Fertigstellungsgrad für die replizierte Reparatur zu erhalten, fügen Sie die hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES > Storage Node wird repariert > ILM**.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle 0** Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid > Storage Node wird repariert > LDR > Data Store**.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra-Inkonsistenzen sind möglicherweise vorhanden, und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM)**: Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:
 - Wählen Sie **SUPPORT > Tools > Metrics**, um die geschätzte Zeit bis zum Abschluss und den Fertigstellungsgrad für den aktuellen Job anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
 - Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data`

Betriebliche Gründe:

```
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 enthält Informationen, einschließlich `repair ID`, für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung von Storage Volumes

Nach der Wiederherstellung von Speichervolumes müssen Sie überprüfen, ob der gewünschte Status des Speicherknoten auf „Online“ gesetzt ist, und sicherstellen, dass der Status beim Neustart des Speicherknotenservers standardmäßig online ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten > LDR > Storage > Speicherzustand — gewünscht** und **Speicherstatus — Strom**.

Der Wert beider Attribute sollte Online sein.

3. Wenn der 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 **Storage State — gewünschte** die Option **Online** aus.
 - c. Klicken Sie Auf **Änderungen Übernehmen**.
 - d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherzustand — gewünscht** und **Speicherzustand — Aktuell** auf Online aktualisiert werden.

Wiederherstellung nach einem Laufwerksausfall

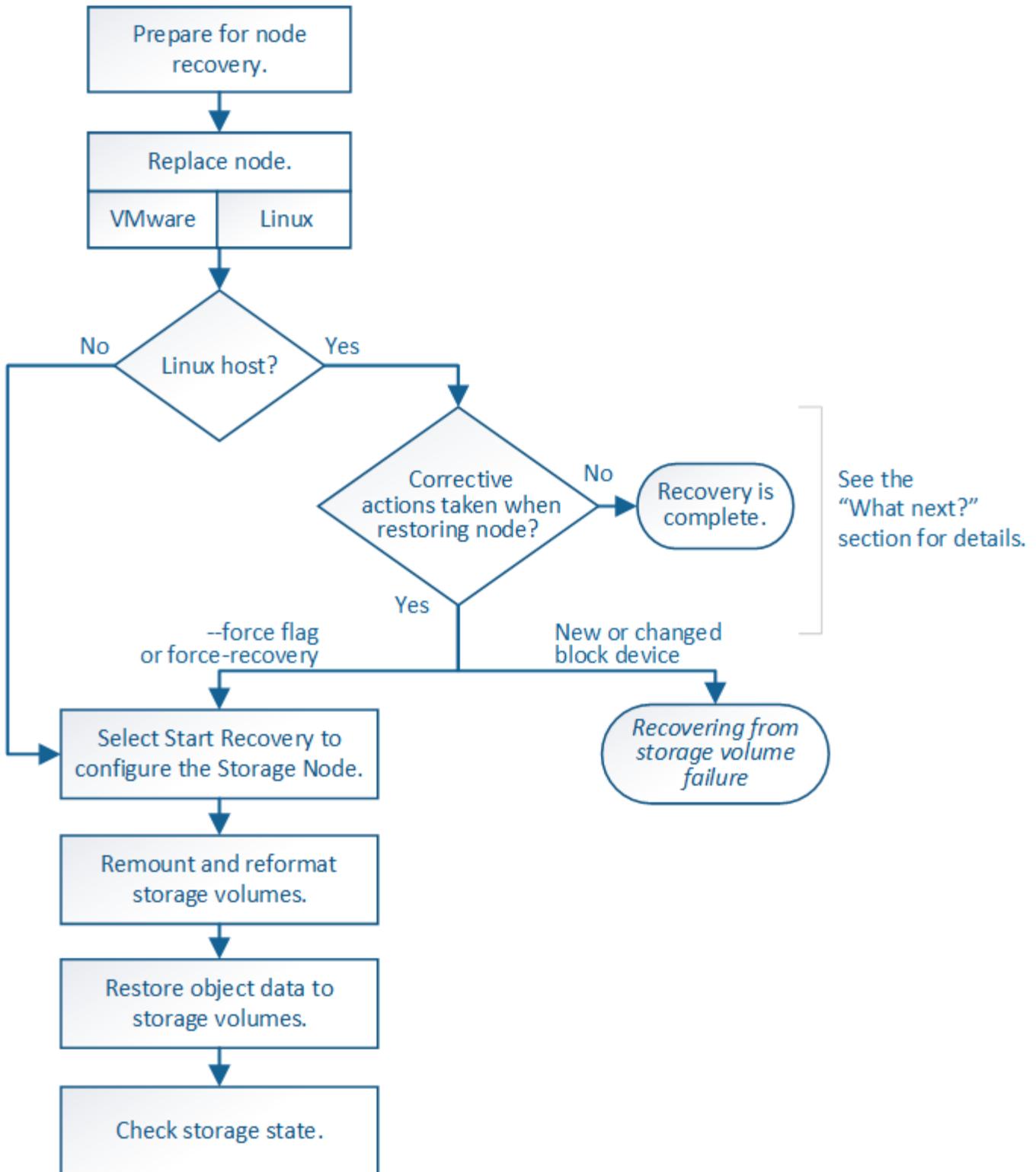
Wiederherstellung nach einem Systemlaufwerk-Fehler: Workflow

Wenn das Systemlaufwerk auf einem softwarebasierten Speicherknoten ausgefallen ist, steht der Speicherknoten dem StorageGRID-System nicht zur Verfügung. Sie müssen einen bestimmten Satz von Aufgaben zur Wiederherstellung nach einem Systemausfall ausführen.

Gehen Sie folgendermaßen vor, um nach einem Systemlaufwerksausfall auf einem softwarebasierten Speicherknoten wiederherzustellen. Dieses Verfahren umfasst die Schritte, die Sie befolgen sollten, wenn Speicher-Volumes ebenfalls ausgefallen sind oder nicht neu gemountet werden können.



Dieses Verfahren gilt nur für softwarebasierte Speicherknoten. Sie müssen eine andere Vorgehensweise als befolgen "[Stellen Sie einen Appliance-Storage-Node wieder her](#)".



Prüfen Sie die Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken

Überprüfen Sie vor der Wiederherstellung eines fehlerhaften Systemlaufwerks eines Storage-Knotens die allgemeine ["Warnungen und Überlegungen zur Wiederherstellung des Grid Node"](#) Und die folgenden spezifischen Warnungen.

Storage-Nodes verfügen über eine Cassandra Datenbank mit Objekt-Metadaten. Unter folgenden Umständen kann die Cassandra-Datenbank neu erstellt werden:

- Ein Storage-Node wird nach mehr als 15 Tagen offline wieder online geschaltet.
- Ein Speichervolume ist ausgefallen und wurde wiederhergestellt.
- Das Systemlaufwerk und ein oder mehrere Storage-Volumes ausfallen und werden wiederhergestellt.

Nach dem Rebuild von Cassandra verwendet das System Informationen von anderen Speicherknoten. Wenn zu viele Storage-Nodes offline sind, sind einige Cassandra-Daten möglicherweise nicht verfügbar. Falls Cassandra vor Kurzem neu aufgebaut wurde, sind Cassandra-Daten möglicherweise noch nicht konsistent im gesamten Grid. Datenverluste können auftreten, wenn Cassandra neu aufgebaut wird, wenn zu viele Storage-Nodes offline sind oder wenn zwei oder mehr Storage-Nodes innerhalb von 15 Tagen neu erstellt werden.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie das folgende Wiederherstellungsverfahren nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen kann zu Datenverlust führen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Siehe "[Durchführen der Standortwiederherstellung durch den technischen Support](#)".



Wenn sich dieser Speicherknoten im schreibgeschützten Wartungsmodus befindet, um das Abrufen von Objekten durch einen anderen Speicherknoten mit ausgefallenen Speichervolumen zu ermöglichen, stellen Sie Volumes auf dem Speicherknoten mit fehlerhaften Speichervolumen wieder her, bevor Sie diesen fehlgeschlagenen Speicherknoten wiederherstellen. Siehe die Anweisungen zu "[Wiederherstellung nach einem Ausfall des Speicher-Volumen bei intakt des Systemlaufwerks](#)".



Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und sich die Kopie auf einem ausgefallenen Storage Volume befindet, können Sie das Objekt nicht wiederherstellen.



Wenn während der Wiederherstellung ein Alarm „Services: Status – Cassandra (SVST)“ (Services: Status – Cassandra (SVST)) angezeigt wird, siehe "[Recovery ausgefallener Storage-Volumes und Wiederherstellung der Cassandra-Datenbank](#)". Nach dem Wiederaufbau von Cassandra sollten die Alarme gelöscht werden. Wenn die Alarme nicht gelöscht werden, wenden Sie sich an den technischen Support.

Ersetzen Sie den Speicherknoten

Wenn das Systemlaufwerk ausgefallen ist, müssen Sie zuerst den Speicherknoten ersetzen.

Sie müssen das Verfahren zum Ersetzen des Node für Ihre Plattform auswählen. Die Schritte zum Ersetzen eines Node sind für alle Typen von Grid-Nodes identisch.



Dieses Verfahren gilt nur für softwarebasierte Speicherknoten. Sie müssen eine andere Vorgehensweise als befolgen "[Stellen Sie einen Appliance-Storage-Node wieder her](#)".

Linux: Wenn Sie sich nicht sicher sind, ob Ihr Systemlaufwerk ausgefallen ist, folgen Sie den Anweisungen, um den Knoten zu ersetzen, um festzustellen, welche Wiederherstellungsschritte erforderlich sind.

Plattform	Verfahren
VMware	"Einen VMware-Knoten ersetzen"
Linux	"Ersetzen Sie einen Linux-Knoten"
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren für "Ersetzen eines Linux-Knotens" .

Wählen Sie Wiederherstellung starten, um Speicherknoten zu konfigurieren

Nachdem Sie einen Speicherknoten ersetzt haben, müssen Sie im Grid Manager die Option Wiederherstellung starten auswählen, um den neuen Knoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben die Provisionierungs-Passphrase.
- Sie haben den Ersatzknoten bereitgestellt und konfiguriert.
- Sie haben das Startdatum aller Reparaturaufträge für Daten, die mit dem Verfahren zur Fehlerkorrektur codiert wurden.
- Sie haben überprüft, ob der Speicher-Node innerhalb der letzten 15 Tage nicht neu erstellt wurde.

Über diese Aufgabe

Wenn der Storage-Node als Container auf einem Linux-Host installiert ist, müssen Sie diesen Schritt nur ausführen, wenn einer dieser Schritte zutrifft:

- Man musste das benutzen `--force` Flag, um den Knoten zu importieren, oder Sie haben ausgegeben `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 **MAINTENANCE > Tasks > Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden in der Liste angezeigt, wenn sie fehlschlagen. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und für die Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknotten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das anzeigt, dass der Knoten in einem unbestimmten Zustand bleibt, wenn Sie das Verfahren zurücksetzen.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux:** Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen:
`storagegrid node force-recovery node-name`

6. Wenn der Speicher-Node die Phase „Warten auf manuelle Schritte“ erreicht hat, fahren Sie mit fort ["Speicher-Volumes neu einbinden und formatieren \(manuelle Schritte\)"](#).

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT	<div style="width: 100%; height: 10px; background-color: #0070C0;"></div>	Waiting For Manual Steps

Reset

Speicher-Volumes neu einbinden und formatieren (manuelle Schritte)

Sie müssen zwei Skripte manuell ausführen, um die erhaltenen Storage Volumes neu einzubinden und ausgefallene Storage Volumes neu zu formatieren. Das erste Skript bindet Volumes wieder ein, die ordnungsgemäß als StorageGRID-Storage-Volumes formatiert sind. Das zweite Skript formatiert alle nicht abgehängt Volumes neu, stellt Cassandra bei Bedarf wieder her und startet Services.

Bevor Sie beginnen

- Sie haben bereits die Hardware für alle ausgefallenen Storage Volumes ausgetauscht, die ausgetauscht werden müssen.

Ausführen des `sn-remount-volumes` Skript kann Ihnen helfen, zusätzliche ausgefallene Storage-Volumes zu identifizieren.

- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Decommission**.)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Expansion**.)
- Das ist schon ["Überprüfen Sie die Warnungen für die Wiederherstellung des Speicherknoten-Systemlaufwerks"](#).



Wenden Sie sich an den technischen Support, wenn mehr als ein Speicherknoten offline ist oder wenn ein Speicherknoten in diesem Grid in den letzten 15 Tagen neu aufgebaut wurde. Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript: Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen voneinander kann zu Datenverlust führen.

Über diese Aufgabe

Zum Abschluss dieses Vorgangs führen Sie die folgenden grundlegenden Aufgaben aus:

- Melden Sie sich beim wiederhergestellten Speicherknoten an.
- Führen Sie die aus `sn-remount-volumes` Skript zum Neumounten ordnungsgemäß formatierter Speicher-Volumes. Wenn dieses Skript ausgeführt wird, führt es Folgendes aus:
 - Hängt jedes Storage-Volume an und ab, um das XFS-Journal wiederzugeben.

- Führt eine Konsistenzprüfung der XFS-Datei durch.
- Wenn das Dateisystem konsistent ist, bestimmt, ob das Storage Volume ein ordnungsgemäß formatiertes StorageGRID Storage Volume ist.
- Wenn das Storage Volume ordnungsgemäß formatiert ist, wird das Storage-Volume wieder gemountet. Alle bestehenden Daten auf dem Volume bleiben erhalten.
- Prüfen Sie die Skriptausgabe und beheben Sie etwaige Probleme.
- Führen Sie die aus `sn-recovery-postinstall.sh` Skript: Wenn dieses Skript ausgeführt wird, führt es Folgendes aus.



Starten Sie einen Storage-Node vor der Ausführung nicht während der Wiederherstellung neu `sn-recovery-postinstall.sh` Formatieren ausgefallener Storage-Volumes und Wiederherstellen von Objekt-Metadaten Vor dem Neubooten des Speicherknoten `sn-recovery-postinstall.sh` Durch das Abschließen werden Fehler bei Diensten verursacht, die zu starten versuchen, und die Knoten der StorageGRID-Appliance den Wartungsmodus beenden. Siehe den Schritt für [Skript nach der Installation](#).

- Umformatiert alle Storage-Volumes, die von der `sn-remount-volumes` Das Skript konnte nicht gemountet werden oder es wurde festgestellt, dass es nicht ordnungsgemäß formatiert wurde.



Wenn ein Speicher-Volume neu formatiert wird, gehen alle Daten auf diesem Volume verloren. Sie müssen ein zusätzliches Verfahren durchführen, um Objektdaten von anderen Standorten im Grid wiederherzustellen, vorausgesetzt, dass ILM-Regeln für die Speicherung von mehr als einer Objektkopie konfiguriert wurden.

- Stellt die Cassandra-Datenbank bei Bedarf auf dem Node wieder her.
- 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Führen Sie das erste Skript aus, um alle ordnungsgemäß formatierten Speicher-Volumes neu zu mounten.



Wenn alle Speicher-Volumes neu sind und formatiert werden müssen, oder wenn alle Speicher-Volumes ausgefallen sind, können Sie diesen Schritt überspringen und das zweite Skript ausführen, um alle nicht abgehängt Speicher-Volumes neu zu formatieren.

- a. Führen Sie das Skript aus: `sn-remount-volumes`

Dieses Skript kann Stunden dauern, bis es auf Storage-Volumes ausgeführt wird, die Daten enthalten.

- b. Überprüfen Sie die Ausgabe, während das Skript ausgeführt wird, und beantworten Sie alle Eingabeaufforderungen.



Nach Bedarf können Sie die verwenden `tail -f` Befehl zum Überwachen des Inhalts der Protokolldatei des Skripts (`/var/local/log/sn-remount-volumes.log`). Die Protokolldatei enthält ausführlichere Informationen als die Befehlsausgabe der Befehlszeile.

```
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 Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

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 Webscale will attempt to restore data redundancy by making additional replicated copies or EC fragments, according to the rules in the active ILM policy.

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 Storage-Volume erfolgreich neu eingebunden und drei Storage-Volumes wiesen Fehler auf.

- `/dev/sdb` Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und hatte eine gültige Volume-Struktur, so dass es erfolgreich neu eingebunden wurde. Daten auf Geräten, die vom Skript neu eingebunden 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 Speichervolumen an eine neue Festplatte angeschlossen ist, beantworten Sie **N** mit der Eingabeaufforderung. Sie müssen das Dateisystem auf einer neuen Festplatte nicht überprüfen.
 - Wenn das Speichervolumen an eine vorhandene Festplatte angeschlossen ist, beantworten Sie **Y** mit der Eingabeaufforderung. Sie können die Ergebnisse der Dateisystemüberprüfung verwenden, um die Quelle der Beschädigung zu bestimmen. Die Ergebnisse werden im gespeichert `/var/local/log/sn-remount-volumes.log` Protokolldatei.
- `/dev/sde` Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und eine gültige Volume-Struktur hatte. Die LDR-Knoten-ID in der `volID`-Datei stimmt jedoch nicht mit der ID für diesen Storage-Node überein (die `configured LDR noid` Oben angezeigt). Diese Meldung gibt an, dass dieses Volume zu einem anderen Speicherknoten gehört.

3. Prüfen Sie die Skriptausgabe und beheben Sie etwaige Probleme.



Wenn ein Speichervolume die Konsistenzprüfung des XFS-Dateisystems fehlgeschlagen ist oder nicht gemountet werden konnte, überprüfen Sie sorgfältig die Fehlermeldungen in der Ausgabe. Sie müssen die Auswirkungen der Ausführung des verstehen `sn-recovery-postinstall.sh` Skript auf diesen Volumes.

- a. Überprüfen Sie, ob die Ergebnisse einen Eintrag für alle Volumes enthalten, die Sie erwartet haben. Wenn keine Volumes aufgeführt sind, führen Sie das Skript erneut aus.
- b. Überprüfen Sie die Meldungen für alle angeschlossenen Geräte. Stellen Sie sicher, dass keine Fehler vorliegen, die darauf hinweisen, dass ein Speichervolume nicht zu diesem Speicherknoten gehört.

Im Beispiel 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 Storage-Volume gemeldet wird, das zu einem anderen Storage Node gehört, wenden Sie sich an den technischen Support. Wenn Sie den ausführen `sn-recovery-postinstall.sh` Skript: Das Speichervolumen wird neu formatiert, was zu Datenverlust führen kann.

- c. Wenn keine Speichergeräte montiert werden konnten, notieren Sie sich den Gerätenamen und reparieren oder ersetzen Sie das Gerät.



Sie müssen Speichergeräte reparieren oder ersetzen, die nicht montiert werden können.

Sie verwenden den Gerätenamen, um die Volume-ID zu suchen. Dies ist erforderlich, wenn Sie den ausführen `repair-data` Skript zum Wiederherstellen von Objektdaten auf dem Volume (beim nächsten Verfahren).

- d. Führen Sie nach der Reparatur oder dem Austausch aller nicht montierbaren Geräte den aus `sn-remount-volumes` Skript erneut, um zu bestätigen, dass alle Speicher-Volumes, die neu gemountet werden können, neu eingebunden wurden.



Wenn ein Storage-Volume nicht gemountet oder nicht ordnungsgemäß formatiert werden kann und Sie mit dem nächsten Schritt fortfahren, werden das Volume und sämtliche Daten auf dem Volume gelöscht. Falls Sie zwei Kopien von Objektdaten hatten, ist nur eine einzige Kopie verfügbar, bis Sie das nächste Verfahren (Wiederherstellen von Objektdaten) abgeschlossen haben.



Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript, wenn Sie glauben, dass die auf einem ausgefallenen Storage-Volume verbleibenden Daten nicht von einer anderen Stelle im Raster neu erstellt werden können (Beispiel: Wenn Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie erstellt, oder wenn Volumes auf mehreren Nodes ausgefallen sind). Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, wie Sie Ihre Daten wiederherstellen können.

4. Führen Sie die aus `sn-recovery-postinstall.sh` Skript: `sn-recovery-postinstall.sh`

Dieses Skript formatiert alle Storage-Volumes, die nicht gemountet werden konnten oder die sich als falsch formatiert herausfanden. Darüber hinaus wird die Cassandra-Datenbank bei Bedarf auf dem Node wiederhergestellt und die Services auf dem Storage-Node gestartet.

Beachten Sie Folgendes:

- Das Skript kann Stunden in Anspruch nehmen.
- Im Allgemeinen sollten Sie die SSH-Sitzung allein 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 Netzwerkunterbrechung auftritt und die SSH-Sitzung beendet wird. Sie können jedoch den Fortschritt auf der Seite Wiederherstellung anzeigen.
- Wenn der Storage-Node den RSM-Service verwendet, wird das Skript möglicherweise 5 Minuten lang blockiert, während die Node-Services neu gestartet werden. Diese 5-minütige Verzögerung wird erwartet, wenn der RSM-Dienst zum ersten Mal startet.



Der RSM-Dienst ist auf Speicherknoten vorhanden, die den ADC-Service enthalten.



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

5. als `sn-recovery-postinstall.sh` Skript wird ausgeführt, überwachen Sie die

Wiederherstellungsseite im Grid Manager.

Die Fortschrittsanzeige und die Spalte Phase auf der Seite Wiederherstellung geben einen allgemeinen Status des an `sn-recovery-postinstall.sh` Skript:

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
No results found.			

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT	<div style="width: 50%; background-color: #0070C0; height: 10px;"></div>	Recovering Cassandra

6. Nach dem `sn-recovery-postinstall.sh` Das Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speichervolumen wiederherstellen, die mit dem Skript formatiert wurden.

Das Skript fragt Sie, ob Sie Objektdaten manuell wiederherstellen möchten.

- In den meisten Fällen sollten Sie "[Stellen Sie Objektdaten mithilfe von Grid Manager wieder her](#)". Antwort `n` Um den Grid-Manager zu verwenden.
- In seltenen Fällen, z. B. wenn Sie vom technischen Support angewiesen werden oder wenn Sie wissen, dass für den Ersatz-Node weniger verfügbare Volumens für Objekt-Storage als der ursprüngliche Node verfügbar sind, müssen Sie dies tun "[Manuelles Wiederherstellen von Objektdaten](#)" Verwenden der `repair-data` Skript: Wenn einer dieser Fälle zutrifft, antworten Sie `y`.

Wenn Sie antworten `y` So stellen Sie Objektdaten manuell wieder her:



- Objektdaten können mit Grid Manager nicht wiederhergestellt werden.
- Sie können den Fortschritt manueller Wiederherstellungsaufträge mit Grid Manager überwachen.

Wiederherstellung von Objektdaten auf einem Storage-Volume (Systemausfall)

Nach der Wiederherstellung von Speicher-Volumen für einen nicht-Appliance-Storage-Node können Sie die replizierten oder mit Löschungen codierten Objektdaten wiederherstellen, die bei einem Ausfall des Storage-Node verloren gingen.

Welches Verfahren sollte ich verwenden?

Stellen Sie nach Möglichkeit Objektdaten mithilfe der Seite **Volume-Wiederherstellung** im Grid Manager wieder her.

- Wenn die Volumens unter **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Knoten** aufgeführt sind, stellen Sie Objektdaten mithilfe des wieder her "[Seite zur Volume-](#)

Wiederherstellung im Grid Manager".

- Wenn die Volumes nicht unter **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Knoten** aufgeführt sind, befolgen Sie die nachstehenden Schritte zur Verwendung des `repair-data` Skript zur Wiederherstellung von Objektdaten.

Wenn der wiederhergestellte Speicher-Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie den verwenden `repair-data` Skript:

Verwenden Sie die `repair-data` Skript zur Wiederherstellung von Objektdaten

Bevor Sie beginnen

- Sie müssen bestätigt haben, dass der wiederhergestellte Speicherknoten einen Verbindungsstatus von **verbunden** hat  Auf der Registerkarte **NODES > Übersicht** im Grid Manager.

Über diese Aufgabe

Objektdaten können von anderen Storage-Nodes, einem Archiv-Node oder einem Cloud Storage-Pool wiederhergestellt werden, wenn die ILM-Regeln des Grid so konfiguriert wurden, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und sich diese Kopie auf einem ausgefallenen Storage Volume befand, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, muss StorageGRID mehrere Anfragen an den Cloud Storage Pool Endpunkt stellen, um Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Recovery-Zeitrahmens und der damit verbundenen Kosten zu erhalten.
- Wenn sich die einzige verbleibende Kopie eines Objekts auf einem Archiv-Node befindet, werden Objektdaten vom Archiv-Node abgerufen. Das Wiederherstellen von Objektdaten auf einem Storage-Node aus einem Archiv-Node dauert länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes, da die Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen zu einer Verzögerung führt.

Informationen zum `repair-data` Skript

Zum Wiederherstellen von Objektdaten führen Sie den aus `repair-data` Skript: Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans zusammen, um sicherzustellen, dass ILM-Regeln eingehalten werden.

Wählen Sie unten **replizierte Daten** oder **Erasur-codierte (EC) Daten** aus, um die verschiedenen Optionen für das zu erfahren `repair-data` Skript erstellen, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding-Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssets ausführen.



Weitere Informationen zum `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile des primären Admin-Knotens.

Replizierte Daten

Zwei Befehle sind zum Wiederherstellen replizierter Daten verfügbar, unabhängig davon, ob Sie den gesamten Node oder nur bestimmte Volumes auf dem Node 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
```

EC-Daten (Erasure Coding)

Zwei Befehle sind zum Wiederherstellen von Erasure-codierten Daten verfügbar. Dabei basiert es darauf, ob Sie den gesamten Node reparieren müssen oder nur bestimmte Volumes auf dem Node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Sie können Reparaturen von Daten, die auf Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Wenn jedoch nicht alle mit Löschkode gekennzeichneten Daten berücksichtigt werden können, kann die Reparatur nicht abgeschlossen werden. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.



Der EC-Reparaturauftrag reserviert vorübergehend eine große Menge an Lagerung. Storage-Warnmeldungen können zwar ausgelöst werden, werden aber nach Abschluss der Reparatur behoben. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturauftrag abgeschlossen wurde, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Suchen Sie nach Hostnamen für Speicherknoten

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die

wiederhergestellten Speicher-Volumen zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`.

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. Befolgen Sie die Anweisungen für **replizierte Daten, Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn nur einige Volumes gescheitert sind, gehen Sie zu [wenn nur einige Volumes ausgefallen sind](#).



Du kannst nicht laufen `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

Replizierte Daten

Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option, wo `--nodes` Ist der Hostname (Systemname), um den gesamten Speicher-Node zu reparieren.

Mit diesem Befehl werden die replizierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Bei der Wiederherstellung von Objektdaten wird die Warnmeldung **Objektverlust** ausgelöst, wenn das StorageGRID-System keine replizierten Objektdaten finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Siehe "[Untersuchen Sie verlorene Objekte](#)".

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option, wo `--nodes` Ist der Hostname (Systemname), um den gesamten Speicher-Node zu reparieren.

Mit diesem Befehl werden die Erasure-codierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasur-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasur-codierte (EC) Daten oder beide verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zu [wenn alle Volumes ausgefallen sind](#).

Geben Sie die Volume-IDs in hexadezimal ein. Beispiel: 0000 ist der erste Band und 000F ist der sechzehnte Band. Sie können ein Volume, einen Bereich von Volumes oder mehrere Volumes angeben, die sich nicht in einer Sequenz befinden.

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 das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wobei `--nodes` Ist der Hostname des Node). Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf das Volume wieder her 0002 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf alle Volumes im Bereich wieder her 0003 Bis 0009 Auf einem Storage-Node mit dem Namen 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 in Volumes wieder her 0001, 0005, und 0008 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Bei der Wiederherstellung von Objektdaten wird die Warnmeldung **Objektverlust** ausgelöst, wenn das StorageGRID-System keine replizierten Objektdaten finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Notieren Sie sich die Beschreibung der Warnmeldung und die empfohlenen Maßnahmen, um die Ursache des Verlusts zu ermitteln und zu ermitteln, ob eine Wiederherstellung möglich ist.

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens (wobei `--nodes` Ist der Hostname des Node). Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt die mit dem Löschen kodierte Daten auf das Volume wieder her 0007 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt Daten mit Lösungscode auf alle Volumes im Bereich wieder her 0004 Bis 0006 Auf einem Storage-Node mit dem Namen 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 Erasure-codierte Daten auf Volumes wieder her 000A, 000C, und 000E Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies

`repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Überwachen Sie Reparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beides verwenden.

Sie können auch den Status der in Verarbeitung beendeten Volume-Wiederherstellungsaufträge überwachen und einen Verlauf der in abgeschlossenen Wiederherstellungsaufträge anzeigen "[Grid Manager](#)".

Replizierte Daten

- Um einen geschätzten Fertigstellungsgrad für die replizierte Reparatur zu erhalten, fügen Sie die hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES > Storage Node wird repariert > ILM**.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle 0** Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid > Storage Node wird repariert > LDR > Data Store**.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra-Inkonsistenzen sind möglicherweise vorhanden, und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM)**: Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:
 - Wählen Sie **SUPPORT > Tools > Metrics**, um die geschätzte Zeit bis zum Abschluss und den Fertigstellungsgrad für den aktuellen Job anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
 - Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data`

Betriebliche Gründe:

```
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 enthält Informationen, einschließlich `repair ID`, für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung des Speicherknoten-Systemlaufwerks

Nach der Wiederherstellung des Systemlaufwerks für einen Speicherknoten müssen Sie überprüfen, ob der gewünschte Status des Speicherknoten auf Online gesetzt ist, und vergewissern Sie sich, dass der Status beim Neustart des Speicherknotenservers standardmäßig online ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten > LDR > Storage > Speicherzustand — gewünscht** und **Speicherstatus — Strom**.

Der Wert beider Attribute sollte Online sein.

3. Wenn der 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 **Storage State — gewünschte** die Option **Online** aus.
 - c. Klicken Sie Auf **Änderungen Übernehmen**.
 - d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherzustand — gewünscht** und **Speicherzustand — Aktuell** auf Online aktualisiert werden.

Stellen Sie Objektdaten mithilfe von Grid Manager wieder her

Mithilfe von Grid Manager können Sie Objektdaten für ein fehlerhaftes Speicher-Volumen oder einen Speicher-Node wiederherstellen. Sie können den Grid Manager auch verwenden, um laufende Wiederherstellungsprozesse zu überwachen und einen Wiederherstellungsverlauf anzuzeigen.

Bevor Sie beginnen

- Sie haben eine der folgenden Verfahren zum Formatieren fehlgeschlagener Volumes durchgeführt:
 - ["Appliance-Storage-Volumes neu einbinden und formatieren \(manuelle Schritte\)"](#)
 - ["Speicher-Volumes neu einbinden und formatieren \(manuelle Schritte\)"](#)
- Sie haben bestätigt, dass der Speicher-Node, auf dem Sie Objekte wiederherstellen, den Verbindungsstatus **Verbunden** hat  Auf der Registerkarte **NODES > Übersicht** im Grid Manager.
- Sie haben Folgendes bestätigt:
 - Eine Grid-Erweiterung zum Hinzufügen eines Storage-Knotens wird nicht ausgeführt.
 - Die Stilllegung des Storage-Node wird nicht ausgeführt oder ist fehlgeschlagen.
 - Eine Recovery eines ausgefallenen Storage-Volumes wird nicht ausgeführt.
 - Eine Wiederherstellung eines Storage-Knotens mit einem ausgefallenen Systemlaufwerk wird nicht ausgeführt.
 - Es wird kein EC-Neuausgleich durchgeführt.
 - Das Klonen von Appliance-Nodes wird nicht ausgeführt.

Über diese Aufgabe

Nachdem Sie die Laufwerke ersetzt und die manuellen Schritte zum Formatieren der Volumes durchgeführt haben, zeigt Grid Manager die Volumes als Kandidaten für die Wiederherstellung auf der Registerkarte **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Nodes** an.

Stellen Sie nach Möglichkeit Objektdaten mithilfe der Seite **Volume-Wiederherstellung** im Grid Manager wieder her. Befolgen Sie diese Richtlinien:

- Wenn die Volumes unter **MAINTENANCE > Volume-Wiederherstellung > zu wiederherstellende Knoten** aufgeführt sind, stellen Sie Objektdaten wie in den Schritten unten beschrieben wieder her. Die Volumes werden aufgelistet, wenn:
 - Einige, aber nicht alle Storage-Volumes in einem Node sind ausgefallen
 - Alle Speicher-Volumes in einem Node sind ausgefallen und werden durch dieselbe Anzahl von Volumes oder mehr ersetzt

Auf der Seite **Volume-Wiederherstellung** im Grid Manager können Sie außerdem die folgenden Optionen aufrufen [Überwachen Sie den Wiederherstellungsprozess für Volumes](#) Und [Wiederherstellungsverlauf anzeigen](#).

- Wenn die Volumes im Grid Manager nicht als Kandidaten für die Wiederherstellung aufgeführt sind, befolgen Sie die entsprechenden Schritte zur Verwendung von `repair-data` Skript zur Wiederherstellung von Objektdaten:
 - ["Wiederherstellung von Objektdaten im Storage-Volumen \(Systemausfall\)"](#)
 - ["Wiederherstellung von Objektdaten auf dem Storage Volume, auf dem das Systemlaufwerk intakt ist"](#)

- "Wiederherstellung von Objektdaten auf Storage Volumes für die Appliance"

Wenn der wiederhergestellte Speicher-Node weniger Volumes enthält als der Knoten, den er ersetzt, müssen Sie den verwenden `repair-data` Skript:

Sie können zwei Typen von Objektdaten wiederherstellen:

- Replizierte Datenobjekte werden von anderen Speicherorten wiederhergestellt, unter der Annahme, dass die ILM-Regeln des Grids für die Bereitstellung von Objektkopien konfiguriert wurden.
 - Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und sich diese Kopie auf einem ausgefallenen Storage Volume befand, können Sie das Objekt nicht wiederherstellen.
 - Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, muss StorageGRID mehrere Anfragen an den Cloud Storage Pool Endpunkt stellen, um Objektdaten wiederherzustellen.
 - Wenn sich die einzige verbleibende Kopie eines Objekts auf einem Archiv-Node befindet, werden Objektdaten vom Archiv-Node abgerufen. Die Wiederherstellung von Objektdaten auf einem Storage Node von einem Archive Node dauert länger als die Wiederherstellung von Objektkopien von anderen Storage Nodes.
- Datenobjekte, die mit dem Erasure Coded (EC) codiert wurden, werden durch Neuzusammensetzen der gespeicherten Fragmente wiederhergestellt. Beschädigte oder verlorene Fragmente werden durch den Erasure-Coding-Algorithmus aus den verbleibenden Daten und Paritätsfragmenten wiederhergestellt.



Die Volume-Wiederherstellung hängt von der Verfügbarkeit von Ressourcen ab, auf denen Objektkopien gespeichert werden. Der Fortschritt der Volume-Wiederherstellung erfolgt nicht linear und kann Tage oder Wochen in Anspruch nehmen.

Wiederherstellen eines fehlerhaften Volumes oder Node

Führen Sie die folgenden Schritte aus, um ein ausgefallenes Volume oder einen ausgefallenen Node wiederherzustellen.

Schritte

1. Gehen Sie im Grid Manager zu **MAINTENANCE > Volume Restoration**.
2. Wählen Sie die Registerkarte **zu wiederherstellende Knoten** aus.

Die Nummer auf der Registerkarte gibt die Anzahl der Nodes an, deren Volumes wiederhergestellt werden müssen.

Maintenance > Volume restoration

Volume restoration

If storage volumes in a Storage Node fail, you can perform volume restoration to restore object data to the recovered volumes. StorageGRID can restore replicated and erasure-coded objects using the copies or fragments that remain on other Storage Nodes, in a Cloud Storage Pool, or on an Archive Node.

Nodes to restore (2) Restoration progress Restoration history

Select a node to restore, including all available volumes in it. You can restore data for only one node at a time. Wait until the restoration on one node is complete before starting restoration on another node.

Nodes and volumes	Status
<input type="radio"/> ^ DC1-SN1-010-060-042-214 Volume 1	Waiting for manual steps ?
<input checked="" type="radio"/> ^ DC1-SN2-010-060-042-215 Volume 1	Ready to restore

[Start restore](#)

- Erweitern Sie jeden Node, um die Volumes anzuzeigen, die wiederhergestellt werden müssen, und ihren Status anzuzeigen.
- Beheben Sie alle Probleme, die die Wiederherstellung jedes Volumes verhindern, die angezeigt werden, wenn Sie Warten auf manuelle Schritte auswählen, wenn es als Volume-Status angezeigt wird.
- Wählen Sie einen Knoten aus, der wiederhergestellt werden soll, wobei alle Volumes den Status bereit zur Wiederherstellung anzeigen.

Sie können die Volumes nur für jeweils einen Node wiederherstellen.

Jedes Volume im Node muss angeben, dass es zur Wiederherstellung bereit ist.

- Wählen Sie **Wiederherstellung starten**.
- Beheben Sie alle Warnungen, die angezeigt werden können, oder wählen Sie **Trotzdem starten**, um die Warnungen zu ignorieren und die Wiederherstellung zu starten.

Knoten werden von der Registerkarte **Knoten zur Wiederherstellung** auf die Registerkarte **Wiederherstellungsfortschritt** verschoben, wenn die Wiederherstellung beginnt.

Wenn eine Volume-Wiederherstellung nicht gestartet werden kann, kehrt der Knoten zur Registerkarte **Nodes to restore** zurück.

Wiederherstellungsfortschritt anzeigen

Die Registerkarte **Restoration Progress** zeigt den Status des Wiederherstellungsprozesses des Volumes und Informationen über die Volumes für einen wiederherzustellenden Knoten an.

Volume restoration

If storage volumes in a Storage Node fail, you can perform volume restoration to restore object data to the recovered volumes. StorageGRID can restore replicated and erasure-coded objects using the copies or fragments that remain on other Storage Nodes, in a Cloud Storage Pool, or on an Archive Node.

Nodes to restore

Restoration progress

Restoration history

Replicated data repair rate:  10,001 objects/s

Erasure-coded data repair rate:  —

Objects safe from data loss (no restore required)  99%

Restoration jobs (1)

Node 	Volume ID 	Data type  	Status  	Progress 	Details
DC1-SN1-010-060-042-214	1	Replicated	Running	76%	

Datenreparaturraten für replizierte und Erasure-Coded-Objekte in allen Volumes sind Durchschnittswerte, die alle gerade verarbeiteten Wiederherstellungen einschließlich der mit dem initiierten Wiederherstellungen zusammenfassen `repair-data` Skript: Der Prozentsatz der Objekte in diesen Volumes, die intakt sind und keine Wiederherstellung erfordern, wird ebenfalls angegeben.



Die Wiederherstellung replizierter Daten hängt von der Verfügbarkeit der Ressourcen ab, auf denen die replizierten Kopien gespeichert sind. Der Fortschritt der replizierten Datenwiederherstellung erfolgt nicht linear und kann Tage oder Wochen dauern.

Im Abschnitt Wiederherstellungsaufträge werden Informationen über die mit Grid Manager begonnenen Volume-Wiederherstellungen angezeigt.

- Die Nummer im Abschnitt Wiederherstellungsaufträge gibt die Anzahl der Volumes an, die entweder wiederhergestellt oder zur Wiederherstellung in die Warteschlange gestellt werden.
- Die Tabelle zeigt Informationen zu jedem Volume in einem Node, der wiederhergestellt wird, und dessen Fortschritt an.
 - Der Fortschritt für jeden Node zeigt den Prozentsatz für jeden Job an.
 - Erweitern Sie die Spalte Details, um die Startzeit der Wiederherstellung und die Job-ID anzuzeigen.
- Wenn die Wiederherstellung eines Volumes fehlschlägt:
 - In der Spalte Status wird auf Fehlgeschlagen angezeigt.
 - Es wird ein Fehler angezeigt, der die Fehlerursache angibt.

Beheben Sie die im Fehler angezeigten Probleme. Wählen Sie dann **Wiederholen**, um die Wiederherstellung des Volumes erneut zu starten.

Wenn mehrere Wiederherstellungsaufträge fehlgeschlagen sind, wird durch Auswahl von **Wiederholen** der zuletzt fehlgeschlagene Job gestartet.

Wiederherstellungsverlauf anzeigen

Auf der Registerkarte **Restoration history** werden Informationen zu allen erfolgreich abgeschlossenen Volume-Wiederherstellungen angezeigt.



Die Größen gelten nicht für replizierte Objekte. Sie werden nur für Wiederherstellungen angezeigt, die EC-Datenobjekte (Erasure Coded) enthalten.

Maintenance > Volume restoration

Volume restoration

If storage volumes in a Storage Node fail, you can perform volume restoration to restore object data to the recovered volumes. StorageGRID can restore replicated and erasure-coded objects using the copies or fragments that remain on other Storage Nodes, in a Cloud Storage Pool, or on an Archive Node.

[Nodes to restore \(2\)](#) [Restoration progress](#) **Restoration history**

Search by node, volume, data type, or start time

Node	Volume ID	Size	Data type	Start time	Total time
DC1-SN1-010-060-042-214	1	-	Replicated	2022-11-09 09:07:24 EST	6 minutes
DC1-SN1-010-060-042-214	1	-	Replicated	2022-11-09 08:33:22 EST	11 minutes
DC1-SN1-010-060-042-214	1	-	Replicated	2022-11-09 08:22:03 EST	10 minutes
DC1-SN1-010-060-042-214	1	-	Replicated	2022-11-09 10:05:02 EST	8 minutes

Überwachen Sie Jobs mit Reparaturdaten

Sie können den Status von Reparaturjobs mit der überwachen `repair-data` Skript über die Befehlszeile.

Dazu gehören Jobs, die Sie manuell initiiert haben, oder Jobs, die StorageGRID automatisch im Rahmen einer Stilllegung initiiert hat.



Wenn Sie Volume-Wiederherstellungsjobs ausführen, "[Überwachen Sie den Fortschritt und zeigen Sie einen Verlauf dieser Jobs im Grid Manager an](#)" Stattdessen.

Überwachen Sie den Status von `repair-data` Jobs abhängig davon, ob Sie **replizierte Daten, Erasure-coded (EC)-Daten** oder beides verwenden.

Replizierte Daten

- Um einen geschätzten Fertigstellungsgrad für die replizierte Reparatur zu erhalten, fügen Sie die hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES > Storage Node wird repariert > ILM**.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle 0** Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid > Storage Node wird repariert > LDR > Data Store**.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra-Inkonsistenzen sind möglicherweise vorhanden, und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM)**: Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:
 - Wählen Sie **SUPPORT > Tools > Metrics**, um die geschätzte Zeit bis zum Abschluss und den Fertigstellungsgrad für den aktuellen Job anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
 - Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data`

Betriebliche Gründe:

```
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 enthält Informationen, einschließlich `repair ID`, für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

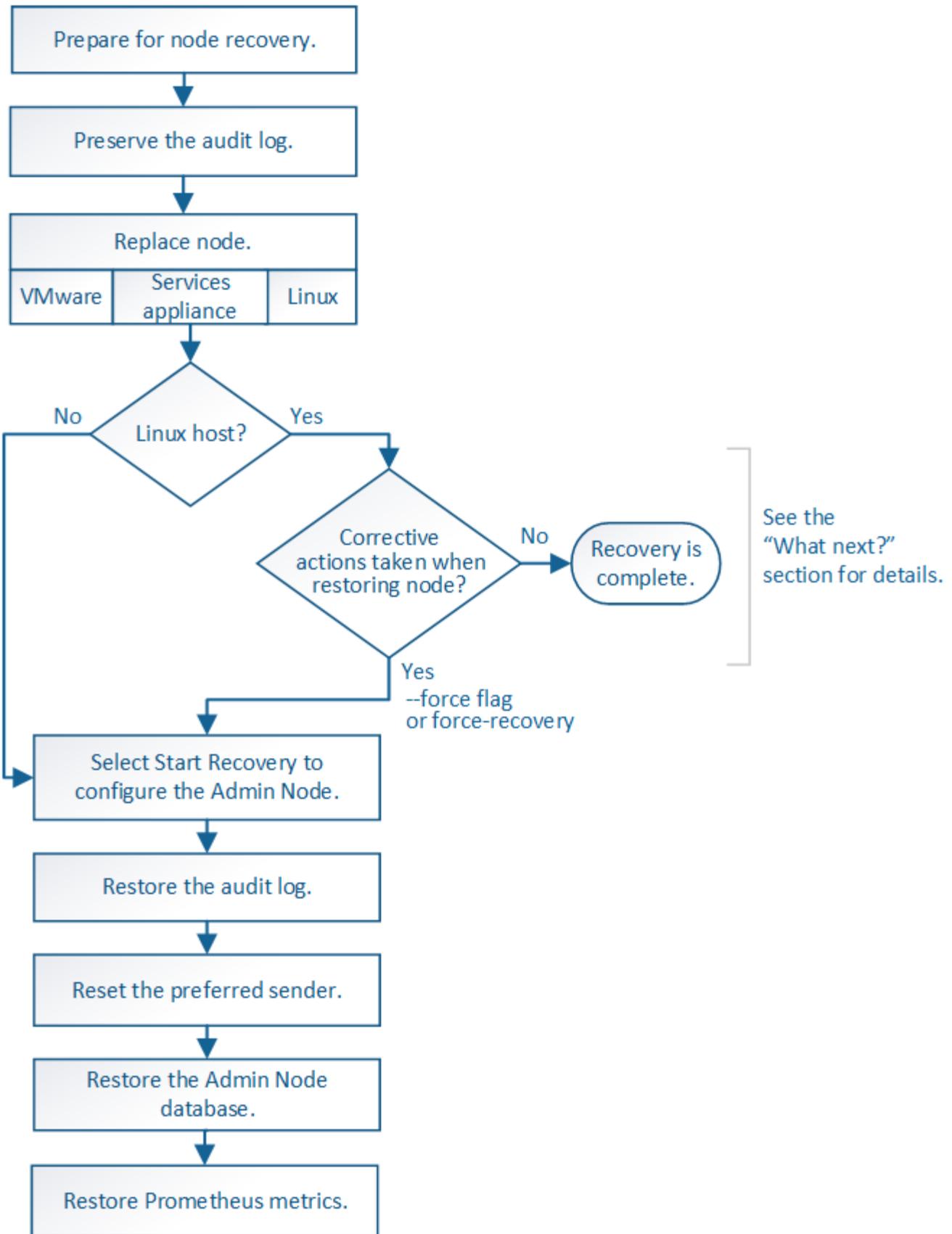
```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Wiederherstellung bei Ausfällen des Admin-Nodes

Wiederherstellung von Admin-Knoten-Ausfällen: Workflow

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 Schritte für die Wiederherstellung eines primären oder nicht primären Admin-Knotens auf hoher Ebene sind identisch, wobei sich die Details der einzelnen Schritte unterscheiden.



Befolgen Sie immer den richtigen Wiederherstellungsvorgang für den Admin-Knoten, den Sie wiederherstellen. Die Verfahren sehen auf hohem Niveau gleich aus, unterscheiden sich aber in den Details.

Wahlmöglichkeiten

- "Wiederherstellung nach Ausfällen des primären Admin-Nodes"
- "Wiederherstellung nach Ausfällen von Admin-Nodes außerhalb des primären Standorts"

Wiederherstellung nach Ausfällen des primären Admin-Nodes

Wiederherstellung nach Ausfällen des primären Admin-Knotens: Übersicht

Sie müssen einen bestimmten Satz von Aufgaben ausführen, um nach einem Ausfall eines primären Admin-Knotens wiederherstellen zu können. Der primäre Admin-Node hostet den Configuration Management Node (CMN)-Service für das Grid.

Ein fehlgeschlagener primärer Admin-Node sollte umgehend ersetzt werden. Der Configuration Management Node (CMN)-Dienst auf dem primären Admin-Node ist für die Ausgabe von Objektkennungen für das Grid verantwortlich. Diese Kennungen werden Objekten bei ihrer Aufnahme zugewiesen. Neue Objekte können nur aufgenommen werden, wenn Kennungen verfügbar sind. Die Objektaufnahme kann fortgesetzt werden, während das CMN nicht verfügbar ist, da die Identifikatoren ungefähr einen Monat im Grid zwischengespeichert werden. Nachdem jedoch die gecachten Kennungen erschöpft sind, können keine neuen Objekte hinzugefügt werden.



Sie müssen einen fehlerhaften primären Administrator-Node innerhalb von etwa einem Monat reparieren oder ersetzen. Andernfalls kann das Grid die Aufnahme neuer Objekte verlieren. Der genaue Zeitraum hängt von der Geschwindigkeit der Objekterfassung ab: Wenn Sie eine genauere Bewertung des Zeitrahmens für Ihr Grid benötigen, wenden Sie sich an den technischen Support.

Prüfprotokolle vom fehlgeschlagenen primären Admin-Node kopieren

Wenn Sie Audit-Protokolle vom fehlgeschlagenen primären Admin-Node kopieren können, sollten Sie diese beibehalten, um den Datensatz der Systemaktivität und -Nutzung des Rasters beizubehalten. Sie können die erhaltenen Audit-Protokolle nach dem wiederhergestellten primären Admin-Knoten wiederherstellen, nachdem er in Betrieb ist.

Über diese Aufgabe

Mit diesem Verfahren werden die Audit-Log-Dateien vom fehlgeschlagenen Admin-Node in einen temporären Speicherort auf einem separaten Grid-Node kopiert. Diese erhaltenen Audit-Protokolle können dann in den Ersatz-Admin-Node kopiert werden. Audit-Protokolle werden nicht automatisch auf den neuen Admin-Node kopiert.

Je nach Art des Fehlers können Sie unter Umständen keine Prüfprotokolle von einem fehlgeschlagenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Node verfügt, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen zum Audit-Protokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Node enthält, können Sie die Audit-Protokolle von einem anderen Admin-Node wiederherstellen.



Wenn die Überwachungsprotokolle jetzt nicht auf den fehlgeschlagenen Admin-Knoten zugreifen können, können Sie möglicherweise später darauf zugreifen, z. B. nach der Host-Wiederherstellung.

Schritte

1. Melden Sie sich nach Möglichkeit beim fehlgeschlagenen Admin-Knoten an. Melden Sie sich andernfalls beim primären Admin-Node oder einem anderen Admin-Node an, falls verfügbar.
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Protokolldatei erstellt wird:`service ams stop`
3. Benennen Sie die Datei `audit.log` um, damit sie die vorhandene Datei nicht überschreiben kann, wenn Sie sie in den wiederhergestellten Admin-Node kopieren.

Benennen Sie `audit.log` in einen eindeutigen nummerierten Dateinamen um. Benennen Sie beispielsweise die Datei `audit.log` in um `2023-10-25.txt.1`.

```
cd /var/local/audit/export
ls -l
mv audit.log 2023-10-25.txt.1
```

4. AMS-Dienst neu starten: `service ams start`
5. Erstellen Sie das Verzeichnis, um alle Audit-Log-Dateien in 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 Eingabeaufforderung das Passwort für den Administrator ein.

6. Alle Audit-Log-Dateien kopieren: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

7. Melden Sie sich als Root an: `exit`

Primären Admin-Node ersetzen

Um einen primären Admin-Node wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen fehlgeschlagenen primären Admin-Node durch einen primären Admin-Node ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen primären Admin-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen primären Admin-Node ersetzen, der auf einer Services-Appliance gehostet wird.

Verwenden Sie das Verfahren, das der für den Node ausgewählten Ersatzplattform entspricht. Nachdem Sie den Knotenaustausch abgeschlossen haben (der für alle Node-Typen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die primäre Admin-Knoten-Wiederherstellung geleitet.

Austauschplattform	Verfahren
VMware	"Einen VMware-Knoten ersetzen"
Linux	"Ersetzen Sie einen Linux-Knoten"
SG100- und SG1000-Services-Appliances	"Ersetzen Sie eine Service Appliance"
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren für "Ersetzen eines Linux-Knotens" .

Primären Ersatzadministrator-Knoten konfigurieren

Der Ersatzknoten muss als primärer Admin-Node für Ihr StorageGRID System konfiguriert sein.

Bevor Sie beginnen

- Für primäre Admin-Nodes, die auf virtuellen Maschinen gehostet werden, wurde die virtuelle Maschine bereitgestellt, eingeschaltet und initialisiert.
- Für primäre Admin-Nodes, die auf einer Services-Appliance gehostet werden, haben Sie die Appliance ersetzt und die installierte Software installiert. Siehe ["Installationsanweisungen für das Gerät"](#).
- Sie haben die letzte Sicherung der Recovery Package-Datei (`sgws-recovery-package-id-revision.zip`).
- Sie haben die Provisionierungs-Passphrase.

Schritte

1. Öffnen Sie Ihren Webbrowser, und navigieren Sie zu `https://primary_admin_node_ip`.

Install

Welcome

Use this page to install a new StorageGRID system, or recover a failed primary Admin Node for an existing system.

Note: You must have access to a StorageGRID license, network configuration and grid topology information, and NTP settings to complete the installation. You must have the latest version of the Recovery Package file to complete a primary Admin Node recovery.



Install a StorageGRID system



Recover a failed primary Admin Node

2. Klicken Sie auf **Wiederherstellen eines fehlgeschlagenen primären Admin-Knotens**.
3. Laden Sie das aktuellste Backup des Wiederherstellungspakets hoch:
 - a. Klicken Sie Auf **Durchsuchen**.
 - b. Suchen Sie die aktuellste Wiederherstellungspakedatei für Ihr StorageGRID-System und klicken Sie auf **Öffnen**.
4. Geben Sie die Provisionierungs-Passphrase ein.
5. Klicken Sie Auf **Wiederherstellung Starten**.

Der Wiederherstellungsprozess beginnt. Der Grid Manager ist möglicherweise einige Minuten lang nicht mehr verfügbar, wenn die erforderlichen Dienste gestartet werden. Wenn die Wiederherstellung abgeschlossen ist, wird die Anmeldeseite angezeigt.

6. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist und das Vertrauen der Vertrauensstelle für den wiederhergestellten Admin-Knoten für das Zertifikat der Standardverwaltungsoberfläche konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Node auf die Vertrauensbasis in Active Directory Federation Services (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.



Informationen zum Konfigurieren einer vertrauenswürdigen Partei finden Sie unter ["Konfigurieren Sie Single Sign-On"](#). Melden Sie sich zum Zugriff auf das Standard-Serverzertifikat bei der Eingabeaufforderung des Admin-Knotens an. Wechseln Sie zum `/var/local/mgmt-api` Und wählen Sie das aus `server.crt` Datei:

7. Bestimmen Sie, ob Sie einen Hotfix anwenden müssen.
 - a. Melden Sie sich mit einem bei Grid Manager an ["Unterstützter Webbrowser"](#).

- b. Wählen Sie **KNOTEN**.
- c. Wählen Sie in der Liste links den primären Admin-Node aus.
- d. Notieren Sie sich auf der Registerkarte Übersicht die Version, die im Feld **Softwareversion** angezeigt wird.
- e. Wählen Sie einen beliebigen anderen Grid-Knoten aus.
- f. Notieren Sie sich auf der Registerkarte Übersicht die Version, die im Feld **Softwareversion** angezeigt wird.
 - Wenn die in den Feldern **Software Version** angezeigten Versionen identisch sind, müssen Sie keinen Hotfix anwenden.
 - Wenn die in den Feldern **Software Version** angezeigten Versionen unterschiedlich sind, müssen Sie dies tun "[Installieren Sie einen Hotfix](#)" Um den wiederhergestellten primären Admin-Knoten auf dieselbe Version zu aktualisieren.

Prüfprotokoll auf wiederhergestellten primären Admin-Knoten wiederherstellen

Wenn Sie das Revisionsprotokoll vom fehlgeschlagenen primären Admin-Knoten erhalten konnten, können Sie es in den primären Admin-Knoten kopieren, den Sie wiederherstellen.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten wird installiert und ausgeführt.
- Sie haben die Überwachungsprotokolle an einen anderen Speicherort kopiert, nachdem der ursprüngliche Admin-Node fehlgeschlagen ist.

Über diese Aufgabe

Wenn ein Admin-Knoten ausfällt, gehen in diesem Admin-Knoten gespeicherte Prüfprotokolle möglicherweise verloren. Es könnte möglich sein, Daten vor Verlust durch Kopieren von Prüfprotokollen aus dem fehlgeschlagenen Admin-Knoten und dann die Wiederherstellung dieser Prüfprotokolle auf den wiederhergestellten Admin-Knoten. Je nach Ausfall ist es möglicherweise nicht möglich, Prüfprotokolle vom fehlgeschlagenen Admin-Node zu kopieren. Wenn die Bereitstellung mehr als einen Admin-Node hat, können Sie in diesem Fall Audit-Protokolle von einem anderen Admin-Node wiederherstellen, da Audit-Protokolle auf allen Admin-Nodes repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Audit-Protokoll nicht vom fehlgeschlagenen Knoten kopiert werden kann, beginnt der wiederhergestellte Admin-Knoten, Ereignisse im Auditprotokoll zu erfassen, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.



Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn eine der folgenden Maßnahmen zutrifft:

- Sie haben einen externen Syslog-Server konfiguriert und Audit-Protokolle werden jetzt an den Syslog-Server anstatt an Admin-Knoten gesendet.
- Sie haben ausdrücklich angegeben, dass Audit-Meldungen nur auf den lokalen Knoten gespeichert werden sollten, die sie generiert haben.

Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)" Entsprechende 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Nachdem Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

2. Prüfen Sie, welche Audit-Dateien erhalten wurden: `cd /var/local/audit/export`

3. Kopieren Sie die erhaltenen Audit-Log-Dateien auf den wiederhergestellten Admin-Knoten: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom fehlgeschlagenen Grid-Knoten, nachdem Sie überprüft haben, ob sie erfolgreich auf den wiederhergestellten Admin-Node kopiert wurden.

5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Log-Dateien auf dem wiederhergestellten Admin-Knoten: `chown ams-user: bycast *`

6. Melden Sie sich als Root an: `exit`

Sie müssen auch alle bereits vorhandenen Clientzugriffe auf die Revisionsfreigabe wiederherstellen. Weitere Informationen finden Sie unter "[Konfigurieren des Zugriffs auf Audit-Clients](#)".

Stellen Sie die Admin-Knoten-Datenbank wieder her, wenn Sie den primären Admin-Knoten wiederherstellen

Wenn Sie die historischen Informationen über Attribute, Alarme und Alarme auf einem primären Admin-Node, der ausgefallen ist, behalten möchten, können Sie die Admin-Node-Datenbank wiederherstellen. Sie können diese Datenbank nur wiederherstellen, wenn Ihr StorageGRID-System einen anderen Admin-Knoten enthält.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten wird installiert und ausgeführt.
- Das StorageGRID-System enthält mindestens zwei Admin-Nodes.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen Informationen verloren. Diese Datenbank enthält folgende Informationen:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **SUPPORT > Tools > Grid Topology** verfügbar sind.

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen für Server und Services, die derzeit Teil des Systems sind oder später hinzugefügt werden.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID-System einen anderen Admin-Knoten hat, können Sie die historischen Informationen wiederherstellen, indem Sie die Admin-Knoten-Datenbank von einem nicht-primären Admin-Knoten (der_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-Node-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

Schritte

1. Melden Sie sich beim Quell-Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Beenden Sie den MI-Dienst vom Quell-Admin-Node: `service mi stop`
3. Beenden Sie vom Quell-Admin-Node den Management Application Program Interface (Management-API)-Service: `service mgmt-api stop`
4. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - b. Beenden SIE DEN MI-Dienst: `service mi stop`
 - c. Beenden Sie den Management API-Service: `service mgmt-api stop`
 - d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
 - e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `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. Wenn Sie dazu aufgefordert werden, bestätigen Sie, 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 vom SSH-Agent. Geben Sie Ein: `ssh-add -D`

5. Starten Sie die Dienste auf dem Quell-Admin-Node neu: `service servermanager start`

Stellen Sie bei der Wiederherstellung des primären Admin-Knotens Prometheus-Kennzahlen wieder her

Optional können Sie die historischen Metriken aufbewahren, die von Prometheus auf einem primären Admin-Node gewartet wurden, der ausgefallen ist. Die Prometheus Kennzahlen können nur wiederhergestellt werden, wenn Ihr StorageGRID System einen anderen Admin-Knoten enthält.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten wird installiert und ausgeführt.
- Das StorageGRID-System enthält mindestens zwei Admin-Nodes.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten gepflegten Kennzahlen verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Node gestartet wurde, zeichnet er die Metriken auf, als ob Sie eine neue Installation des StorageGRID-Systems durchgeführt hatten.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID-System einen anderen Admin-Knoten hat, können Sie die historischen Metriken wiederherstellen, indem Sie die Prometheus-Datenbank von einem nicht-primären Admin-Knoten (den *Source 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 dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

Schritte

1. Melden Sie sich beim Quell-Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- b. Stoppen Sie den Prometheus Service: `service prometheus stop`
- c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`
- d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `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. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, 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. Der folgende Status wird angezeigt:

Datenbank geklont, Dienste starten

- a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:`ssh-add -D`
4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node `neu.service prometheus start`

Wiederherstellung nach Ausfällen von Admin-Nodes außerhalb des primären Standorts

Wiederherstellung nach Ausfällen von nicht-primären Admin-Knoten: Übersicht

Sie müssen die folgenden Aufgaben durchführen, um nach einem Ausfall eines nicht primären Admin-Knotens wiederherzustellen. Ein Admin-Node hostet den Configuration Management Node (CMN)-Service und ist als primärer Admin-Node bekannt. Obwohl Sie mehrere Admin-Nodes haben können, enthält jedes StorageGRID-System nur einen primären Admin-Node. Alle anderen Admin-Nodes sind nicht primäre Admin-Nodes.

Prüfprotokolle vom fehlgeschlagenen Admin-Knoten kopieren

Wenn Sie in der Lage sind, Audit-Protokolle vom fehlgeschlagenen Admin-Node zu kopieren, sollten Sie diese beibehalten, um die Aufzeichnung der Systemaktivität und -Nutzung des Rasters beizubehalten. Sie können die erhaltenen Audit-Protokolle nach dem Wiederherstellen des nicht-primären Admin-Knotens wiederherstellen, nachdem er ausgeführt wurde.

Mit diesem Verfahren werden die Audit-Log-Dateien vom fehlgeschlagenen Admin-Node in einen temporären Speicherort auf einem separaten Grid-Node kopiert. Diese erhaltenen Audit-Protokolle können dann in den Ersatz-Admin-Node kopiert werden. Audit-Protokolle werden nicht automatisch auf den neuen Admin-Node kopiert.

Je nach Art des Fehlers können Sie unter Umständen keine Prüfprotokolle von einem fehlgeschlagenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Node verfügt, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen zum Audit-Protokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Node enthält, können Sie die Audit-Protokolle von einem anderen Admin-Node wiederherstellen.



Wenn die Überwachungsprotokolle jetzt nicht auf den fehlgeschlagenen Admin-Knoten zugreifen können, können Sie möglicherweise später darauf zugreifen, z. B. nach der Host-Wiederherstellung.

1. Melden Sie sich nach Möglichkeit beim fehlgeschlagenen Admin-Knoten an. Melden Sie sich andernfalls beim primären Admin-Node oder einem anderen Admin-Node an, falls verfügbar.

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Protokolldatei erstellt wird:`service ams stop`

3. Benennen Sie die Datei `audit.log` um, damit sie die vorhandene Datei nicht überschreiben kann, wenn Sie sie in den wiederhergestellten Admin-Node kopieren.

Benennen Sie `audit.log` in einen eindeutigen nummerierten Dateinamen um. Benennen Sie beispielsweise die Datei `audit.log` in um `2023-10-25.txt.1`.

```
cd /var/local/audit/export
ls -l
mv audit.log 2023-10-25.txt.1
```

4. AMS-Dienst neu starten: `service ams start`

5. Erstellen Sie das Verzeichnis, um alle Audit-Log-Dateien in 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 Eingabeaufforderung das Passwort für den Administrator ein.

6. Alle Audit-Log-Dateien kopieren: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

7. Melden Sie sich als Root an: `exit`

Nicht-primärer Admin-Node ersetzen

Um einen nicht-primären Admin-Node wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen nicht primären Admin-Node durch einen nicht-primären Admin-Node ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen nicht-primären Admin-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen nicht-primären Admin-Node ersetzen, der auf einer Services

Appliance gehostet wird.

Verwenden Sie das Verfahren, das der für den Node ausgewählten Ersatzplattform entspricht. Nachdem Sie den Knotenaustausch abgeschlossen haben (der für alle Node-Typen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die Wiederherstellung eines nicht-primären Admin-Knotens geleitet.

Austauschplattform	Verfahren
VMware	"Einen VMware-Knoten ersetzen"
Linux	"Ersetzen Sie einen Linux-Knoten"
SG100- und SG1000-Services-Appliances	"Ersetzen Sie eine Service Appliance"
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren für "Ersetzen eines Linux-Knotens" .

Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren

Nach dem Ersetzen eines nicht-primären Admin-Knotens müssen Sie im Grid-Manager die Option Wiederherstellung starten wählen, um den neuen Knoten als Ersatz für den fehlgeschlagenen Knoten zu konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben die Provisionierungs-Passphrase.
- Sie haben den Ersatzknoten bereitgestellt und konfiguriert.

Schritte

1. Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden in der Liste angezeigt, wenn sie fehlschlagen. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und für die Wiederherstellung bereit ist.
3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknotten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das anzeigt, dass der Knoten in einem unbestimmten Zustand bleibt, wenn Sie das Verfahren zurücksetzen.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **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 Vorgangs erneut versuchen möchten, müssen Sie den Geräteknoten durch Ausführen in einen vorinstallierten Zustand wiederherstellen `sgareinstall` Auf dem Node. Siehe "[Appliance für die Neuinstallation vorbereiten](#)"

(nur Plattformaustausch)".

6. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist und das Vertrauen der Vertrauensstelle für den wiederhergestellten Admin-Knoten für das Zertifikat der Standardverwaltungsoberfläche konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Node auf die Vertrauensbasis in Active Directory Federation Services (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.



Informationen zum Konfigurieren einer vertrauenswürdigen Partei finden Sie unter ["Konfigurieren Sie Single Sign-On"](#). Melden Sie sich zum Zugriff auf das Standard-Serverzertifikat bei der Eingabeaufforderung des Admin-Knotens an. Wechseln Sie zum `/var/local/mgmt-api` Und wählen Sie das aus `server.crt` Datei:

Stellen Sie das Prüfprotokoll auf dem wiederhergestellten Admin-Node, der nicht dem primären Administrator gehört, wieder her

Wenn Sie das Audit-Protokoll vom fehlgeschlagenen nicht-primären Admin-Node erhalten konnten, damit die Informationen des historischen Audit-Protokolls beibehalten werden, können Sie es in den nicht-primären Admin-Node kopieren, den Sie wiederherstellen.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten wird installiert und ausgeführt.
- Sie haben die Überwachungsprotokolle an einen anderen Speicherort kopiert, nachdem der ursprüngliche Admin-Node fehlgeschlagen ist.

Über diese Aufgabe

Wenn ein Admin-Knoten ausfällt, gehen in diesem Admin-Knoten gespeicherte Prüfprotokolle möglicherweise verloren. Es könnte möglich sein, Daten vor Verlust durch Kopieren von Prüfprotokollen aus dem fehlgeschlagenen Admin-Knoten und dann die Wiederherstellung dieser Prüfprotokolle auf den wiederhergestellten Admin-Knoten. Je nach Ausfall ist es möglicherweise nicht möglich, Prüfprotokolle vom fehlgeschlagenen Admin-Node zu kopieren. Wenn die Bereitstellung mehr als einen Admin-Node hat, können Sie in diesem Fall Audit-Protokolle von einem anderen Admin-Node wiederherstellen, da Audit-Protokolle auf allen Admin-Nodes repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Audit-Protokoll nicht vom fehlgeschlagenen Knoten kopiert werden kann, beginnt der wiederhergestellte Admin-Knoten, Ereignisse im Auditprotokoll zu erfassen, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.

Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn eine der folgenden Maßnahmen zutrifft:



- Sie haben einen externen Syslog-Server konfiguriert und Audit-Protokolle werden jetzt an den Syslog-Server anstatt an Admin-Knoten gesendet.
- Sie haben ausdrücklich angegeben, dass Audit-Meldungen nur auf den lokalen Knoten gespeichert werden sollten, die sie generiert haben.

Siehe ["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#) Entsprechende 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 im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Nachdem Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Prüfen Sie, welche Audit-Dateien erhalten wurden:

```
cd /var/local/audit/export
```

3. Kopieren Sie die erhaltenen Audit-Log-Dateien auf den wiederhergestellten Admin-Knoten:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom fehlgeschlagenen Grid-Knoten, nachdem Sie überprüft haben, ob sie erfolgreich auf den wiederhergestellten Admin-Node kopiert wurden.

5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Log-Dateien auf dem wiederhergestellten Admin-Knoten:

```
chown ams-user:bycast *
```

6. Melden Sie sich als Root an: `exit`

Sie müssen auch alle bereits vorhandenen Clientzugriffe auf die Revisionsfreigabe wiederherstellen. Weitere Informationen finden Sie unter "[Konfigurieren des Zugriffs auf Audit-Clients](#)".

Stellen Sie die Admin-Node-Datenbank wieder her, wenn Sie einen nicht-primären Admin-Node wiederherstellen

Wenn Sie die historischen Informationen zu Attributen, Alarmen und Warnmeldungen bei einem nicht primären Admin-Node behalten möchten, der ausgefallen ist, können Sie die Admin-Knoten-Datenbank vom primären Admin-Node wiederherstellen.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten wird installiert und ausgeführt.
- Das StorageGRID-System enthält mindestens zwei Admin-Nodes.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen Informationen verloren. Diese Datenbank enthält folgende Informationen:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **SUPPORT > Tools > Grid Topology** verfügbar sind.

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen für Server und Services, 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-Node-Datenbank vom primären Admin-Knoten (den_Quell-Admin-Node_) auf den wiederhergestellten Knoten kopieren.



Das Kopieren der Admin-Node-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quellknoten angehalten werden.

Schritte

1. Melden Sie sich beim Quell-Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Führen Sie den folgenden Befehl vom Quell-Admin-Knoten aus. Geben Sie dann die Provisionierungs-Passphrase ein, wenn Sie dazu aufgefordert werden. `recover-access-points`
3. Beenden Sie den MI-Dienst vom Quell-Admin-Node: `service mi stop`
4. Beenden Sie vom Quell-Admin-Node den Management Application Program Interface (Management-API)-Service: `service mgmt-api stop`
5. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - b. Beenden SIE DEN MI-Dienst: `service mi stop`
 - c. Beenden Sie den Management API-Service: `service mgmt-api stop`
 - d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
 - e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `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. Wenn Sie dazu aufgefordert werden, bestätigen Sie, 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 vom SSH-Agent. Geben Sie `ssh-add -D`

6. Starten Sie die Dienste auf dem Quell-Admin-Node neu: `service servermanager start`

Stellen Sie Prometheus-Kennzahlen wieder her, wenn Sie einen nicht-primären Admin-Node wiederherstellen

Optional können Sie die historischen Metriken aufbewahren, die von Prometheus auf einem nicht primären Admin-Node gewartet wurden, der ausgefallen ist.

Bevor Sie beginnen

- Der wiederhergestellte Admin-Knoten wird installiert und ausgeführt.
- Das StorageGRID-System enthält mindestens zwei Admin-Nodes.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten gepflegten Kennzahlen verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Node gestartet wurde, zeichnet er die Metriken auf, als ob Sie eine neue Installation des StorageGRID-Systems durchgeführt hatten.

Wenn Sie einen nicht-primären Admin-Knoten wiederhergestellt haben, können Sie die historischen Metriken wiederherstellen, indem Sie die Prometheus-Datenbank vom primären Admin-Knoten (den `_Source Admin-Node_`) auf den wiederhergestellten Admin-Knoten kopieren.



Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

Schritte

1. Melden Sie sich beim Quell-Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten 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 im aufgeführte Passwort ein `Passwords.txt` Datei:

- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- b. Stoppen Sie den Prometheus Service: `service prometheus stop`
- c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`
- d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `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. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, 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. Der folgende Status wird angezeigt:

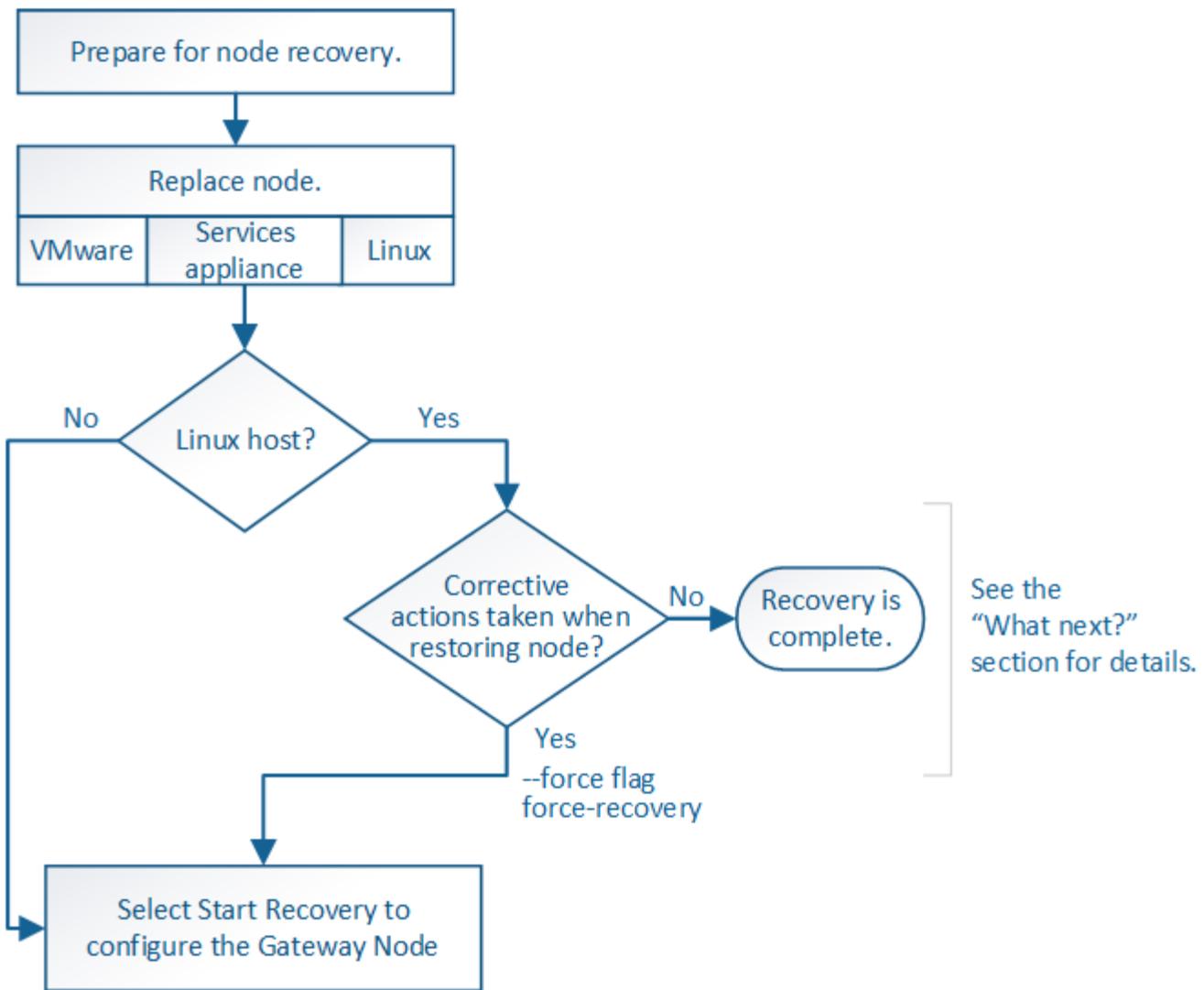
Datenbank geklont, Dienste starten

- a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:`ssh-add -D`
4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node `neu.service prometheus start`

Wiederherstellung nach Gateway-Node-Ausfällen

Wiederherstellung nach Gateway-Node-Ausfällen: Workflow

Sie müssen eine Reihe von Aufgaben genau durchführen, um nach einem Gateway Node-Ausfall wiederherstellen zu können.



Gateway-Node Ersetzen

Sie können einen fehlgeschlagenen Gateway-Node durch einen Gateway-Node ersetzen, der auf derselben physischen oder virtuellen Hardware ausgeführt wird, oder Sie können einen Gateway-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen Gateway-Node ersetzen, der auf einer Services-Appliance gehostet wird.

Das Verfahren zum Austausch des Nodes, das Sie befolgen müssen, hängt davon ab, welche Plattform vom Austausch-Node verwendet wird. Nach Abschluss des Austauschverfahrens für den Node (geeignet für alle Node-Typen) werden Sie durch dieses Verfahren zum nächsten Schritt für die Gateway Node Recovery geleitet.

Austauschplattform	Verfahren
VMware	"Einen VMware-Knoten ersetzen"
Linux	"Ersetzen Sie einen Linux-Knoten"

Austauschplattform	Verfahren
SG100- und SG1000-Services-Appliances	"Ersetzen Sie eine Service Appliance"
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren für "Ersetzen eines Linux-Knotens" .

Wählen Sie **Wiederherstellung starten**, um **Gateway-Node** zu konfigurieren

Nachdem Sie einen Gateway-Node ersetzt haben, müssen Sie im Grid Manager **Recovery** starten auswählen, um den neuen Node als Ersatz für den ausgefallenen Node zu konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Berechtigung **Wartung** oder **Stammzugriff**.
- Sie haben die **Provisionierungs-Passphrase**.
- Sie haben den Ersatzknoten bereitgestellt und konfiguriert.

Schritte

1. Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Recovery**.
2. Wählen Sie in der Liste **Ausstehende Knoten** den **Rasterknoten** aus, den Sie wiederherstellen möchten.

Nodes werden in der Liste angezeigt, wenn sie fehlschlagen. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und für die Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknotten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das anzeigt, dass der Knoten in einem unbestimmten Zustand bleibt, wenn Sie das Verfahren zurücksetzen.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

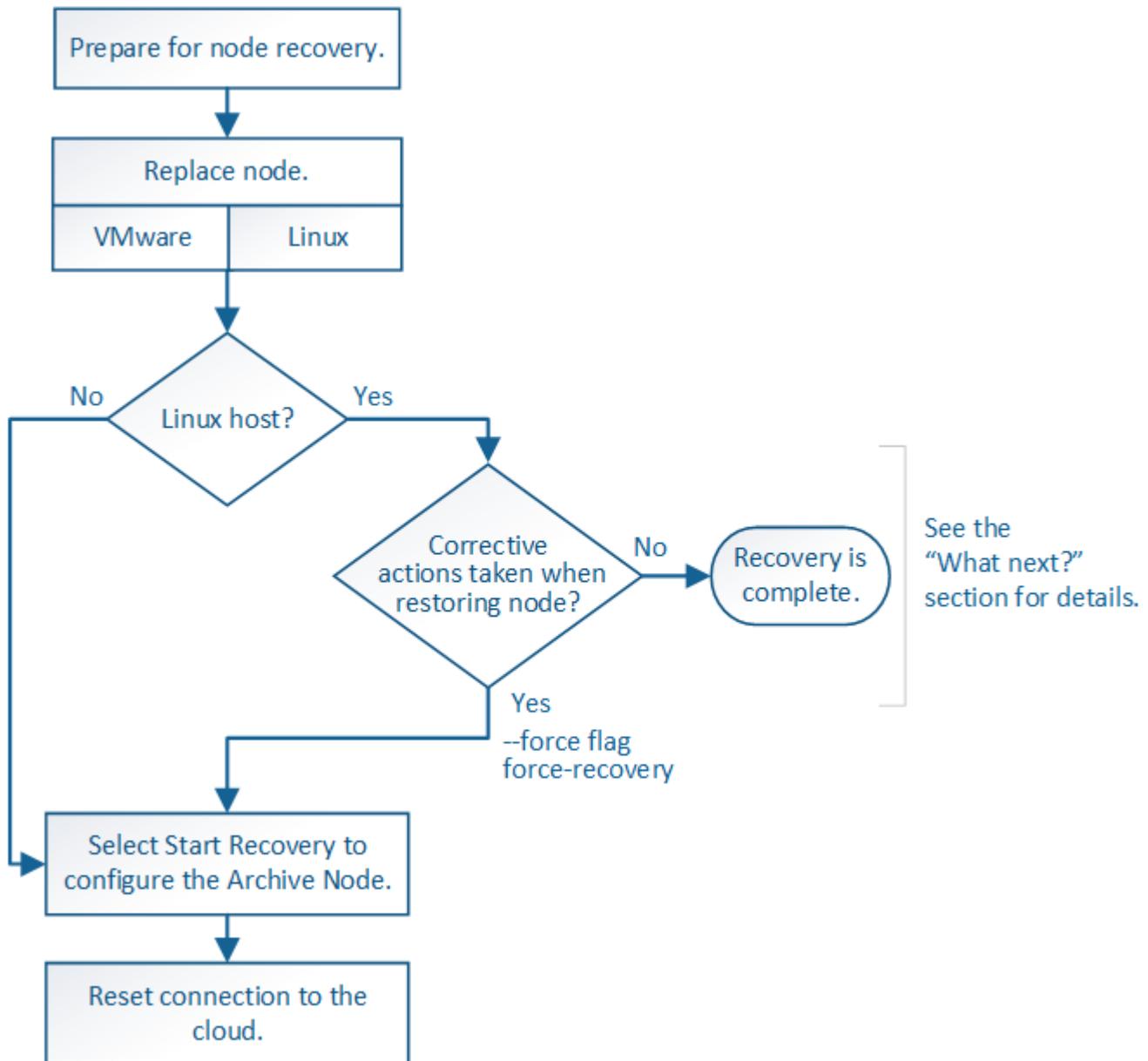
- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux:** Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen:
`storagegrid node force-recovery node-name`
- **Appliance:** Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Vorgangs erneut versuchen möchten, müssen Sie den Geräteknoten durch Ausführen in einen vorinstallierten Zustand wiederherstellen `sgareinstall` Auf dem Node. Siehe "[Appliance für die Neuinstallation vorbereiten](#)"

(nur Plattformaustausch)".

Wiederherstellung nach Ausfällen des Archivierungs-Nodes

Wiederherstellung nach Ausfällen von Archive Node: Workflow

Sie müssen eine Reihe von Aufgaben genau durchführen, um nach einem Ausfall des Archivierungs-Knotens wiederherstellen zu können.



Die Wiederherstellung von Archivknoten ist von den folgenden Problemen betroffen:

- Wenn die ILM-Richtlinie für die Replizierung einer einzelnen Kopie konfiguriert ist

In einem StorageGRID-System, das für eine einzelne Objektkopie konfiguriert ist, kann ein Ausfall des Archiv-Nodes zu einem nicht wiederherstellbaren Verlust von Daten führen. Wenn ein Fehler auftritt, gehen alle diese Objekte verloren. Sie müssen jedoch weiterhin Wiederherstellungsverfahren durchführen, um Ihr StorageGRID-System zu „bereinigen“ und verlorene Objektinformationen aus der Datenbank zu löschen.

- Wenn während der Wiederherstellung des Speicherknosens ein Ausfall des Archivknosens auftritt.

Wenn der Archivknoten bei der Verarbeitung der Massenabrufe im Rahmen einer Speicherknotenwiederherstellung ausfällt, Sie müssen das Verfahren wiederholen, um Kopien von Objektdaten auf den Storage-Node von Anfang an wiederherzustellen, um sicherzustellen, dass alle vom Archiv-Node abgerufenen Objektdaten auf dem Storage-Node wiederhergestellt werden.

Archivknoten Ersetzen

Um einen Archiv-Knoten wiederherzustellen, müssen Sie zuerst den Knoten ersetzen.

Sie müssen das Verfahren zum Ersetzen des Node für Ihre Plattform auswählen. Die Schritte zum Ersetzen eines Node sind für alle Typen von Grid-Nodes identisch.

Plattform	Verfahren
VMware	"Einen VMware-Knoten ersetzen"
Linux	"Ersetzen Sie einen Linux-Knoten"
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren für "Ersetzen eines Linux-Knotens" .

Wählen Sie Wiederherstellung starten, um den Knoten Archiv zu konfigurieren

Nachdem Sie einen Archivknoten ersetzt haben, müssen Sie im Grid Manager die Option Wiederherstellung starten auswählen, um den neuen Knoten als Ersatz für den fehlgeschlagenen Knoten zu konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben die Provisionierungs-Passphrase.
- Sie haben den Ersatzknoten bereitgestellt und konfiguriert.

Schritte

1. Wählen Sie im Grid Manager **MAINTENANCE > Tasks > Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden in der Liste angezeigt, wenn sie fehlschlagen. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und für die Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknotten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Es wird ein Dialogfeld angezeigt, das anzeigt, dass der Knoten in einem unbestimmten Zustand bleibt, wenn Sie das Verfahren zurücksetzen.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux:** Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen:
`storagegrid node force-recovery node-name`

Die Verbindung mit dem Archivierungs-Node zur Cloud wird zurückgesetzt

Nachdem Sie einen Archiv-Node wiederhergestellt haben, der die Cloud über die S3-API

anzieht, müssen Sie die Konfigurationseinstellungen ändern, um Verbindungen zurückzusetzen. Ein ORSU-Alarm (Outbound Replication Status) wird ausgelöst, wenn der Archivknoten keine Objektdaten abrufen kann.



Wenn Ihr Archive Node über TSM Middleware eine Verbindung zu externem Speicher herstellt, wird der Node automatisch zurückgesetzt, und Sie müssen ihn nicht neu konfigurieren.

Bevor Sie beginnen

Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Ziel**.
3. Bearbeiten Sie das Feld **Zugriffsschlüssel**, indem Sie einen falschen Wert eingeben und auf **Änderungen anwenden** klicken.
4. Bearbeiten Sie das Feld **Zugriffsschlüssel**, indem Sie den richtigen Wert eingeben und auf **Änderungen anwenden** klicken.

Alle Grid-Node-Typen: VMware Node ersetzen

Wenn Sie einen ausgefallenen StorageGRID-Knoten wiederherstellen, der auf VMware gehostet wurde, entfernen Sie den ausgefallenen Knoten und stellen einen Recovery-Knoten bereit.

Bevor Sie beginnen

Sie haben festgestellt, dass die virtuelle Maschine nicht wiederhergestellt werden kann und ersetzt werden muss.

Über diese Aufgabe

Sie verwenden den VMware vSphere Web Client, um zuerst die dem ausgefallenen Grid-Node zugeordnete virtuelle Maschine zu entfernen. Anschließend können Sie eine neue Virtual Machine implementieren.

Dieses Verfahren ist nur ein Schritt im Recovery-Prozess des Grid Node. Das Verfahren zum Entfernen und Implementieren eines Node ist für alle VMware Nodes identisch, einschließlich Admin-Nodes, Storage-Nodes, Gateway-Nodes und Archiv-Nodes.

Schritte

1. Melden Sie sich beim VMware vSphere Web Client an.
2. Navigieren Sie zu der ausgefallenen virtuellen Maschine des Grid-Node.
3. Notieren Sie sich alle Informationen, die zur Implementierung des Recovery-Nodes erforderlich sind.
 - a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie die Registerkarte **Einstellungen bearbeiten** aus, und notieren Sie die verwendeten Einstellungen.
 - b. Wählen Sie die Registerkarte **vApp Options** aus, um die Netzwerkeinstellungen des Grid Node anzuzeigen und aufzuzeichnen.
4. Wenn der fehlgeschlagene Grid-Node ein Storage-Node ist, ermitteln Sie, ob eine der virtuellen Festplatten, die für die Datenspeicherung verwendet werden, unbeschädigt sind, und bewahren Sie sie für die erneute Verbindung mit dem wiederhergestellten Grid-Node auf.

5. Schalten Sie die virtuelle Maschine aus.
6. Wählen Sie **actions > All vCenter actions > Delete from Disk**, um die virtuelle Maschine zu löschen.
7. Implementieren Sie eine neue Virtual Machine als Ersatz-Node und verbinden Sie sie mit einem oder mehreren StorageGRID Netzwerken. Anweisungen finden Sie unter "[StorageGRID-Knoten als virtuelle Maschine implementieren](#)".

Bei der Implementierung des Node können Sie optional Node-Ports neu zuordnen oder CPU- oder Speichereinstellungen erhöhen.



Nach der Bereitstellung des neuen Knotens können Sie entsprechend Ihren Speicheranforderungen neue virtuelle Festplatten hinzufügen, alle virtuellen Festplatten, die vom zuvor entfernten ausgefallenen Grid-Knoten oder beiden beibehalten werden, neu anbinden.

8. Führen Sie das Recovery-Verfahren für den Node anhand des Node aus, den Sie wiederherstellen.

Node-Typ	Gehen Sie zu
Primärer Admin-Node	"Primären Ersatzadministrator-Knoten konfigurieren"
Nicht primärer Admin-Node	"Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren"
Gateway-Node	"Wählen Sie Wiederherstellung starten, um Gateway-Node zu konfigurieren"
Storage-Node	"Wählen Sie Wiederherstellung starten, um Speicherknoten zu konfigurieren"
Archiv-Node	"Wählen Sie Wiederherstellung starten, um den Knoten Archiv zu konfigurieren"

Alle Grid-Node-Typen: Ersetzen Sie den Linux-Node

Alle Grid-Node-Typen: Ersetzen Sie den Linux-Node

Wenn ein Fehler erfordert, dass Sie einen oder mehrere neue physische oder virtuelle Hosts bereitstellen oder Linux auf einem vorhandenen Host neu installieren, stellen Sie den Ersatz-Host bereit und konfigurieren Sie ihn, bevor Sie den Grid-Node wiederherstellen können. Dieses Verfahren ist ein Schritt der Wiederherstellung des Grid-Nodes für alle Arten von Grid-Nodes.

„Linux“ bezieht sich auf eine Red hat® Enterprise Linux®, Ubuntu®, CentOS- oder Debian®-Bereitstellung. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um eine Liste der unterstützten Versionen zu erhalten.

Dieses Verfahren wird nur als ein Schritt bei der Wiederherstellung von softwarebasierten Speicherknoten, primären oder nicht primären Admin-Nodes, Gateway-Nodes oder Archiv-Nodes durchgeführt. Die Schritte sind unabhängig vom Typ des wiederhererenden Grid-Node identisch.

Wenn mehr als ein Grid-Node auf einem physischen oder virtuellen Linux-Host gehostet wird, können Sie die Grid-Nodes in beliebiger Reihenfolge wiederherstellen. Die Wiederherstellung eines primären Admin-Knotens zuerst verhindert jedoch, falls vorhanden, dass die Wiederherstellung anderer Grid-Knoten abstuckt, während sie versuchen, den primären Admin-Knoten zu kontaktieren, um sich für die Wiederherstellung zu registrieren.

Implementieren Sie neue Linux-Hosts

Bis auf ein paar Ausnahmen bereiten Sie die neuen Hosts wie während der Erstinstallation vor.

Um neue oder neu installierte physische oder virtuelle Linux-Hosts bereitzustellen, gehen Sie wie folgt vor, um die Hosts in den StorageGRID-Installationsanweisungen für Ihr Linux-Betriebssystem vorzubereiten:

- ["Installation von Linux \(Red hat Enterprise Linux oder CentOS\)"](#)
- ["Linux installieren \(Ubuntu oder Debian\)"](#)

Dieses Verfahren umfasst Schritte zur Durchführung folgender Aufgaben:

1. Installieren Sie Linux.
2. Konfigurieren Sie das Hostnetzwerk.
3. Hostspeicher konfigurieren.
4. Die Container-Engine einbauen.
5. Installieren Sie den StorageGRID Host Service.



Beenden Sie den Vorgang „StorageGRID Host Service installieren“ in den Installationsanweisungen. Starten Sie nicht den Task „Deployment Grid Nodes“.

Beachten Sie bei der Durchführung dieser Schritte die folgenden wichtigen Richtlinien:

- Verwenden Sie die gleichen Hostnamen, die Sie auf dem ursprünglichen Host verwendet haben.
- Wenn Sie StorageGRID-Nodes mit Shared Storage unterstützen oder einige oder alle Laufwerke oder SSDs von den ausgefallenen zu den Ersatz-Nodes verschoben haben, müssen Sie dieselben Storage-Zuordnungen wiederherstellen, die auf dem ursprünglichen Host vorhanden waren. Wenn Sie beispielsweise WWIDs und Aliase in verwendet haben `/etc/multipath.conf` Wie in der Installationsanleitung empfohlen, verwenden Sie die gleichen Alias-/WWID-Paare in `/etc/multipath.conf` Auf dem Ersatzhost.
- Wenn der StorageGRID-Node Storage verwendet, der einem NetApp ONTAP System zugewiesen ist, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

Stellen Sie die Grid-Nodes für den Host wieder her

Um einen fehlerhaften Grid-Knoten auf einem neuen Linux-Host wiederherzustellen, führen Sie die folgenden Schritte aus, um die Node-Konfigurationsdatei wiederherzustellen.

1. [Stellen Sie den Knoten wieder her und validieren Sie diesen](#) Durch Wiederherstellen der Node-Konfigurationsdatei. Für eine neue Installation erstellen Sie für jeden Grid-Node, der auf einem Host installiert werden soll, eine Node-Konfigurationsdatei. Beim Wiederherstellen eines Grid-Node auf einem Ersatzhost stellen Sie die Node-Konfigurationsdatei für ausgefallene Grid-Nodes wieder her oder ersetzen sie.
2. [Starten Sie den StorageGRID Host Service](#).
3. Nach Bedarf [Stellen Sie alle Nodes wieder her, die nicht gestartet werden können](#).

Falls alle Block-Storage-Volumes vom vorherigen Host erhalten würden, müssen möglicherweise weitere Recovery-Verfahren durchgeführt werden. Mit den Befehlen in diesem Abschnitt können Sie ermitteln, welche zusätzlichen Verfahren erforderlich sind.

Wiederherstellung und Validierung der Grid Nodes

Sie müssen die Grid-Konfigurationsdateien für alle ausgefallenen Grid-Nodes wiederherstellen, dann die Grid-Konfigurationsdateien validieren und Fehler beheben.

Über diese Aufgabe

Sie können jeden Grid-Node importieren, der auf dem Host vorhanden sein soll, solange er vorhanden ist
`/var/local` Das Volume ging aufgrund des Ausfalls des vorherigen Hosts nicht verloren. Beispiel: Der
`/var/local` Möglicherweise ist das Volume immer noch vorhanden, wenn Sie gemeinsam genutzten Storage für Daten-Volumes von StorageGRID Systemen verwendet haben, wie in der StorageGRID Installationsanleitung für Ihr Linux Betriebssystem beschrieben. Durch das Importieren des Knotens wird seine Knotenkonfigurationsdatei auf den Host wiederhergestellt.

Wenn es nicht möglich ist, fehlende Knoten zu importieren, müssen Sie die zugehörigen Grid-Konfigurationsdateien neu erstellen.

Sie müssen dann die Grid-Konfigurationsdatei validieren und alle Netzwerk- oder Storage-Probleme beheben, bevor Sie StorageGRID neu starten. Wenn Sie die Konfigurationsdatei für einen Node neu erstellen, müssen Sie denselben Namen für den Austausch-Node verwenden, der für den wiederherzustellenden Node verwendet wurde.

Weitere Informationen zum Standort des finden Sie in der Installationsanleitung `/var/local` Volume für einen Node:

- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)

Schritte

1. Führen Sie in der Befehlszeile des wiederhergestellten Hosts alle derzeit konfigurierten StorageGRID-Grid-Knoten auf:
`sudo storagegrid node list`

Wenn keine Grid-Nodes konfiguriert sind, wird keine Ausgabe ausgegeben. Wenn einige Grid-Nodes konfiguriert sind, erwarten Sie die 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-Nodes, die auf dem Host konfiguriert werden sollen, nicht aufgeführt sind, müssen Sie die fehlenden Grid-Nodes wiederherstellen.

2. So importieren Sie Grid-Knoten mit einem `/var/local` Lautstärke:

- 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` Befehl ist nur erfolgreich, wenn der Ziel-Node sauber heruntergefahren wurde auf dem Host, auf dem er zuletzt ausgeführt wurde. Wenn dies nicht der Fall ist, beobachten Sie einen Fehler, der dem folgenden ähnlich ist:

`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 Node, der einem anderen Host gehört, ausgeführt wird, führen Sie den Befehl erneut mit dem aus `--force` Flag, um den Import abzuschließen:`sudo storagegrid --force node import node-var-local-volume-path`



Alle mit dem importierten Knoten `--force` Flag erfordert weitere Wiederherstellungsschritte, bevor sie das Raster erneut verbinden können, wie unter beschrieben "[Nächste Schritte: Falls erforderlich, zusätzliche Recovery-Schritte durchführen](#)".

3. Für Grid-Nodes ohne `/var/local` Volume neu erstellen, um die Konfigurationsdatei des Node auf dem Host wiederherzustellen. Anweisungen hierzu finden Sie unter:

- "[Erstellen Sie Node-Konfigurationsdateien für Red hat Enterprise Linux oder CentOS](#)"
- "[Erstellen Sie Knoten-Konfigurationsdateien für Ubuntu oder Debian](#)"



Wenn Sie die Konfigurationsdatei für einen Node neu erstellen, müssen Sie denselben Namen für den Austausch-Node verwenden, der für den wiederherzuernden Node verwendet wurde. Stellen Sie bei Linux-Bereitstellungen sicher, dass der Name der Konfigurationsdatei den Node-Namen enthält. Sie sollten, wenn möglich, dieselben Netzwerkschnittstellen, Gerätezuordnungen blockieren und IP-Adressen verwenden. Dieses Verfahren minimiert die Datenmenge, die während des Recovery auf den Node kopiert werden muss. Dadurch kann die Recovery erheblich schneller (in manchen Fällen nur Minuten statt Wochen) erfolgen.



Wenn Sie neue Blockgeräte (Geräte, die zuvor vom StorageGRID-Knoten nicht genutzt wurden) als Werte für eine der mit zu startenden Konfigurationsvariablen verwenden `BLOCK_DEVICE_` Wenn Sie die Konfigurationsdatei für einen Node neu erstellen, befolgen Sie die Richtlinien in [Beheben Sie fehlende Blockgerätfehler](#).

4. Führen Sie den folgenden Befehl auf dem wiederhergestellten Host aus, um alle StorageGRID Knoten aufzulisten.

```
sudo storagegrid node list
```

5. Überprüfen Sie die Node-Konfigurationsdatei für jeden Grid-Node, dessen Name in der Ausgabe der StorageGRID-Node-Liste 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 näher erläutert, die bei der Wiederherstellung möglicherweise eine besondere Bedeutung haben.

Beheben Sie fehlende Fehler an der Netzwerkschnittstelle

Wenn das Hostnetzwerk nicht richtig konfiguriert ist oder ein Name falsch geschrieben wird, tritt ein Fehler auf, wenn StorageGRID die in angegebene Zuordnung überprüft `/etc/storagegrid/nodes/node-name.conf` Datei:

Möglicherweise wird ein Fehler oder eine Warnung angezeigt, die diesem Muster entspricht:

```
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 konnte für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk gemeldet werden. Dieser Fehler bedeutet, dass der `/etc/storagegrid/nodes/node-name.conf` Datei ordnet das angezeigte StorageGRID-Netzwerk der Host-Schnittstelle namens zu `host-interface-name`, Aber es gibt keine Schnittstelle mit diesem Namen auf dem aktuellen Host.

Wenn Sie diesen Fehler erhalten, überprüfen Sie, ob Sie die Schritte unter ausgeführt haben "[Implementieren Sie neue Linux-Hosts](#)". Verwenden Sie dieselben Namen für alle Host-Schnittstellen, die auf dem ursprünglichen Host verwendet wurden.

Wenn Sie die Host-Schnittstellen nicht benennen können, die mit der Node-Konfigurationsdatei übereinstimmen, können Sie die Node-Konfigurationsdatei bearbeiten und den Wert des `GRID_NETWORK_TARGET`, `DES ADMIN_NETWORK_TARGET` oder `DES CLIENT_NETWORK_TARGET` ändern, um einer vorhandenen Hostschnittstelle zu entsprechen.

Stellen Sie sicher, dass die Host-Schnittstelle Zugriff auf den entsprechenden physischen Netzwerk-Port oder VLAN bietet und dass die Schnittstelle keinen direkten Bezug auf ein Bond- oder Bridge-Gerät hat. Sie müssen entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät auf dem Host konfigurieren oder ein Bridge- und virtuelles Ethernet-Paar (`veth`) verwenden.

Beheben Sie fehlende Blockgerätfehler

Das System überprüft, ob jeder wiederhergestellte Knoten einer gültigen Blockgerätespezialdatei oder einem gültigen Softlink zu einer speziellen Blockgerätedatei zugeordnet wird. Wenn StorageGRID eine ungültige Zuordnung im findet `/etc/storagegrid/nodes/node-name.conf` Datei: Es wird ein Fehler des Blockgerätes angezeigt.

Wenn Sie einen Fehler beobachten, 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
```

Es bedeutet das `/etc/storagegrid/nodes/node-name.conf` Ordnet das Blockgerät zu, das von *Node-Name* für verwendet wird `PURPOSE` Auf den angegebenen Pfadnamen im Linux-Dateisystem, aber es gibt keine gültige Block Device-Sonderdatei oder Softlink zu einer Block Device-Sonderdatei an diesem Speicherort.

Stellen Sie sicher, dass Sie die Schritte in abgeschlossen haben "[Implementieren Sie neue Linux-Hosts](#)". Verwenden Sie für alle Blockgeräte dieselben persistenten Gerätenamen, die auf dem ursprünglichen Host verwendet wurden.

Wenn Sie die fehlende Sonderdatei für das Blockgerät nicht wiederherstellen oder neu erstellen können, können Sie ein neues Blockgerät mit der entsprechenden Größe und Speicherkategorie zuweisen und die Node-Konfigurationsdatei bearbeiten, um den Wert von zu ändern `BLOCK_DEVICE_PURPOSE` Um auf die neue Block-Device-Sonderdatei zu verweisen.

Ermitteln Sie mithilfe der Tabellen für Ihr Linux-Betriebssystem die geeignete Größe und Storage-Kategorie:

- "[Speicher- und Leistungsanforderungen für Red hat Enterprise Linux oder CentOS](#)"
- "[Speicher- und Leistungsanforderungen für Ubuntu oder Debian](#)"

Überprüfen Sie die Empfehlungen zur Konfiguration des Hostspeichers, bevor Sie mit dem Austausch des Blockgeräts fortfahren:

- "[Konfigurieren Sie den Hostspeicher für Red hat Enterprise Linux oder CentOS](#)"
- "[Konfigurieren Sie den Hostspeicher für Ubuntu oder Debian](#)"



Wenn Sie ein neues Blockspeichergerät für eine der Konfigurationsdateivariablen angeben müssen, die mit `BLOCK_DEVICE_` beginnen, stellen Sie sicher, dass das neue Blockgerät nicht formatiert ist, bevor Sie weitere Wiederherstellungsverfahren durchführen. 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 gegen neue Spezialdateien für das Blockspeichergerät aus.



Führen Sie den folgenden Befehl nur für neue Block Storage-Geräte aus. Führen Sie diesen Befehl nicht aus, wenn Sie glauben, dass der Blockspeicher weiterhin gültige Daten für den wiederhergestellten 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 Host Service

Um die StorageGRID Nodes zu starten und sicherzustellen, dass sie nach einem Neustart des Hosts neu gestartet werden, müssen Sie den StorageGRID Host Service aktivieren und starten.

Schritte

1. Führen Sie auf jedem Host folgende 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 „not running“ oder „` stopped“ zurückgibt, führen Sie den folgenden Befehl aus:

```
sudo storagegrid node start node-name
```

4. Wenn Sie zuvor den StorageGRID-Hostdienst aktiviert und gestartet haben (oder wenn Sie sich nicht sicher sind, ob der Dienst aktiviert und gestartet wurde), führen Sie auch den folgenden Befehl aus:

```
sudo systemctl reload-or-restart storagegrid
```

Wiederherstellung von Nodes, die nicht ordnungsgemäß gestartet werden können

Wenn ein StorageGRID Node nicht normal dem Grid neu beigetreten ist und nicht als wiederherstellbar angezeigt wird, ist er möglicherweise beschädigt. Sie können den Node in den Recovery-Modus erzwingen.

Schritte

1. Vergewissern Sie sich, dass die Netzwerkkonfiguration des Node korrekt ist.

Der Node konnte aufgrund falscher Netzwerkschnittstellen-Zuordnungen oder einer falschen Grid-Netzwerk-IP-Adresse oder eines falschen Gateways möglicherweise nicht erneut dem Grid beitreten.

2. Wenn die Netzwerkkonfiguration korrekt ist, geben Sie das aus `force-recovery` Befehl:

```
sudo storagegrid node force-recovery node-name
```

3. Führen Sie die zusätzlichen Wiederherstellungsschritte für den Node durch. Siehe ["Nächste Schritte: Falls erforderlich, zusätzliche Recovery-Schritte durchführen"](#).

Was ist weiter: Führen Sie zusätzliche Recovery-Schritte, wenn erforderlich

Abhängig von den spezifischen Aktionen, die Sie unternommen haben, um die StorageGRID Nodes auf dem Ersatzhost auszuführen, müssen Sie möglicherweise zusätzliche Recovery-Schritte für jeden Node durchführen.

Die Node-Recovery ist abgeschlossen, wenn Sie keine Korrekturmaßnahmen vornehmen müssen, während Sie den Linux Host ersetzt oder den ausgefallenen Grid Node auf dem neuen Host wiederhergestellt haben.

Korrekturmaßnahmen und nächste Schritte

Während des Austauschs von Nodes müssen Sie möglicherweise eine der folgenden Korrekturmaßnahmen ergreifen:

- Man musste das benutzen `--force` Flag zum Importieren des Knotens.
- Für alle `<PURPOSE>`, Der Wert des `BLOCK_DEVICE_<PURPOSE>` Die Variable der Konfigurationsdatei bezieht sich auf ein Blockgerät, das nicht die gleichen Daten enthält, die es vor dem Ausfall des Hosts gemacht hat.
- Sie sind ausgestellt `storagegrid node force-recovery node-name` Für den Node.
- 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-Node	"Primären Ersatzadministrator-Knoten konfigurieren"
Nicht primärer Admin-Node	"Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren"
Gateway-Node	"Wählen Sie Wiederherstellung starten, um Gateway-Node zu konfigurieren"
Archiv-Node	"Wählen Sie Wiederherstellung starten, um den Knoten Archiv zu konfigurieren"

Art der Wiederherstellung	Nächster Schritt
Storage-Node (softwarebasiert): <ul style="list-style-type: none"> • Wenn man das benutzen musste <code>--force</code> Flag, um den Knoten zu importieren, oder Sie haben ausgegeben <code>storagegrid node force-recovery node-name</code> • Wenn Sie eine vollständige Neuinstallation des Knotens durchführen mussten, oder Sie müssen <code>/var/local</code> wiederherstellen 	"Wählen Sie Wiederherstellung starten, um Speicherknoten zu konfigurieren"
Storage-Node (softwarebasiert): <ul style="list-style-type: none"> • Wenn Sie ein neues Blockgerät hinzugefügt haben. • Wenn, für alle <code><PURPOSE></code>, Der Wert des <code>BLOCK_DEVICE_<PURPOSE></code> Die Variable der Konfigurationsdatei bezieht sich auf ein Blockgerät, das nicht die gleichen Daten enthält, die es vor dem Ausfall des Hosts gemacht hat. 	"Wiederherstellung nach einem Storage-Volume-Ausfall bei intaktem Systemlaufwerk"

Austausch eines fehlerhaften Node durch Services Appliance

Ersetzen Sie einen fehlerhaften Knoten durch eine Service-Appliance: Übersicht

Sie können eine SG100- oder SG1000-Services-Appliance verwenden, um einen fehlgeschlagenen Gateway-Node, einen ausgefallenen nicht-primären Admin-Node oder einen ausgefallenen primären Admin-Node wiederherzustellen, der auf VMware, einem Linux-Host oder einer Services Appliance gehostet wurde. Dieses Verfahren ist ein Schritt der Wiederherstellung des Grid-Nodes.

Bevor Sie beginnen

- Sie haben festgestellt, dass eine der folgenden Situationen zutrifft:
 - Die virtuelle Maschine, die den Knoten hostet, kann nicht wiederhergestellt werden.
 - Der physische oder virtuelle Linux-Host für den Grid-Node ist ausgefallen und muss ersetzt werden.
 - Die Services-Appliance, die den Grid-Node hostet, muss ersetzt werden.
- Sie haben bestätigt, dass die Installationsversion des StorageGRID-Geräts auf der Services-Appliance mit der Softwareversion Ihres StorageGRID-Systems übereinstimmt. Siehe ["Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance"](#).



Implementieren Sie keine SG100- und SG1000-Service-Appliance am selben Standort. Das kann zu einer unvorhersehbaren Performance führen.

Über diese Aufgabe

In den folgenden Fällen können Sie eine SG100- oder SG1000-Services-Appliance verwenden, um einen fehlgeschlagenen Grid-Node wiederherzustellen:

- Der fehlerhafte Knoten wurde auf VMware oder Linux (["Plattformwechsel"](#))
- Der fehlerhafte Knoten wurde auf einer Service-Appliance gehostet (["Platformaustausch"](#))

Installation der Services Appliance (nur Plattformänderung)

Wenn Sie einen fehlerhaften Grid-Node wiederherstellen, der auf VMware oder einem Linux-Host gehostet wurde, und Sie eine Services-Appliance für den Ersatz-Node verwenden, müssen Sie zuerst die neue Appliance-Hardware installieren und dabei denselben Node-Namen (Systemname) wie der ausgefallene Node verwenden.

Bevor Sie beginnen

Sie haben die folgenden Informationen über den ausgefallenen Node:

- **Knotenname:** Sie müssen die Services-Appliance mit dem gleichen Knotennamen wie der ausgefallene Knoten installieren. Der Node-Name ist der Hostname (Systemname).
- **IP-Adressen:** Sie können dem Services-Gerät dieselben IP-Adressen zuweisen wie dem ausgefallenen Knoten, was die bevorzugte Option ist, oder Sie können eine neue ungenutzte IP-Adresse in jedem Netzwerk auswählen.

Über diese Aufgabe

Führen Sie diese Vorgehensweise nur aus, wenn Sie einen ausgefallenen Node, der auf VMware oder Linux gehostet wurde, wiederherstellen und diesen durch einen Node ersetzen, der auf einer Services Appliance gehostet wird.

Schritte

1. Befolgen Sie die Anweisungen zum Installieren einer neuen SG100- oder SG1000-Services-Appliance. Siehe "[Schnellstart für die Hardwareinstallation](#)".
2. Verwenden Sie bei der Aufforderung zu einem Node-Namen den Node-Namen des ausgefallenen Node.

Appliance für die Neuinstallation vorbereiten (nur Plattformaustausch)

Bei der Wiederherstellung eines Grid-Node, der auf einer Services Appliance gehostet wurde, müssen Sie zuerst die Appliance für die Neuinstallation der StorageGRID Software vorbereiten.

Führen Sie diese Schritte nur aus, wenn Sie einen ausgefallenen Node ersetzen, der auf einer Services Appliance gehostet wurde. Befolgen Sie diese Schritte nicht, wenn der ausgefallene Knoten ursprünglich auf VMware oder einem Linux-Host gehostet wurde.

Schritte

1. Loggen Sie sich beim fehlgeschlagenen Grid-Node ein:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Bereiten Sie die Appliance auf die Installation der StorageGRID Software vor. Geben Sie Ein:
`sgareinstall`
3. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie Folgendes ein: `y`

Die Appliance wird neu gestartet, und Ihre SSH-Sitzung wird beendet. In der Regel dauert es etwa 5 Minuten, bis das Installationsprogramm für StorageGRID-Appliances verfügbar ist, obwohl in einigen Fällen Sie möglicherweise bis zu 30 Minuten warten müssen.

Die Services-Appliance wird zurückgesetzt und die Daten auf dem Grid-Node sind nicht mehr verfügbar. Die während der ursprünglichen Installation konfigurierten IP-Adressen sollten intakt bleiben. Nach Abschluss des Vorgangs wird jedoch empfohlen, dies zu bestätigen.

Nach Ausführung des `sgareinstall` Der Befehl entfernt alle über StorageGRID bereitgestellten Konten, Passwörter und SSH-Schlüssel und generiert neue Host-Schlüssel.

Starten der Softwareinstallation auf der Services-Appliance

Um einen Gateway-Node oder Admin-Node auf einer SG100- oder SG1000-Service-Appliance zu installieren, verwenden Sie das Installationsprogramm der StorageGRID-Appliance, das auf der Appliance enthalten ist.

Bevor Sie beginnen

- Die Appliance ist in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Netzwerkverbindungen und IP-Adressen werden für die Appliance mithilfe des Installationsprogramms für die StorageGRID-Appliance konfiguriert.
- Wenn Sie einen Gateway-Node oder einen nicht-primären Admin-Node installieren, kennen Sie die IP-Adresse des primären Admin-Nodes für das StorageGRID-Grid.
- Alle auf der Seite „IP-Konfiguration“ des Installationsprogramms für das StorageGRID-Gerät aufgelisteten Netznetzwerksubnetze sind in der Liste für das Netzwerk des Grid-Netzwerks auf dem primären Administratorknoten definiert.

Siehe "[Schnellstart für die Hardwareinstallation](#)".

- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Sie haben eine der IP-Adressen, die der Appliance zugewiesen sind. Sie können die IP-Adresse für das Admin-Netzwerk, das Grid-Netzwerk oder das Client-Netzwerk verwenden.
- Wenn Sie einen primären Admin-Knoten installieren, haben Sie die Ubuntu- oder Debian-Installationsdateien für diese Version von StorageGRID zur Verfügung.



Eine aktuelle Version der StorageGRID-Software wird während der Fertigung vorinstalliert auf die Services-Appliance geladen. Wenn die vorinstallierte Version der Software mit der Version übereinstimmt, die in Ihrer StorageGRID-Bereitstellung verwendet wird, benötigen Sie die Installationsdateien nicht.

Über diese Aufgabe

So installieren Sie die StorageGRID-Software auf einer SG100- oder SG1000-Services-Appliance:

- Für einen primären Admin-Node geben Sie den Namen des Knotens an und laden dann die entsprechenden Softwarepakete hoch (falls erforderlich).
- Für einen nicht-primären Admin-Node oder einen Gateway-Node geben Sie die IP-Adresse des primären Admin-Node und den Namen des Node an oder bestätigen Sie diese.
- Sie starten die Installation und warten, bis Volumes konfiguriert und die Software installiert ist.

- Durch den Prozess partway, die Installation pausiert. Um die Installation fortzusetzen, müssen Sie sich beim Grid Manager anmelden und den ausstehenden Node als Ersatz für den ausgefallenen Node konfigurieren.
- Nachdem Sie den Node konfiguriert haben, wird die Installation der Appliance abgeschlossen und die Appliance wird neu gestartet.

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für die SG100- oder SG1000-Services-Appliance ein.

`https://Controller_IP:8443`

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Home

This Node

Node type: Gateway ▾

Node name: NetApp-SGA

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery: Uncheck to manually enter the Primary Admin Node IP

Connection state: Admin Node discovery is in progress

Cancel Save

Installation

Current state: Unable to start installation. The Admin Node connection is not ready.

Start installation

2. So installieren Sie einen primären Admin-Knoten:

- a. Wählen Sie im Abschnitt This Node für **Node Type** die Option **Primary Admin** aus.
- b. Geben Sie im Feld **Knotenname** den gleichen 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 Version der zu installierenden Software richtig ist, fahren sie mit fort [Installationsschritt](#).
- d. Wenn Sie eine andere Version der Software hochladen möchten, 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 Checksum-Datei* für die StorageGRID-Software hochzuladen.

Die Dateien werden nach der Auswahl automatisch hochgeladen.

- b. Klicken Sie auf **Startseite**, um zur Startseite des StorageGRID-Appliance-Installationsprogramms zurückzukehren.

3. So installieren Sie einen Gateway-Node oder einen nicht-primären Admin-Node:

- a. Wählen Sie im Abschnitt This Node für **Node Type** die Option **Gateway** oder **Non-Primary Admin** aus, je nach Typ des wiederherzustellenden Knotens.
- b. Geben Sie im Feld **Knotenname** den gleichen Namen ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.
- c. Legen Sie im Abschnitt primäre Administratorknoten-Verbindung fest, ob Sie die IP-Adresse für den primären Admin-Node angeben müssen.

Das Installationsprogramm der StorageGRID-Appliance kann diese IP-Adresse automatisch erkennen, wenn der primäre Admin-Node oder mindestens ein anderer Grid-Node mit Admin_IP konfiguriert ist, sich im selben Subnetz befindet.

- d. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	<ul style="list-style-type: none"> a. Deaktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie Auf Speichern. d. Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.

Option	Beschreibung
Automatische Erkennung aller verbundenen primären Admin-Nodes	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen Admin-Node-Erkennung aktivieren. b. Wählen Sie aus der Liste der ermittelten IP-Adressen den primären Admin-Node für das Grid aus, in dem diese Service-Appliance bereitgestellt wird. c. Klicken Sie Auf Speichern. d. Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.

4. im Abschnitt Installation müssen Sie bestätigen, dass der aktuelle Status bereit ist, die Installation des Knotennamens zu starten, 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-Installationsprogramms auf **Installation starten**.

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.



Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, klicken Sie in der Menüleiste auf **Monitor-Installation**.

Verwandte Informationen

["Wartung von SG100 und SG1000 Appliances"](#)

Überwachen Sie die Installation der Services Appliance

Das Installationsprogramm der StorageGRID Appliance stellt den Status bereit, bis die Installation abgeschlossen ist. Nach Abschluss der Softwareinstallation wird die Appliance neu gestartet.

Schritte

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt 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

In dieser Phase löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken und konfiguriert die Hosteinstellungen.

◦ 2. Installieren Sie das Betriebssystem

Während dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID vom primären Admin-Node auf die Appliance oder installiert das Betriebssystem aus dem Installationspaket für den primären Admin-Node.

3. Überwachen Sie den Installationsfortschritt, bis einer der folgenden Schritte eintritt:

- Bei Appliance-Gateway-Knoten oder nicht-primären Appliance-Admin-Knoten wird die Phase **Install StorageGRID** angehalten. Auf der eingebetteten Konsole wird eine Meldung angezeigt, die Sie dazu auffordert, diesen Knoten auf dem Admin-Knoten mithilfe des Grid-Managers zu genehmigen.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Für primäre Administrator-Knoten der Appliance wird eine fünfte Phase (Installationsprogramm für StorageGRID laden) angezeigt. Wenn die fünfte Phase länger als 10 Minuten in Bearbeitung ist, aktualisieren Sie die Seite manuell.

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Complete
4. Finalize installation	Complete
5. Load StorageGRID Installer	Running

Step	Progress	Status
Starting StorageGRID Installer		Do not refresh. You will be redirected when the installer is ready

4. Fahren Sie mit dem nächsten Schritt des Wiederherstellungsprozesses für den Typ des Grid-Node der Appliance, den Sie wiederherstellen, fort.

Art der Wiederherstellung	Referenz
Gateway-Node	"Wählen Sie Wiederherstellung starten, um Gateway-Node zu konfigurieren"
Nicht primärer Admin-Node	"Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren"
Primärer Admin-Node	"Primären Ersatzadministrator-Knoten konfigurieren"

Durchführen der Standortwiederherstellung durch den technischen Support

Falls eine gesamte StorageGRID Site ausfällt oder mehrere Storage Nodes ausfallen, müssen Sie sich an den technischen Support wenden. Der technische Support analysiert das Unternehmen, entwickelt einen Recovery-Plan und stellt die ausgefallenen Nodes oder Standorte dann auf eine Art und Weise wieder her, die Ihre Geschäftsziele erfüllt. Die Recovery-Zeit wird optimiert und unnötige Datenverluste werden vermieden.



Das Standort-Recovery kann nur durch den technischen Support durchgeführt werden.

StorageGRID Systeme sind für die unterschiedlichsten Fehler anfällig und viele Recovery- und Wartungsvorgänge können problemlos selbst durchgeführt werden. Es ist jedoch schwierig, ein einfaches, generalisiertes Standortwiederherstellungsverfahren zu erstellen, da die detaillierten Schritte von Faktoren abhängen, die spezifisch für Ihre Situation sind. Beispiel:

- **Ihre Geschäftsziele:** Nach dem vollständigen Verlust einer StorageGRID-Website sollten Sie bewerten, wie Sie Ihre Geschäftsziele am besten erreichen können. Möchten Sie beispielsweise den verlorenen Standort neu aufbauen? Möchten Sie die verlorene StorageGRID Site an einem neuen Standort ersetzen? Jede Kundensituation ist anders, und Ihr Recovery-Plan muss Ihre Prioritäten berücksichtigen.
- **Exakte Art des Fehlers:** Stellen Sie vor Beginn einer Standortwiederherstellung fest, ob Knoten am ausgefallenen Standort intakt sind oder ob ein Speicher-Knoten wiederherstellbare Objekte enthält. Wenn

Sie Nodes oder Storage Volumes neu erstellen, die gültige Daten enthalten, kann es zu unnötigen Datenverlusten kommen.

- **Aktive ILM-Richtlinie:** Die Anzahl, Art und der Speicherort von Objektkopien in Ihrem Grid wird durch Ihre aktive ILM-Richtlinie gesteuert. Die Besonderheiten Ihrer ILM-Richtlinie können sich auf die Menge der wiederherstellbaren Daten sowie auf die spezifischen für die Recovery erforderlichen Techniken auswirken.



Wenn ein Standort die einzige Kopie eines Objekts enthält und der Standort verloren geht, geht das Objekt verloren.

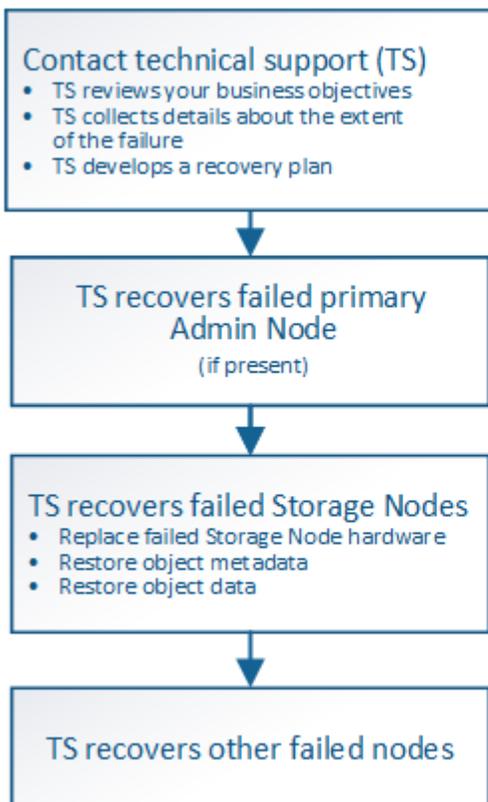
- **Bucket (oder Container) Konsistenz:** Die auf einen Bucket (oder Container) angewendete Konsistenzstufe wirkt sich darauf aus, ob StorageGRID die Objektmetadaten vollständig auf alle Nodes und Standorte repliziert, bevor einem Client mitgeteilt wird, dass die Objektaufnahme erfolgreich war. Wenn die Konsistenzstufe für eventuelle Konsistenz sorgt, sind einige Objektmetadaten bei einem Standortausfall verloren gegangen. Dies kann sich auf die Menge der wiederherstellbaren Daten und möglicherweise auf die Details des Recovery-Verfahrens auswirken.
- **Historie der neuesten Änderungen:** Die Details Ihres Wiederherstellungsverfahrens können davon beeinflusst werden, ob zum Zeitpunkt des Ausfalls Wartungsarbeiten durchgeführt wurden oder ob kürzlich Änderungen an Ihrer ILM-Richtlinie vorgenommen wurden. Der technische Support muss den aktuellen Verlauf des Grid sowie dessen aktuelle Situation vor Beginn einer Wiederherstellung des Standorts beurteilen.

Überblick über die Standortwiederherstellung

Dies ist eine allgemeine Übersicht über das Verfahren, das der technische Support zur Wiederherstellung eines ausgefallenen Standorts verwendet.



Das Standort-Recovery kann nur durch den technischen Support durchgeführt werden.



Caution: Do not use the recovery procedures designed for a single failed Storage Node. Data loss will occur.

1. Wenden Sie sich an den technischen Support.

Der technische Support führt eine detaillierte Bewertung der Fehler durch und prüft gemeinsam mit Ihnen Ihre Geschäftsziele. Auf der Grundlage dieser Informationen entwickelt der technische Support einen Recovery-Plan, der auf Ihre Situation zugeschnitten ist.

2. Der technische Support stellt den primären Admin-Knoten wieder her, wenn er ausgefallen ist.

3. Der technische Support stellt alle Storage-Knoten wieder her, folgt dieser Beschreibung:

- a. Ersetzen Sie bei Bedarf Storage Node Hardware oder Virtual Machines.
- b. Wiederherstellung von Objektmetadaten am ausgefallenen Standort
- c. Wiederherstellung von Objektdaten auf den wiederhergestellten Storage-Nodes



Wenn die Wiederherstellungsverfahren für einen einzelnen ausgefallenen Speicherknoten verwendet werden, kann es zu Datenverlusten kommen.



Wenn ein kompletter Standort ausfällt, sind spezielle Befehle erforderlich, um Objekte und Objektmetadaten erfolgreich wiederherzustellen.

4. Der technische Support stellt andere ausgefallene Nodes wieder her.

Nach der Wiederherstellung von Objektmetadaten und -Daten können fehlerhafte Gateway-Nodes, nicht primäre Admin-Nodes oder Archiv-Nodes anhand von Standardverfahren wiederhergestellt werden.

Verwandte Informationen

["Deaktivierung der Website"](#)

Verfahren zur Deaktivierung

Ablauf der Stilllegung: Übersicht

Sie können einen Außerbetriebnahme durchführen, um Grid-Nodes oder eine ganze Website dauerhaft vom StorageGRID System zu entfernen.

Um einen Grid-Node oder einen Standort zu entfernen, führen Sie einen der folgenden Verfahren zur Deaktivierung durch:

- Führen Sie ein aus ["Stilllegung des Grid-Nodes"](#) Um einen oder mehrere Knoten zu entfernen, die sich an einem oder mehreren Standorten befinden können. Die entfernenden Nodes können online und mit dem StorageGRID System verbunden sein oder offline bzw. getrennt sein.
- Führen Sie ein aus ["Website-Deaktivierung"](#) Um einen Standort zu entfernen. Sie führen eine **verbundene Deaktivierung** durch, wenn alle Knoten mit StorageGRID verbunden sind. Sie führen eine * nicht verbundene Website-Stilllegung * durch, wenn alle Knoten von StorageGRID getrennt sind.



Bevor Sie eine Website außer Betrieb nehmen, müssen Sie sich an Ihren NetApp Ansprechpartner wenden. NetApp überprüft Ihre Anforderungen, bevor Sie alle Schritte im Decommission Site Wizard aktivieren. Sie sollten keinen Versuch Unternehmen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie der Meinung sind, dass eine Wiederherstellung der Site oder die Wiederherstellung von Objektdaten von der Site möglich wäre.

Wenn ein Standort eine Mischung aus verbundenen (✔) Und nicht verbundene Knoten (☾ Oder 🔄), Sie müssen alle Offline-Knoten wieder online bringen.



Wenn Sie eine zweite Wartung durchführen müssen, können Sie "[Unterbrechen Sie die Deaktivierung, während die Speicherknoten entfernt werden](#)". Die Schaltfläche **Pause** ist nur aktiviert, wenn die ILM-Bewertung oder die mit Erasure Coding versehenen Phasen der Datenauswertung erreicht sind. Die ILM-Evaluierung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt. Nach Abschluss des zweiten Wartungsverfahrens können Sie die Außerbetriebnahme fortsetzen.

Der Grid-Node wird deaktiviert

Deaktivierung von Grid Nodes: Übersicht

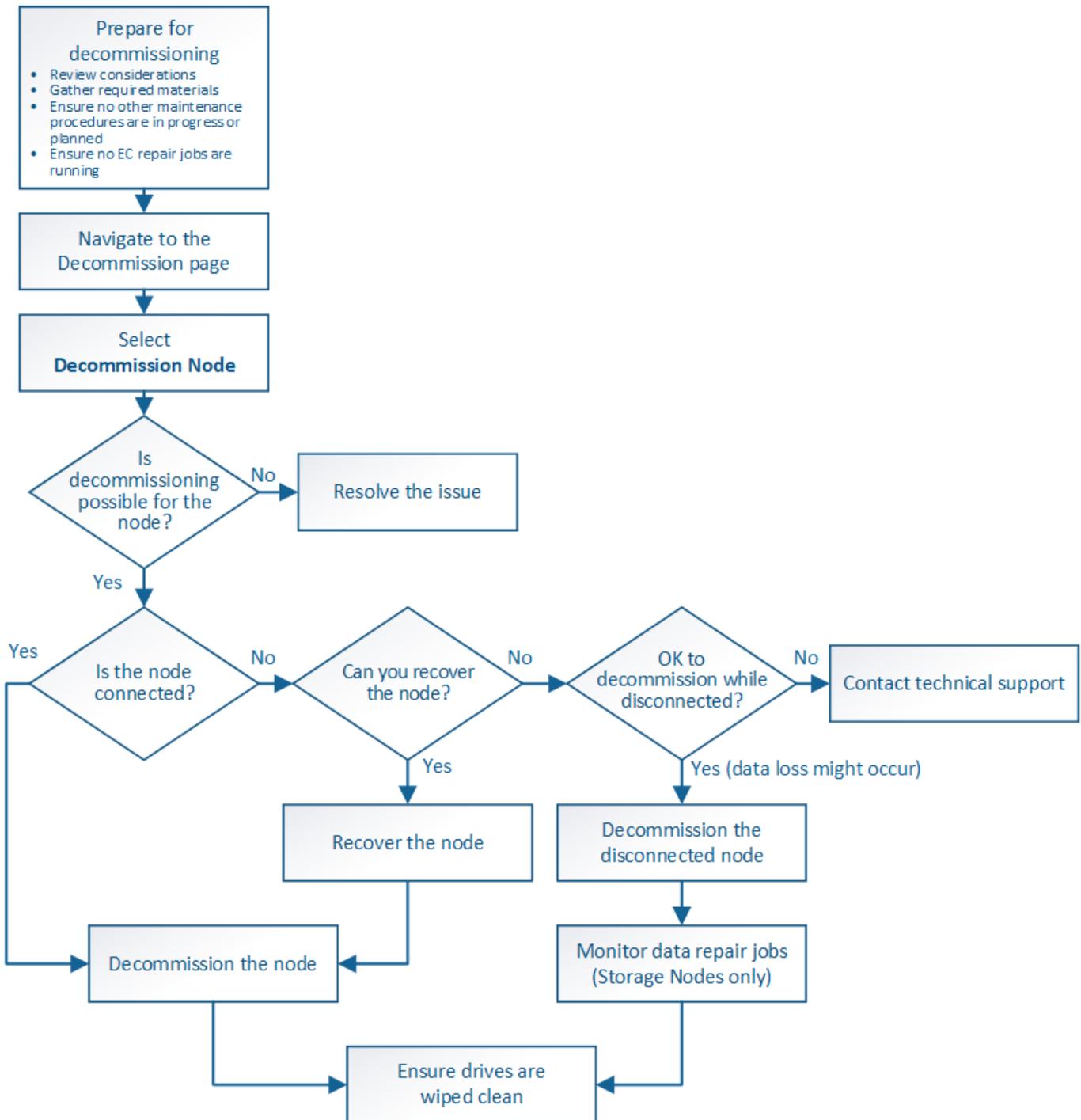
Sie können den Node Decounter-Vorgang verwenden, um einen oder mehrere Storage-Nodes, Gateway-Nodes oder nicht-primäre Admin-Nodes an einem oder mehreren Standorten zu entfernen. Sie können den primären Admin-Node oder einen Archive Node nicht stilllegen.

Im Allgemeinen sollten die Grid-Knoten nur dann außer Betrieb gesetzt werden, wenn sie mit dem StorageGRID-System verbunden sind und alle Knoten im normalen Zustand sind (mit grünen Symbolen auf den **NODES**-Seiten und auf der Seite **Decommission-Knoten**). Bei Bedarf können Sie jedoch einen nicht verbundenen Grid-Node außer Betrieb nehmen. Bevor Sie einen getrennten Knoten entfernen, stellen Sie sicher, dass Sie die Auswirkungen und Einschränkungen dieses Prozesses verstehen.

Wenn einer der folgenden Optionen zutrifft, wird das Verfahren zur Deaktivierung des Nodes ausgeführt:

- Sie haben dem System einen größeren Speicherknoten hinzugefügt, und Sie möchten einen oder mehrere kleinere Speicherknoten entfernen, während gleichzeitig Objekte erhalten bleiben.
- Sie benötigen weniger Storage insgesamt.
- Sie benötigen keinen Gateway-Node mehr.
- Sie benötigen keinen nicht mehr primären Admin-Node.
- Das Raster enthält einen getrennten Knoten, den Sie nicht wiederherstellen oder wieder in den Online-Modus versetzen können.

Das Flussdiagramm zeigt die grundlegenden Schritte zur Deaktivierung von Grid-Nodes.



Überlegungen zur Deaktivierung des Grid Node

Allgemeine Überlegungen zur Stilllegung von Grid-Nodes

Bevor Sie dieses Verfahren zur Deaktivierung von einem oder mehreren Nodes starten, müssen Sie die Auswirkungen des Entfernens der einzelnen Node verstehen. Bei der erfolgreichen Ausmusterung eines Node werden seine Services deaktiviert und der Node wird automatisch heruntergefahren.

Sie können einen Node nicht ausmustern, wenn Sie dazu den StorageGRID in einem ungültigen Status belassen. Folgende Regeln werden durchgesetzt:

- Der primäre Admin-Node kann nicht stillgelegt werden.
- Archive Nodes können nicht stillgelegt werden.
- Sie können einen Admin-Node oder einen Gateway-Node nicht stilllegen, wenn eine seiner Netzwerkschnittstellen Teil einer HA-Gruppe ist.
- Sie können einen Speicher-Node nicht stilllegen, wenn dessen Entfernung das ADC-Quorum beeinträchtigen würde.
- Sie können einen Storage Node nicht stilllegen, wenn er für die aktive ILM-Richtlinie erforderlich ist.
- Sie sollten nicht mehr als 10 Storage-Nodes in einem einzigen Decommission-Node-Verfahren außer Betrieb nehmen.
- Sie können einen verbundenen Knoten nicht stilllegen, wenn Ihr Raster getrennte Knoten enthält (Knoten, deren Zustand Unbekannt oder Administrativ inaktiv ist). Sie müssen zunächst die getrennten Nodes außer Betrieb nehmen oder wiederherstellen.
- Wenn Ihr Grid mehrere getrennte Knoten enthält, muss die Software gleichzeitig ausmustern, wodurch das Potenzial für unerwartete Ergebnisse erhöht wird.
- Wenn ein getrennter Knoten nicht entfernt werden kann (z. B. ein Speicher-Knoten, der für das ADC-Quorum erforderlich ist), kann kein anderer getrennter Knoten entfernt werden.
- Wenn Sie ein älteres Gerät durch ein neueres Gerät ersetzen möchten, sollten Sie dies in Betracht ziehen ["Klonen des Appliance-Node"](#) Statt den alten Node außer Betrieb zu setzen und den neuen Node in einer Erweiterung hinzuzufügen.



Entfernen Sie die Virtual Machine oder andere Ressourcen eines Grid-Node erst, wenn Sie im Ausmusterungsverfahren dazu aufgefordert werden.

Überlegungen zur Deaktivierung von Admin Node oder Gateway Node

Prüfen Sie die folgenden Überlegungen, bevor Sie einen Admin-Node oder einen Gateway-Node außer Betrieb setzen.

- Für das Verfahren zur Deaktivierung ist ein exklusiver Zugriff auf einige Systemressourcen erforderlich. Sie müssen also bestätigen, dass keine weiteren Wartungsverfahren ausgeführt werden.
- Der primäre Admin-Node kann nicht stillgelegt werden.
- Sie können einen Admin-Node oder einen Gateway-Node nicht stilllegen, wenn eine seiner Netzwerkschnittstellen Teil einer HA-Gruppe ist. Sie müssen zuerst die Netzwerkschnittstellen aus der HA-Gruppe entfernen. Siehe Anweisungen für ["Verwalten von HA-Gruppen"](#).
- Bei Bedarf können Sie die ILM-Richtlinie sicher ändern und gleichzeitig einen Gateway-Node oder einen Admin-Node außer Betrieb nehmen.
- Wenn Sie einen Admin-Node deaktivieren und Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, müssen Sie daran denken, das Vertrauen des Knotens zu entfernen, das auf die Grundlage von Active Directory Federation Services (AD FS) basiert.
- Wenn Sie verwenden ["Grid-Verbund"](#), Stellen Sie sicher, dass die IP-Adresse des Node, den Sie decommissionieren, nicht für eine Netzverbundverbindung angegeben wurde.

Storage-Nodes

Überlegungen zur Deaktivierung von Storage Node

Wenn Sie einen Storage Node außer Betrieb nehmen möchten, müssen Sie wissen, wie StorageGRID die Objektdaten und Metadaten dieses Node managt.

Bei der Ausmusterung von Storage-Nodes gelten die folgenden Überlegungen und Einschränkungen:

- Das System muss zu jeder Zeit genügend Storage Nodes enthalten, um den betrieblichen Anforderungen gerecht zu werden, einschließlich des ADC-Quorums und der aktiven ILM-Richtlinie. Um diese Einschränkung zu erfüllen, müssen Sie möglicherweise einen neuen Storage-Node zu einem Erweiterungsvorgang hinzufügen, bevor Sie einen vorhandenen Storage-Node stilllegen können.
- Wenn der Storage-Node getrennt wird, wenn Sie ihn ausmustern, muss das System die Daten mithilfe der Daten der verbundenen Storage-Nodes rekonstruieren. Dies kann zu Datenverlusten führen.
- Wenn Sie einen Storage-Node entfernen, müssen große Mengen von Objektdaten über das Netzwerk übertragen werden. Obwohl diese Transfers den normalen Systembetrieb nicht beeinträchtigen sollten, können sie sich auf die gesamte vom StorageGRID System benötigte Netzwerkbandbreite auswirken.
- Aufgaben für die Deaktivierung von Storage-Nodes haben eine niedrigere Priorität als Aufgaben, die mit normalen Systemvorgängen verbunden sind. Dadurch wird die Ausmusterung normale StorageGRID Systemvorgänge nicht beeinträchtigt und es muss keine Zeit für die Inaktivität des Systems eingeplant werden. Da die Ausmusterung im Hintergrund erfolgt, ist es schwierig zu schätzen, wie lange der Vorgang dauert. Im Allgemeinen erfolgt die Ausmusterung von Storage-Nodes schneller, wenn das System still ist oder nur ein Storage-Node gleichzeitig entfernt wird.
- Es kann Tage oder Wochen dauern, bis ein Storage-Node außer Betrieb gesetzt wurde. Planen Sie dieses Verfahren entsprechend. Der Prozess zur Deaktivierung sorgt zwar dafür, dass der Betrieb des Systems nicht beeinträchtigt wird, aber weitere Verfahren werden möglicherweise eingeschränkt. Im Allgemeinen sollten geplante System-Upgrades oder -Erweiterungen durchgeführt werden, bevor Grid-Nodes entfernt werden.
- Während bestimmter Phasen können Verfahren zur Deaktivierung von Speicherknoten angehalten werden, damit andere Wartungsvorgänge bei Bedarf ausgeführt und nach Abschluss wieder aufgenommen werden können.
- Wenn eine Ausmusterung ausgeführt wird, können keine Datenreparaturvorgänge auf Grid-Nodes ausgeführt werden.
- Während der Deaktivierung eines Storage Node sollten Sie keine Änderungen an der ILM-Richtlinie vornehmen.
- Wenn Sie einen Storage-Node entfernen, werden die Daten des Node zu anderen Grid-Nodes migriert. Diese Daten werden jedoch nicht vollständig aus dem ausgemusterten Grid-Node entfernt. Zum endgültigen und sicheren Entfernen von Daten müssen die Laufwerke des ausgemusterten Grid-Nodes nach Abschluss des Stilllegen-Vorgangs gelöscht werden.
- Wenn Sie einen Storage-Node außer Betrieb nehmen, werden möglicherweise die folgenden Warnmeldungen und Alarmer ausgelöst. Darüber hinaus erhalten Sie möglicherweise entsprechende E-Mail- und SNMP-Benachrichtigungen:
 - **Kommunikation mit Knoten** Warnung nicht möglich. Diese Warnmeldung wird ausgelöst, wenn Sie einen Speicherknoten außer Betrieb setzen, der den ADC-Dienst enthält. Die Meldung wird nach Abschluss des Stilllegen-Vorgangs behoben.
 - VSTU-Alarm (Object Verification Status). Dieser Alarm auf Benachrichtigungsebene zeigt an, dass der Speicherknoten während der Stilllegung in den Wartungsmodus wechselt.
 - CASA (Data Store Status) Alarm. Dieser Großalarm zeigt an, dass die Cassandra-Datenbank ausfällt, da die Dienste angehalten wurden.

Verwandte Informationen

["Wiederherstellung von Objektdaten auf dem Storage-Volume"](#)

Das ADC-Quorum verstehen

Bestimmte Storage-Nodes können an einem Datacenter-Standort möglicherweise nicht außer Betrieb gesetzt werden, falls nach der Ausmusterung zu wenige Dienste des Administrative Domain Controller (ADC) verbleiben würden. Dieser Service, der auf einigen Storage-Nodes enthalten ist, pflegt Grid-Topologiedaten und stellt Konfigurationsdienste für das Grid bereit. Das StorageGRID System erfordert, dass an jedem Standort und zu jeder Zeit ein Quorum von ADC-Services verfügbar ist.

Sie können einen Speicher-Node nicht stilllegen, wenn das Entfernen des Knotens dazu führen würde, dass das ADC-Quorum nicht mehr erfüllt wird. Um das ADC-Quorum während eines Stilllegungsvorgangs zu erfüllen, muss an jedem Datacenter mindestens drei Storage-Nodes über den ADC-Service verfügen. Bei mehr als drei Storage-Nodes an einem Datacenter mit dem ADC-Service muss ein einfacher Großteil dieser Nodes nach der Ausmusterung verfügbar sein ($(0.5 * \text{Storage Nodes with ADC}) + 1$).

Nehmen Sie beispielsweise an, ein Datacenter-Standort umfasst derzeit sechs Storage-Nodes mit ADC-Services, und Sie möchten drei Storage-Nodes außer Betrieb nehmen. Aufgrund der Quorum-Anforderung des ADC müssen Sie zwei Verfahren zur Deaktivierung durchführen:

- Beim ersten Stilllegen müssen Sie sicherstellen, dass vier Speicherknoten mit ADC-Diensten verfügbar bleiben ($(0.5 * 6) + 1$). Das bedeutet, dass Sie zunächst nur zwei Storage-Nodes außer Betrieb nehmen können.
- Im zweiten Verfahren können Sie den dritten Speicherknoten entfernen, da das ADC-Quorum jetzt nur noch drei ADC-Dienste benötigt ($(0.5 * 4) + 1$).

Wenn ein Speicherknoten außer Betrieb gesetzt werden muss, aber aufgrund der ADC-Quorum-Anforderung nicht in der Lage ist, müssen Sie einen neuen Speicherknoten in einer Erweiterung hinzufügen und angeben, dass er über einen ADC-Dienst verfügen soll. Anschließend können Sie den vorhandenen Storage-Node ausmustern.

Verwandte Informationen

["Erweitern Sie Ihr Raster"](#)

Prüfen der ILM-Richtlinie und Storage-Konfiguration

Wenn Sie einen Storage-Node außer Betrieb nehmen möchten, sollten Sie die ILM-Richtlinie Ihres StorageGRID Systems überprüfen, bevor Sie den Ausmusterungsprozess starten.

Bei der Ausmusterung werden alle Objektdaten vom ausgemusterten Storage Node zu anderen Storage-Nodes migriert.



Die ILM-Richtlinie, die Sie während der Stilllegung haben, wird *nach* der Deaktivierung verwendet. Sie müssen sicherstellen, dass diese Richtlinie sowohl vor Beginn der Stilllegung als auch nach Abschluss der Stilllegung Ihre Daten erfüllt.

Sie sollten die Regeln in der aktiven ILM-Richtlinie überprüfen, um sicherzustellen, dass das StorageGRID System weiterhin über ausreichende Kapazität des richtigen Typs und an den richtigen Standorten verfügt, um

die Ausmusterung eines Storage-Nodes bewältigen zu können.

Bedenken Sie Folgendes:

- Werden ILM-Evaluierungsservices möglich sein, Objektdaten so zu kopieren, dass ILM-Regeln erfüllt sind?
- Was passiert, wenn ein Standort während der Stilllegung vorübergehend nicht mehr verfügbar ist? Können zusätzliche Kopien an einem alternativen Speicherort erstellt werden?
- Wie wird sich der Ausmusterungsprozess auf die finale Verteilung der Inhalte auswirken? Wie in beschrieben "[Storage-Nodes Konsolidieren](#)", Sie sollten neue Storage-Nodes hinzufügen, bevor Sie alte stilllegen. Wenn Sie nach der Stilllegung eines kleineren Storage-Nodes einen größeren Ersatz-Storage-Node hinzufügen, könnten die alten Storage-Nodes nahezu an Kapazität arbeiten und der neue Storage-Node könnte fast keinen Inhalt haben. Die meisten Schreibvorgänge für neue Objektdaten würden dann auf den neuen Storage-Node geleitet, wodurch die allgemeine Effizienz der Systemvorgänge verringert wird.
- Wird das System jederzeit genügend Storage-Nodes enthalten, um die aktive ILM-Richtlinie zu erfüllen?



Eine ILM-Richtlinie, die nicht zufriedengestellt werden kann, führt zu Rückprotokollen und Alarmen und kann den Betrieb des StorageGRID Systems unterbrechen.

Überprüfen Sie, ob die vorgeschlagene Topologie, die sich aus dem Stilllegungsvorgang ergibt, die ILM-Richtlinie erfüllt, indem Sie die in der Tabelle aufgeführten Faktoren bewerten.

Einzuschätzen	Hinweise
Verfügbare Kapazität	Werden genügend Storage-Kapazitäten für alle im StorageGRID System gespeicherten Objektdaten vorhanden sein, Sollen die permanenten Kopien der aktuell auf dem Storage Node gespeicherten Objektdaten stillgelegt werden?gibt es genügend Kapazität, um das erwartete Wachstum gespeicherter Objektdaten für ein vernünftiges Zeitintervall nach der Stilllegung zu verarbeiten?
Speicherort	Wenn genügend Kapazität im gesamten StorageGRID System verbleibt, sind die Kapazitäten an den richtigen Standorten, um den Geschäftsregeln des StorageGRID Systems gerecht zu werden?
Storage-Typ	Wird es genügend Storage des entsprechenden Typs geben, nachdem die Ausmusterung abgeschlossen ist? So kann es beispielsweise aufgrund von ILM-Regeln geben, dass Inhalte je nach Alter von einem Storage-Typ auf einen anderen verschoben werden. Wenn dies der Fall ist, müssen Sie sicherstellen, dass in der endgültigen Konfiguration des StorageGRID Systems genügend Storage des entsprechenden Typs verfügbar ist.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Erweitern Sie Ihr Raster"](#)

Trennen Sie nicht verbundene Storage-Nodes außer Betrieb

Sie müssen wissen, was passieren kann, wenn Sie einen Storage-Knoten außer Betrieb setzen, während er nicht verbunden ist (Zustand ist unbekannt oder administrativ ausgefallen).

Wenn Sie einen Storage-Node, der vom Raster getrennt wird, außer Betrieb nehmen, verwendet StorageGRID Daten von anderen Storage-Nodes, um die Objektdaten und Metadaten des getrennten Node zu rekonstruieren. Dazu werden am Ende des Stilllegungsvorgangs automatisch Datenreparaturaufgaben gestartet.

Bevor Sie einen getrennten Storage-Node stilllegen, müssen Sie Folgendes beachten:

- Getrennte Nodes dürfen niemals außer Betrieb genommen werden, es sei denn, Sie sind sicher, dass sie nicht online geschaltet oder wiederhergestellt werden können.



Führen Sie dieses Verfahren nicht aus, wenn Sie der Meinung sind, dass Objektdaten vom Node wiederhergestellt werden können. Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, ob das Recovery von Nodes möglich ist.

- Wenn ein getrennter Storage-Node die einzige Kopie eines Objekts enthält, geht dieses Objekt verloren, wenn Sie den Node ausmustern. Die Datenrekonstruktionsaufgaben können Objekte nur rekonstruieren und wiederherstellen, wenn mindestens eine replizierte Kopie oder genug Fragmente mit Lösungscode auf aktuell verbundenen Storage-Nodes vorhanden sind.
- Wenn Sie einen getrennten Storage-Node ausmustern, wird der Vorgang der Ausmusterung relativ schnell abgeschlossen. Die Ausführung von Datenreparaturen kann jedoch Tage oder Wochen dauern und wird nicht durch die Außerbetriebnahme überwacht. Sie müssen diese Jobs manuell überwachen und nach Bedarf neu starten. Siehe "[Prüfen Sie die Reparatur von Daten](#)".
- Wenn Sie mehrere getrennte Storage-Nodes gleichzeitig außer Betrieb nehmen, kann es zu Datenverlusten kommen. Das System ist möglicherweise nicht in der Lage, Daten zu rekonstruieren, wenn zu wenige Kopien von Objektdaten, Metadaten oder Erasure-Coding-Fragmenten verfügbar sind.



Wenn Sie mehr als einen getrennten Storage Node haben, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

Storage-Nodes Konsolidieren

Sie können Storage-Nodes konsolidieren, um die Anzahl der Storage-Nodes für einen Standort oder eine Bereitstellung zu verringern und gleichzeitig die Storage-Kapazität zu erhöhen.

Wenn Sie Storage-Nodes konsolidieren, erweitern Sie das StorageGRID System, um neue Storage-Nodes mit größerer Kapazität hinzuzufügen, und Mustern die alten Storage-Nodes mit geringerer Kapazität aus. Während der Deaktivierung werden Objekte von den alten Storage Nodes zu den neuen Storage Nodes migriert.



Wenn Sie ältere und kleinere Appliances mit neuen Modellen oder Appliances mit höherer Kapazität konsolidieren, nutzen viele die Node-Klonfunktion oder das Verfahren zum Klonen von Nodes und setzen die Stilllegung um, wenn Sie keinen Einzelaustausch vornehmen.

Beispielsweise können Sie zwei neue Storage-Nodes mit größerer Kapazität hinzufügen, um drei ältere

Storage-Nodes zu ersetzen. Sie würden zuerst das Erweiterungsverfahren verwenden, um die beiden neuen, größeren Storage-Nodes hinzuzufügen, und anschließend die drei alten Storage-Nodes mit geringerer Kapazität entfernen.

Durch Hinzufügen neuer Kapazität vor dem Entfernen vorhandener Storage-Nodes wird eine ausgewogenere Datenverteilung im gesamten StorageGRID System sichergestellt. Sie reduzieren auch die Möglichkeit, dass ein vorhandener Storage-Node über die Storage-Grenzmarke hinaus geschoben werden kann.

Verwandte Informationen

["Erweitern Sie Ihr Raster"](#)

Ausmustern mehrerer Storage-Nodes

Wenn mehr als ein Storage-Node entfernt werden muss, können Sie sie nacheinander oder parallel absetzen.

- Wenn Sie Storage-Nodes nacheinander ausmustern, müssen Sie warten, bis der erste Storage-Node heruntergefahren wurde, bevor Sie den nächsten Storage-Node außer Betrieb nehmen.
- Wenn Sie Storage-Nodes parallel ausmustern, verarbeiten die Storage-Nodes zugleich Aufgaben zur Deaktivierung aller Storage-Nodes. Dies kann dazu führen, dass alle permanenten Kopien einer Datei als "read-only," markiert werden, wenn das Löschen in Gittern, in denen diese Funktion aktiviert ist, vorübergehend deaktiviert wird.

Prüfen Sie die Reparatur von Daten

Bevor Sie einen Grid-Node außer Betrieb nehmen, müssen Sie bestätigen, dass keine Datenreparatur-Jobs aktiv sind. Wenn Reparaturen fehlgeschlagen sind, müssen Sie sie neu starten und vor der Außerbetriebnahme abschließen lassen.

Wenn Sie einen nicht verbundenen Speicherknoten stilllegen müssen, führen Sie diese Schritte auch nach Abschluss des Stilllegungsvorgangs aus, um sicherzustellen, dass der Datenreparaturauftrag erfolgreich abgeschlossen wurde. Sie müssen sicherstellen, dass alle Fragmente, die mit Erasure-Coding-Verfahren codiert wurden, die sich auf dem entfernten Node befanden, erfolgreich wiederhergestellt wurden.

Die Schritte gelten nur für Systeme mit Erasure-Coding-Objekten.

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` bis `#`.

- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

2. Auf laufende Reparaturen prüfen: `repair-data show-ec-repair-status`

- Wenn Sie noch nie einen Datenreparaturauftrag ausgeführt haben, wird die Ausgabe angezeigt `No job found`. Sie müssen keine Reparaturjobs neu starten.
- Wenn der Datenreparaturauftrag zuvor ausgeführt wurde oder derzeit ausgeführt wird, listet die Ausgabe Informationen für die Reparatur auf. Jede Reparatur hat eine eindeutige Reparatur-ID.

Fahren Sie mit dem nächsten Schritt fort.

- Sie können auch den Status der in Verarbeitung befindeten Wiederherstellungsaufträge überwachen und den Verlauf der in abgeschlossenen Wiederherstellungsaufträge anzeigen "[Grid Manager](#)".

```

root@ADM1-0:~# repair-data show-ec-repair-status
Repair ID      Affected Nodes / Volumes      Start Time      End Time      State      Estimated Bytes Affected      Bytes Repaired      Percentage
-----
4216507958013005550  DC1-S1-0-182 (Volumes: 2)  2022-08-17T21:37:30.051543  2022-08-17T21:37:37.320998  Completed  1015788876                    0                    0
18214680851049518682  DC1-S1-0-182 (Volumes: 1)  2022-08-17T20:37:58.869362  2022-08-17T20:38:45.299688  Completed  0                              0                    100
7962734388032289010  DC1-S1-0-182 (Volumes: 0)  2022-08-17T20:42:29.578740                                Stopped                               0                    0                    Unknown
  
```

3. Wenn der Zustand für alle Reparaturen ist `Completed`, Sie brauchen keine Reparatur-Jobs neu zu starten.
4. Wenn der Status für eine Reparatur ist `Stopped`, Sie müssen diese Reparatur neu starten.
 - a. Beziehen Sie die Reparatur-ID für die fehlerhafte Reparatur von der Ausgabe.
 - b. Führen Sie die aus `repair-data start-ec-node-repair` Befehl.

Verwenden Sie die `--repair-id` Option zum Festlegen der Reparatur-ID. Wenn Sie beispielsweise eine Reparatur mit der Reparatur-ID 949292 erneut versuchen möchten, führen Sie den folgenden Befehl aus: `repair-data start-ec-node-repair --repair-id 949292`

- c. Verfolgen Sie den Status der EC-Datenreparaturen weiter, bis der Zustand für alle Reparaturen vorliegt `Completed`.

Sammeln Sie die erforderlichen Materialien

Bevor Sie einen Grid-Node außer Betrieb nehmen, müssen Sie die folgenden Informationen erhalten.

Element	Hinweise
Wiederherstellungspaket <code>.zip</code> Datei	Unbedingt " Laden Sie das neueste Wiederherstellungspaket herunter " <code>.zip</code> Datei (sgws-recovery-package-id-revision.zip). Sie können die Recovery Package-Datei verwenden, um das System wiederherzustellen, wenn ein Fehler auftritt.
<code>Passwords.txt</code> Datei	Diese Datei enthält die Passwörter, die für den Zugriff auf Grid-Knoten in der Befehlszeile erforderlich sind und im Wiederherstellungspaket enthalten sind.
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im <code>Passwords.txt</code> Datei:
Beschreibung der Topologie des StorageGRID Systems vor der Stilllegung	Falls verfügbar, finden Sie eine Dokumentation, die die aktuelle Topologie des Systems beschreibt.

Verwandte Informationen

["Anforderungen an einen Webbrowser"](#)

Öffnen Sie die Seite Decommission Nodes

Wenn Sie im Grid Manager auf die Seite Decommission Nodes zugreifen, sehen Sie auf einen Blick, welche Knoten deaktiviert werden können.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Berechtigung Wartung oder Stammzugriff.

Schritte

1. Wählen Sie **MAINTENANCE > Tasks > Decommission**.
2. Wählen Sie **Decommission Nodes**.

Die Seite Decommission Nodes wird angezeigt. Auf dieser Seite können Sie:

- Legen Sie fest, welche Grid-Nodes derzeit deaktiviert werden können.
- Den Systemzustand aller Grid-Nodes anzeigen
- Sortieren Sie die Liste in aufsteigender oder absteigender Reihenfolge nach **Name, Standort, Typ** oder **hat ADC**.
- Geben Sie Suchbegriffe ein, um bestimmte Nodes schnell zu finden. Beispielsweise werden auf dieser Seite die Grid-Nodes in zwei Datacentern angezeigt. Die Spalte Decommission Mögliche gibt an, dass Sie den Gateway-Node, einen der fünf Storage-Nodes und den nicht primären Admin-Node außer Betrieb nehmen können.

Decommission Nodes

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes



Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, primary Admin Node decommissioning is not supported.
DC1-ARC1	Data Center 1	Archive Node	-		No, Archive Nodes decommissioning is not supported.
<input type="checkbox"/> 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.
<input type="checkbox"/> DC1-S4	Data Center 1	Storage Node	No		
<input type="checkbox"/> DC2-ADM1	Data Center 2	Admin Node	-		
DC2-S1	Data Center 2	Storage Node	Yes		No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services.

3. Überprüfen Sie die Spalte **Decommission möglich** für jeden Knoten, den Sie stilllegen möchten.

Wenn ein Gitterknoten außer Betrieb genommen werden kann, enthält diese Spalte ein grünes Häkchen, und die linke Spalte enthält ein Kontrollkästchen. Wenn ein Node nicht stillgelegt werden kann, wird in dieser Spalte das Problem beschrieben. Wenn mehr als ein Grund dafür besteht, dass ein Node nicht ausgemustert werden kann, wird der kritischsten Grund angezeigt.

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
Nein, die Ausmusterung von Node-Typen wird nicht unterstützt.	Sie können den primären Admin-Node oder einen Archive Node nicht stilllegen.	Keine.
<p>Nein, mindestens ein Grid-Node ist getrennt.</p> <p>Hinweis: Diese Meldung wird nur für verbundene Grid-Knoten angezeigt.</p>	<p>Ein verbundener Grid-Node kann nicht stillgelegt werden, wenn ein Grid-Node getrennt wird.</p> <p>Die Spalte Health enthält eines der folgenden Symbole für getrennte Grid-Knoten:</p> <ul style="list-style-type: none"> •  (Grau): Administrativ nach unten •  (Blau): Unbekannt 	Wechseln Sie zum Schritt, in dem die Optionen für das Stilllegen aufgeführt sind .
<p>Nein, ein oder mehrere erforderliche Nodes sind derzeit getrennt und müssen wiederhergestellt werden.</p> <p>Hinweis: Diese Meldung wird nur für getrennte Gitterknoten angezeigt.</p>	Ein getrennter Grid-Node kann nicht stillgelegt werden, wenn ein oder mehrere erforderliche Nodes ebenfalls getrennt sind (z. B. ein Storage Node, der für das ADC-Quorum erforderlich ist).	<p>a. Überprüfen Sie die möglichen Meldungen zur Dekommission für alle nicht verbundenen Knoten.</p> <p>b. Ermitteln Sie, welche Nodes nicht stillgelegt werden können, da sie erforderlich sind.</p> <ul style="list-style-type: none"> ◦ Wenn der Status eines erforderlichen Knotens „Administrativ ausgefallen“ ist, stellen Sie den Knoten wieder in den Online-Modus. ◦ Wenn der Systemzustand eines erforderlichen Node Unbekannt ist, führen Sie einen Wiederherstellungsvorgang für den Node durch, um den erforderlichen Node wiederherzustellen.

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
Nein, Mitglied der HA-Gruppe(n): X. Bevor Sie diesen Node außer Betrieb nehmen können, müssen Sie ihn aus allen HA-Gruppen entfernen.	Sie können einen Admin-Node und einen Gateway-Node nicht stilllegen, wenn eine Node-Schnittstelle zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehört.	Bearbeiten Sie die HA-Gruppe, um die Schnittstelle des Node zu entfernen, oder entfernen Sie die gesamte HA-Gruppe. Siehe Anweisungen für " Administration von StorageGRID ".
Nein, Standort x erfordert mindestens n Storage Nodes mit ADC-Services.	Nur Speicher-Nodes. Sie können einen Speicher-Node nicht stilllegen, wenn nicht genügend Knoten am Standort verbleiben würden, um die ADC-Quorum-Anforderungen zu unterstützen.	Eine Erweiterung durchführen. Fügen Sie dem Standort einen neuen Speicherknoten hinzu, und geben Sie an, dass ein ADC-Dienst vorhanden sein soll. Siehe Informationen zum " ADC-Quorum ".

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
<p>Nein, mindestens ein Profil für das Erasure Coding benötigt mindestens n Storage Nodes. Wenn das Profil in einer ILM-Regel nicht verwendet wird, können Sie es deaktivieren.</p>	<p>Nur Speicher-Nodes. Sie können einen Speicher-Node nicht außer Betrieb nehmen, wenn für die vorhandenen Erasure Coding-Profile genügend Knoten vorhanden wären.</p> <p>Wenn beispielsweise ein Profil für das Erasure Coding 4+2 Erasure Coding vorhanden ist, müssen mindestens 6 Storage Nodes verbleiben.</p>	<p>Führen Sie für jedes betroffene Erasure Coding-Profil einen der folgenden Schritte aus, je nachdem, wie das Profil verwendet wird:</p> <ul style="list-style-type: none"> • In der aktiven ILM-Richtlinie verwendet: Eine Erweiterung durchführen. Fügen Sie genügend neue Storage-Nodes hinzu, um das Erasure Coding-Verfahren fortzusetzen. Siehe Anweisungen für "Erweitern Sie Ihr Raster". • Wird in einer ILM-Regel verwendet, aber nicht in der aktiven ILM-Richtlinie: Bearbeiten oder löschen Sie die Regel und deaktivieren Sie dann das Erasure Coding-Profil. • In keiner ILM-Regel verwendet: Deaktivieren Sie das Erasure Coding-Profil. <p>Hinweis: eine Fehlermeldung erscheint, wenn Sie versuchen, ein Erasure Coding-Profil zu deaktivieren und Objektdaten noch mit dem Profil verknüpft sind. Sie müssen möglicherweise mehrere Wochen warten, bevor Sie den Deaktivierungsprozess erneut versuchen.</p> <p>Erfahren Sie in den Anweisungen für, wie Sie ein Erasure Coding-Profil deaktivieren können "Objektmanagement mit ILM".</p>

4. Falls für den Knoten ein Stilllegen möglich ist, bestimmen Sie, welche Prozedur Sie durchführen müssen:

Wenn Ihr Grid Folgendes enthält:	Gehe zu...
Alle getrennten Grid-Nodes	"Die getrennten Grid-Nodes werden deaktiviert"
Nur verbundene Grid-Nodes	"Verbundene Grid-Nodes ausmustern"

Die getrennten Grid-Nodes werden deaktiviert

Möglicherweise müssen Sie einen Knoten außer Betrieb setzen, der derzeit nicht mit dem Grid verbunden ist (einen Node, dessen Status unbekannt oder administrativ ausgefallen ist).

Bevor Sie beginnen

- Sie verstehen die Anforderungen und "[Überlegungen für die Deaktivierung von Grid-Nodes](#)".
- Sie haben alle erforderlichen Elemente erhalten.
- Sie haben sichergestellt, dass keine Datenreparaturjobs aktiv sind. Siehe "[Prüfen Sie die Reparatur von Daten](#)".
- Sie haben bestätigt, dass die Wiederherstellung von Storage-Nodes an keiner Stelle im Grid ausgeführt wird. In diesem Fall müssen Sie warten, bis alle Cassandra-Rebuilds im Rahmen der Recovery abgeschlossen sind. Anschließend können Sie mit der Stilllegung fortfahren.
- Sie haben sichergestellt, dass andere Wartungsvorgänge während der Deaktivierung des Nodes nicht ausgeführt werden, es sei denn, der Vorgang zur Deaktivierung des Nodes wurde angehalten.
- Die Spalte **Decommission möglich** für den Knoten oder Knoten, die Sie außer Betrieb nehmen möchten, enthält ein grünes Häkchen.
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Sie können nicht verbundene Knoten identifizieren, indem Sie in der Spalte **Health** nach Unbekannt (blau) oder Administrativ Down (grau)-Symbolen suchen. Im Beispiel ist der Speicherknoten DC1-S4 getrennt; alle anderen Knoten sind verbunden.

Beachten Sie vor dem Stilllegen getrennter Nodes Folgendes:

- Dieses Verfahren dient in erster Linie zum Entfernen eines einzelnen nicht verbundenen Knotens. Wenn Ihr Grid mehrere getrennte Knoten enthält, muss die Software gleichzeitig ausmustern, wodurch das Potenzial für unerwartete Ergebnisse erhöht wird.



Seien Sie vorsichtig, wenn Sie mehrere getrennte Grid-Nodes gleichzeitig außer Betrieb nehmen, insbesondere wenn Sie mehrere getrennte Storage-Nodes auswählen.

- Wenn ein getrennter Knoten nicht entfernt werden kann (z. B. ein Speicher-Knoten, der für das ADC-Quorum erforderlich ist), kann kein anderer getrennter Knoten entfernt werden.

Beachten Sie vor dem Stilllegen eines nicht verbundenen **Storage Node** Folgendes

- Sie sollten einen getrennten Storage Node niemals außer Betrieb nehmen, es sei denn, Sie sind sicher, dass er nicht online gestellt oder wiederhergestellt werden kann.



Wenn Sie glauben, dass Objektdaten immer noch vom Node wiederhergestellt werden können, führen Sie dieses Verfahren nicht durch. Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, ob das Recovery von Nodes möglich ist.

- Wenn Sie mehrere getrennte Storage-Nodes außer Betrieb nehmen, kann es zu Datenverlusten kommen. Das System ist möglicherweise nicht in der Lage, Daten zu rekonstruieren, wenn nicht genügend Objektkopien, Fragmente mit Erasure-Coding-Verfahren oder Objekt-Metadaten verfügbar sind.



Wenn Sie mehr als einen getrennten Storage Node haben, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

- Wenn Sie einen getrennten Storage-Node außer Betrieb nehmen, startet StorageGRID am Ende des Stilllegungsvorgangs die Reparatur der Daten. Diese Jobs versuchen, die Objektdaten und Metadaten, die auf dem getrennten Node gespeichert waren, zu rekonstruieren.
- Wenn Sie einen getrennten Storage-Node ausmustern, wird der Vorgang der Ausmusterung relativ schnell abgeschlossen. Die Ausführung von Datenreparaturen kann jedoch Tage oder Wochen dauern und wird nicht durch die Außerbetriebnahme überwacht. Sie müssen diese Jobs manuell überwachen und nach Bedarf neu starten. Siehe "[Prüfen Sie die Reparatur von Daten](#)".
- Wenn Sie einen getrennten Storage-Node stilllegen, der die einzige Kopie eines Objekts enthält, geht das Objekt verloren. Die Datenrekonstruktionsaufgaben können Objekte nur rekonstruieren und wiederherstellen, wenn mindestens eine replizierte Kopie oder genug Fragmente mit Lösungscode auf aktuell verbundenen Storage-Nodes vorhanden sind.

Beachten Sie vor dem Stilllegen eines nicht verbundenen **Admin-Node** oder **Gateway-Node** Folgendes:

- Wenn Sie einen getrennten Admin-Node stilllegen, verlieren Sie die Audit-Protokolle von diesem Node. Diese Protokolle sollten jedoch auch im primären Admin-Node vorhanden sein.
- Sie können einen Gateway-Node sicher außer Betrieb setzen, während er getrennt ist.

Schritte

1. Versuchen Sie, getrennte Grid-Nodes wieder online zu bringen oder sie wiederherzustellen.

Anweisungen hierzu finden Sie in den Wiederherstellungsverfahren.

2. Wenn Sie einen nicht verbundenen Grid-Node nicht wiederherstellen können und ihn während der Trennung außer Betrieb nehmen möchten, aktivieren Sie das Kontrollkästchen für diesen Node.



Wenn Ihr Grid mehrere getrennte Knoten enthält, muss die Software gleichzeitig ausmustern, wodurch das Potenzial für unerwartete Ergebnisse erhöht wird.



Seien Sie vorsichtig, wenn Sie mehrere getrennte Grid-Nodes gleichzeitig stilllegen möchten, insbesondere wenn Sie mehrere getrennte Storage-Nodes auswählen. Wenn Sie mehr als einen getrennten Storage Node haben, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

3. Geben Sie die Provisionierungs-Passphrase ein.

Die Schaltfläche **Start Decommission** ist aktiviert.

4. Klicken Sie Auf **Start Decommission**.

Es wird eine Warnung angezeigt, die angibt, dass Sie einen nicht verbundenen Knoten ausgewählt haben und dass Objektdaten verloren gehen, wenn der Knoten die einzige Kopie eines Objekts hat.

⚠ Warning

The selected nodes are disconnected (health is Unknown or Administratively Down). If you continue and the node has the only copy of an object, the object will be lost when the node is removed.

The following grid nodes have been selected for decommissioning and will be permanently removed from the StorageGRID Webscale system.

DC1-S4

Do you want to continue?

Cancel

OK

5. Überprüfen Sie die Liste der Knoten, und klicken Sie auf **OK**.

Der Vorgang zur Deaktivierung wird gestartet und für jeden Node wird der Fortschritt angezeigt. Während des Verfahrens wird ein neues Wiederherstellungspaket mit der Änderung der Grid-Konfiguration generiert.

Decommission Nodes

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package page](#) to download it.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Name	Type	Progress	Stage
DC1-S4	Storage Node	<div style="width: 10%;"></div>	Prepare Task

Search

Pause Resume

6. Sobald das neue Wiederherstellungspaket verfügbar ist, klicken Sie auf den Link oder wählen Sie **WARTUNG > System > Wiederherstellungspaket**, um die Seite Wiederherstellungspaket aufzurufen. Laden Sie anschließend die herunter .zip Datei:

Siehe Anweisungen für "[Herunterladen des Wiederherstellungspakets](#)".



Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Grid wiederherstellen können, wenn während des Stillfalls etwas schief geht.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

7. Überwachen Sie die Seite Dekommission regelmäßig, um sicherzustellen, dass alle ausgewählten Knoten erfolgreich außer Betrieb gesetzt werden.

Storage-Nodes können Tage oder Wochen ausmustern. Wenn alle Aufgaben abgeschlossen sind, wird die Liste der Knotenauswahl 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 Nodes im Rahmen der Stilllegung automatisch heruntergefahren wurden, entfernen Sie alle verbleibenden Virtual Machines oder anderen Ressourcen, die dem ausgemusterten Node zugeordnet sind.



Führen Sie diesen Schritt erst aus, wenn die Nodes automatisch heruntergefahren wurden.

9. Wenn Sie einen Storage Node außer Betrieb nehmen, überwachen Sie den Status der Reparatur-Jobs mit **replizierten Daten** und **Erase-codierten (EC) Daten**, die während des Stilllegungsprozesses automatisch gestartet werden.

Replizierte Daten

- Um einen geschätzten Fertigstellungsgrad für die replizierte Reparatur zu erhalten, fügen Sie die hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES > Storage Node wird repariert > ILM**.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle 0** Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid > Storage Node wird repariert > LDR > Data Store**.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra-Inkonsistenzen sind möglicherweise vorhanden, und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA)**: Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM)**: Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:
 - Wählen Sie **SUPPORT > Tools > Metrics**, um die geschätzte Zeit bis zum Abschluss und den Fertigstellungsgrad für den aktuellen Job anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
 - Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data`

Betriebliche Gründe:

```
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 enthält Informationen, einschließlich `repair ID`, für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Nachdem Sie fertig sind

Sobald die getrennten Nodes außer Betrieb genommen und alle Reparatur-Jobs abgeschlossen sind, können Sie alle verbundenen Grid-Nodes je nach Bedarf ausmustern.

Führen Sie anschließend die folgenden Schritte aus, nachdem Sie den Vorgang zur Deaktivierung abgeschlossen haben:

- Stellen Sie sicher, dass die Laufwerke des ausgemusterten Grid-Node sauber gelöscht werden. Verwenden Sie ein handelsübliches Datenwischwerkzeug oder einen Dienst, um die Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn Sie einen Appliance-Node deaktiviert haben und die Daten auf der Appliance mithilfe der Node-Verschlüsselung geschützt wurden, löschen Sie die Konfiguration des Verschlüsselungsmanagement-Servers (Clear KMS) mithilfe des StorageGRID Appliance Installer. Wenn Sie die Appliance einem anderen Grid hinzufügen möchten, müssen Sie die KMS-Konfiguration löschen. Anweisungen hierzu finden Sie unter ["Überwachung der Node-Verschlüsselung im Wartungsmodus"](#).

Verwandte Informationen

["Verfahren zur Recovery von Grid-Nodes"](#)

Verbundene Grid-Nodes ausmustern

Sie können Nodes, die mit dem Grid verbunden sind, außer Betrieb nehmen und dauerhaft entfernen.

Bevor Sie beginnen

- Sie verstehen die Anforderungen und ["Überlegungen für die Deaktivierung von Grid-Nodes"](#).
- Sie haben alle benötigten Materialien zusammengestellt.

- Sie haben sichergestellt, dass keine Datenreparaturjobs aktiv sind.
- Sie haben bestätigt, dass die Wiederherstellung von Storage-Nodes an keiner Stelle im Grid ausgeführt wird. Wenn dies der Fall ist, warten Sie, bis eine Cassandra-Neuerstellung als Teil der Wiederherstellung abgeschlossen ist. Anschließend können Sie mit der Stilllegung fortfahren.
- Sie haben sichergestellt, dass andere Wartungsvorgänge während der Deaktivierung des Nodes nicht ausgeführt werden, es sei denn, der Vorgang zur Deaktivierung des Nodes wurde angehalten.
- Sie haben die Provisionierungs-Passphrase.
- Die Grid-Nodes sind verbunden.
- Die Spalte **Decommission possible** für den Knoten oder Knoten, den Sie stilllegen möchten, enthält ein grünes Häkchen.



Die Stilllegung wird nicht gestartet, wenn ein oder mehrere Volumes offline (unmounted) sind oder online (gemountet) sind, sondern sich in einem Fehlerzustand befinden.



Wenn ein oder mehrere Volumes offline geschaltet werden, während eine Deaktivierung durchgeführt wird, wird die Deaktivierung durchgeführt, nachdem diese Volumes wieder online geschaltet wurden.

- Alle Grid-Nodes weisen den normalen Zustand (grün) auf . Wenn eines dieser Symbole in der Spalte **Gesundheit** angezeigt wird, müssen Sie versuchen, das Problem zu lösen:

Symbol	Farbe	Schweregrad
	Gelb	Hinweis
	Hellorange	Gering
	Dunkelorange	Major
	Rot	Kritisch

- Wenn Sie zuvor einen getrennten Speicherknoten außer Betrieb genommen haben, wurden die Reparaturaufträge erfolgreich abgeschlossen. Siehe "[Prüfen Sie die Reparatur von Daten](#)".



Entfernen Sie die virtuelle Maschine oder andere Ressourcen eines Grid-Node erst, wenn Sie in diesem Verfahren dazu aufgefordert werden.

Schritte

1. Aktivieren Sie auf der Seite Decommission Nodes das Kontrollkästchen für jeden Rasterknoten, den Sie stilllegen möchten.
2. Geben Sie die Provisionierungs-Passphrase ein.

Die Schaltfläche **Start Decommission** ist aktiviert.

3. Klicken Sie Auf **Start Decommission**.
4. Überprüfen Sie die Liste der Knoten im Bestätigungsdialog und klicken Sie auf **OK**.

Daraufhin wird der Vorgang zum Stilllegen des Node gestartet, und der Fortschritt wird für jeden Node angezeigt. Während des Verfahrens wird ein neues Wiederherstellungspaket generiert, um die Änderung der Grid-Konfiguration anzuzeigen.

Decommission Nodes

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package page](#) to download it.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Name	Type	Progress	Stage
DC1-S5	Storage Node	<div style="width: 10%;"></div>	Prepare Task



Nehmen Sie einen Speicher-Node nicht offline, nachdem der Ausmusterung-Vorgang gestartet wurde. Wenn Sie den Status ändern, werden einige Inhalte möglicherweise nicht an andere Orte kopiert.

5. Sobald das neue Wiederherstellungspaket verfügbar ist, klicken Sie auf den Link oder wählen Sie **WARTUNG > System > Wiederherstellungspaket**, um die Seite Wiederherstellungspaket aufzurufen. Laden Sie anschließend die herunter .zip Datei:

Siehe Anweisungen für "[Herunterladen des Wiederherstellungspakets](#)".



Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Grid wiederherstellen können, wenn während des Stillfalls etwas schief geht.

6. Überwachen Sie die Seite Decommission Nodes regelmäßig, um sicherzustellen, dass alle ausgewählten Knoten erfolgreich deaktiviert wurden.

Storage-Nodes können Tage oder Wochen ausmustern. Wenn alle Aufgaben abgeschlossen sind, wird die Liste der Knotenauswahl mit einer Erfolgsmeldung erneut angezeigt.

7. Befolgen Sie den entsprechenden Schritt für Ihre Plattform. Beispiel:
 - **Linux:** Möglicherweise möchten Sie die Volumes trennen und die Knoten-Konfigurationsdateien löschen, die Sie während der Installation erstellt haben.
 - **VMware:** Sie können die vCenter "Delete from Disk" Option verwenden, um die virtuelle Maschine zu löschen. Möglicherweise müssen Sie auch alle Datenfestplatten löschen, die unabhängig von der virtuellen Maschine sind.
 - **StorageGRID-Appliance:** Der Appliance-Knoten wird automatisch in einen nicht bereitgestellten Zustand zurückgesetzt, in dem Sie auf das Installationsprogramm der StorageGRID-Appliance zugreifen können. Sie können das Gerät ausschalten oder es einem anderen StorageGRID-System

hinzufügen.

Führen Sie die folgenden Schritte aus, nachdem Sie den Vorgang zur Deaktivierung des Node abgeschlossen haben:

- Stellen Sie sicher, dass die Laufwerke des ausgemusterten Grid-Node sauber gelöscht werden. Verwenden Sie ein handelsübliches Datenwischwerkzeug oder einen Dienst, um die Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn Sie einen Appliance-Node stillgelegt haben und die Daten auf der Appliance durch Knotenverschlüsselung geschützt wurden, verwenden Sie den StorageGRID-Appliance-Installer, um die Konfiguration des Schlüsselmanagement-Servers zu löschen (KMS löschen). Sie müssen die KMS-Konfiguration löschen, wenn Sie die Appliance einem anderen Grid hinzufügen möchten. Anweisungen hierzu finden Sie unter "[Überwachung der Node-Verschlüsselung im Wartungsmodus](#)".

Verwandte Informationen

["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)

Anhalten und Fortsetzen des Stilllegen-Prozesses für Storage-Nodes

Wenn Sie einen zweiten Wartungsvorgang durchführen müssen, können Sie das Verfahren zur Deaktivierung eines Storage Nodes während bestimmter Phasen unterbrechen. Nachdem das andere Verfahren abgeschlossen ist, können Sie die Stilllegung fortsetzen.



Die Schaltfläche **Pause** ist nur aktiviert, wenn die ILM-Bewertung oder die mit Erasure Coding versehenen Phasen der Datenauswertung erreicht sind. Die ILM-Evaluierung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Berechtigung **Wartung** oder **Stammzugriff**.

Schritte

1. Wählen Sie **MAINTENANCE > Tasks > Decommission**.

Die Seite Decommission wird angezeigt.

2. Wählen Sie **Decommission Nodes**.

Die Seite Decommission Nodes wird angezeigt. Wenn die Deaktivierung eine der folgenden Stufen erreicht, ist die Schaltfläche **Pause** aktiviert.

- ILM-Evaluierung
- Erasure-codierte Daten werden stillgelegt

3. Wählen Sie **Pause**, um den Vorgang zu unterbrechen.

Die aktuelle Phase wird angehalten, und die Schaltfläche **Fortsetzen** ist aktiviert.

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

 Decommissioning procedure has been paused. Click 'Resume' to resume the procedure.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Name	Type	Progress	Stage
DC1-S5	Storage Node	<div style="width: 50%; background-color: orange;"></div>	Evaluating ILM

- Nachdem der andere Wartungsvorgang abgeschlossen ist, wählen Sie **Fortsetzen** aus, um mit der Stilllegung fortzufahren.

Fehlerbehebung bei der Ausmusterung von Nodes

Wenn der Node aufgrund eines Fehlers deaktiviert wird, können Sie spezifische Schritte zum Beheben des Problems durchführen.

Bevor Sie beginnen

Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

Wenn Sie den stillgelegten Grid-Node herunterfahren, wird die Aufgabe angehalten, bis der Grid-Node neu gestartet wird. Der Grid-Node muss sich online sein.

Schritte

- Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- Erweitern Sie in der Struktur Grid Topology jeden Storage Node-Eintrag und überprüfen Sie, ob die DDS- und LDR-Dienste online sind.

Um eine Ausmusterung von Storage-Nodes durchzuführen, müssen alle Nodes und alle Services zu Beginn der Deaktivierung eines Online-Nodes/Standorts in einem ordnungsgemäßen Zustand sein.

- Um die aktiven Grid-Aufgaben anzuzeigen, wählen Sie **Primary Admin Node > CMN > Grid Tasks > Übersicht**.
- Überprüfen Sie den Status der Task „Stilllegen“.
 - Wenn der Status der Aufgabe des Decommissioning Grid auf ein Problem beim Speichern von Grid-Task-Bundles hinweist, wählen Sie **primary Admin Node > CMN > Events > Übersicht** aus
 - Prüfen Sie die Anzahl der verfügbaren Audit-Relais.

Wenn das Attribut Available Audit Relay ein oder größer ist, ist der CMN-Dienst mit mindestens einem ADC-Dienst verbunden. ADC-Dienste fungieren als Überwachungsrelais.

Der CMN-Dienst muss mit mindestens einem ADC-Dienst verbunden sein, und eine Mehrheit (50 Prozent

plus einer) der ADC-Dienste des StorageGRID-Systems muss verfügbar sein, damit eine Grid-Aufgabe von einer Phase der Stilllegung in eine andere und zum Abschluss verschoben werden kann.

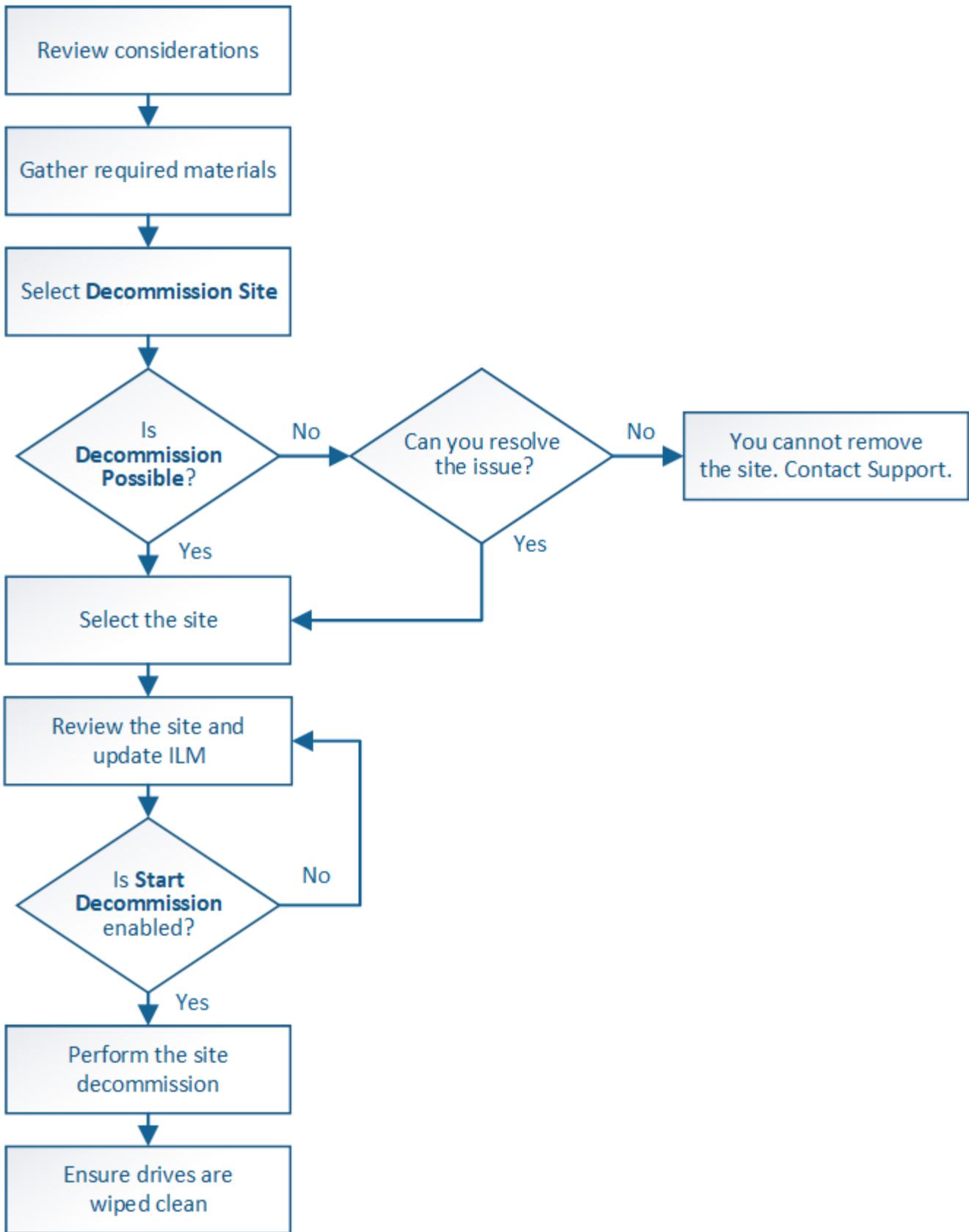
- a. Wenn der CMN-Dienst nicht mit genügend ADC-Diensten verbunden ist, stellen Sie sicher, dass Storage-Nodes online sind, und überprüfen Sie die Netzwerkverbindung zwischen dem primären Admin-Node und Storage-Nodes.

Deaktivierung der Website

Website-Deaktivierung: Übersicht

Möglicherweise müssen Sie einen Datacenter-Standort aus dem StorageGRID System entfernen. Um eine Website zu entfernen, müssen Sie sie ausmustern.

Das Flussdiagramm zeigt die Schritte für die Außerbetriebnahme eines Standorts auf hoher Ebene.



Überlegungen zum Entfernen eines Standorts

Bevor Sie die Website wieder entfernen, müssen Sie zunächst die entsprechenden Überlegungen überprüfen.

Was geschieht, wenn Sie eine Website ausmustern

Durch die Stilllegung einer Website StorageGRID werden alle Nodes an der Website und der Standort selbst endgültig vom StorageGRID System entfernt.

Nach Abschluss der Deaktivierung der Website:

- StorageGRID kann nicht mehr zum Anzeigen und Zugreifen auf den Standort oder auf einen der Nodes am Standort verwendet werden.
- Sie können keine Speicherpools oder Profile für das Erasure Coding, die auf den Standort verweisen, mehr verwenden. Wenn StorageGRID einen Standort stilllegt, werden diese Storage-Pools automatisch entfernt und diese Profile zum Erasure Coding deaktiviert.

Unterschiede zwischen dem angeschlossenen Standort und dem Verfahren zur Deaktivierung des Standorts

Im Rahmen der Deaktivierung einer Website können Sie eine Site entfernen, in der alle Nodes mit StorageGRID verbunden sind (die als Deaktivierung verbundenen Site bezeichnet wird), oder eine Site entfernen, in der alle Nodes von StorageGRID getrennt sind (die so genannte Deaktivierung einer getrennten Site wird als deaktiviert). Bevor Sie beginnen, müssen Sie die Unterschiede zwischen diesen Verfahren verstehen.



Wenn ein Standort eine Mischung aus verbundenen (✔) und nicht verbundene Knoten (☾) Oder (⊖), Sie müssen alle Offline-Knoten wieder online bringen.

- Durch eine Deaktivierung einer verbundenen Website können Sie einen betrieblichen Standort aus dem StorageGRID System entfernen. Beispielsweise können Sie eine verbundene Website ausmustern, um eine funktionierende, aber nicht mehr benötigte Website zu entfernen.
- Wenn StorageGRID einen verbundenen Standort entfernt, wird ILM für das Management der Objektdaten am Standort verwendet. Bevor Sie eine verbundene Site außer Betrieb nehmen können, müssen Sie die Site von allen ILM-Regeln entfernen und eine neue ILM-Richtlinie aktivieren. Die ILM-Prozesse zur Migration von Objektdaten und die internen Prozesse zur Entfernung eines Standorts können gleichzeitig durchgeführt werden. Es empfiehlt sich jedoch, die ILM-Schritte zu schließen, bevor Sie den tatsächlichen Außerbetriebnahme starten.
- Bei einer getrennten Deaktivierung der Website können Sie fehlerhafte Standorte aus dem StorageGRID System entfernen. So können Sie beispielsweise eine abgelöste Außerbetriebnahme des Standorts durchführen, um einen Standort zu entfernen, der durch einen Brand oder eine Überschwemmung zerstört wurde.

Wenn StorageGRID eine getrennte Site entfernt, werden alle Nodes als nicht wiederherstellbar erachtet und nicht versucht, Daten zu erhalten. Bevor Sie eine getrennte Site jedoch außer Betrieb nehmen können, müssen Sie die Website jedoch von allen ILM-Regeln entfernen und eine neue ILM-Richtlinie aktivieren.



Bevor Sie eine Deaktivierung des Standorts durchführen, müssen Sie sich an Ihren NetApp Ansprechpartner wenden. NetApp überprüft Ihre Anforderungen, bevor Sie alle Schritte im Decommission Site Wizard aktivieren. Sie sollten keinen Versuch Unternehmen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie der Meinung sind, dass eine Wiederherstellung der Site oder die Wiederherstellung von Objektdaten von der Site möglich wäre.

Allgemeine Anforderungen für das Entfernen eines verbundenen oder getrennten Standorts

Bevor Sie einen angeschlossenen oder getrennten Standort entfernen, müssen Sie die folgenden Anforderungen erfüllen:

- Sie können eine Site, die den primären Admin-Node enthält, nicht stilllegen.
- Sie können eine Site, die einen Archivknoten enthält, nicht stilllegen.
- Sie können einen Standort nicht ausmustern, wenn einer der Nodes über eine Schnittstelle verfügt, die zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehört. Sie müssen entweder die HA-Gruppe bearbeiten, um die Schnittstelle des Node zu entfernen, oder die gesamte HA-Gruppe entfernen.
- Sie können eine Site nicht stilllegen, wenn sie eine Mischung aus verbundenen (enthält  Und getrennt ( Oder ) Knoten.
- Sie können einen Standort nicht stilllegen, wenn ein Knoten an einem anderen Standort getrennt ist ( Oder )
- Sie können das Verfahren zur Deaktivierung der Website nicht starten, wenn gerade ein ec-Node-Reparaturvorgang durchgeführt wird. Siehe "[Prüfen Sie die Reparatur von Daten](#)" Zur Nachverfolgung von Reparaturen mit Erasure-Coding-Daten.
- Während die Deaktivierung der Website läuft:
 - Sie können keine ILM-Regeln erstellen, die sich auf den deaktivierten Standort beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf den Standort zu verweisen.
 - Sie können keine anderen Wartungsverfahren wie Erweiterungen oder Upgrades durchführen.



Wenn Sie während der Stilllegung einer verbundenen Website einen weiteren Wartungsvorgang durchführen müssen, können Sie dies auch tun "[Halten Sie das Verfahren an, während die Speicherknoten entfernt werden](#)". Die Schaltfläche **Pause** ist nur aktiviert, wenn die ILM-Bewertung oder die mit Erasure Coding versehenen Phasen der Datenauswertung erreicht sind. Die ILM-Evaluierung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt. Nach Abschluss des zweiten Wartungsverfahrens können Sie die Außerbetriebnahme fortsetzen.

- Falls Nodes nach dem Starten der Deaktivierung der Website wiederhergestellt werden müssen, müssen Sie den Support kontaktieren.
- Sie können nicht mehr als einen Standort gleichzeitig stilllegen.
- Wenn die Site einen oder mehrere Admin-Nodes enthält und Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, müssen Sie alle Vertrauensstellen der Vertrauensstelle für die Site von Active Directory Federation Services (AD FS) entfernen.

Anforderungen für Information Lifecycle Management (ILM)

Beim Entfernen eines Standorts müssen Sie Ihre ILM-Konfiguration aktualisieren. Der Assistent für die Decommission Site führt Sie durch eine Reihe von erforderlichen Schritten, um Folgendes sicherzustellen:

- Die ILM-Richtlinie für den Standort wird nicht genutzt. In diesem Fall müssen Sie eine neue ILM-Richtlinie mit neuen ILM-Regeln erstellen und aktivieren.
- Es gibt keine vorgeschlagene ILM-Richtlinie. Wenn Sie über eine vorgeschlagene Richtlinie verfügen, müssen Sie diese löschen.

- Keine ILM-Regeln beziehen sich auf den Standort, auch wenn diese Regeln in der aktiven oder vorgeschlagenen Richtlinie nicht verwendet werden. Sie müssen alle Regeln, die sich auf die Website beziehen, löschen oder bearbeiten.

Wenn StorageGRID die Website dekomprimiert, werden alle ungenutzten Erasure Coding-Profile, die auf diesen Standort verweisen, automatisch deaktiviert und alle nicht verwendeten Storage-Pools, die auf den Standort verweisen, werden automatisch gelöscht. Wenn der Speicherpool Alle Speicherknoten vorhanden ist (StorageGRID 11.6 und früher), wird er entfernt, da er alle Standorte verwendet.



Bevor Sie einen Standort entfernen können, müssen Sie möglicherweise neue ILM-Regeln erstellen und eine neue ILM-Richtlinie aktivieren. Diese Anweisungen setzen voraus, dass Sie über gute Kenntnisse der Funktionsweise von ILM verfügen und mit der Erstellung von Storage-Pools, Profilen zur Fehlerkorrektur, ILM-Regeln sowie der Simulation und Aktivierung einer ILM-Richtlinie vertraut sind. Siehe "[Objektmanagement mit ILM](#)".

Überlegungen zu den Objektdaten an einem angeschlossenen Standort

Wenn Sie eine verbundene Site außer Betrieb nehmen, müssen Sie beim Erstellen neuer ILM-Regeln und einer neuen ILM-Richtlinie festlegen, welche Daten an der Website gespeichert werden. Sie können entweder oder beide der folgenden Aktionen ausführen:

- Verschieben Sie Objektdaten vom ausgewählten Standort zu einem oder mehreren anderen Standorten in der Tabelle.

Beispiel für das Verschieben von Daten: Angenommen, Sie möchten eine Website in Raleigh ausmustern, weil Sie eine neue Website in Sunnyvale hinzugefügt haben. In diesem Beispiel möchten Sie alle Objektdaten vom alten Standort auf den neuen Standort verschieben. Bevor Sie Ihre ILM-Regeln und ILM-Richtlinie aktualisieren, müssen Sie die Kapazität an beiden Standorten prüfen. Sie müssen sicherstellen, dass der Standort in Sunnyvale über genügend Kapazität für die Objektdaten vom Standort Raleigh verfügt und dass im Rahmen eines zukünftigen Wachstums in Sunnyvale ausreichend Kapazität zur Verfügung steht.



Um sicherzustellen, dass eine ausreichende Kapazität verfügbar ist, müssen Sie dies möglicherweise tun "[Erweitern Sie Ihr Raster](#)" Indem Sie Speicher-Volumes oder Speicher-Nodes zu einem vorhandenen Standort hinzufügen oder einen neuen Standort hinzufügen, bevor Sie diesen Vorgang durchführen.

- Löschen von Objektkopien vom ausgewählten Standort.

Beispiel für das Löschen von Daten: Angenommen, Sie verwenden derzeit eine ILM-Regel mit 3 Kopien, um Objektdaten auf drei Standorten zu replizieren. Bevor Sie einen Standort außer Betrieb nehmen, können Sie eine äquivalente ILM-Regel mit zwei Kopien erstellen, um Daten an nur zwei Standorten zu speichern. Wenn Sie eine neue ILM-Richtlinie aktivieren, die die Regel mit zwei Kopien verwendet, löscht StorageGRID die Kopien vom dritten Standort, da diese die ILM-Anforderungen nicht mehr erfüllen. Die Objektdaten werden jedoch weiterhin gesichert und die Kapazität der beiden verbleibenden Standorte bleibt gleich.



Erstellen Sie niemals eine ILM-Regel für eine einzelne Kopie, um die Entfernung eines Standorts aufzunehmen. Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Zusätzliche Anforderungen für die Deaktivierung einer verbundenen Website

Bevor StorageGRID einen verbundenen Standort entfernen kann, müssen Sie Folgendes sicherstellen:

- Alle Knoten in Ihrem StorageGRID-System müssen über einen Verbindungsstatus von **Connected** (verfügen ); die Knoten können jedoch aktive Warnmeldungen haben.



Wenn ein oder mehrere Knoten getrennt werden, können Sie die Schritte 1-4 des Assistenten zum Decommission Site ausführen. Sie können jedoch Schritt 5 des Assistenten nicht ausführen, der den Stilllegungsvorgang startet, es sei denn, alle Nodes sind verbunden.

- Wenn der Standort, den Sie entfernen möchten, einen Gateway-Node oder einen Admin-Node enthält, der für den Lastausgleich verwendet wird, müssen Sie dies möglicherweise tun **"Erweitern Sie Ihr Raster"** Um einen gleichwertigen neuen Node an einem anderen Standort hinzuzufügen. Es muss sichergestellt sein, dass Clients eine Verbindung zum Ersatz-Node herstellen können, bevor der Standort ausgemastert wird.
- Wenn der Standort, den Sie entfernen möchten, einen Gateway-Node oder Admin-Knoten enthält, die sich in einer HA-Gruppe befinden, können Sie die Schritte 1-4 des Assistenten zur Decommission Site ausführen. Sie können jedoch Schritt 5 des Assistenten nicht ausführen. Dieser startet den Stilllegungsvorgang, bis Sie diese Nodes aus allen HA-Gruppen entfernen. Wenn bestehende Clients mit einer HA-Gruppe verbunden sind, die Nodes vom Standort enthält, müssen Sie sicherstellen, dass nach dem Entfernen des Standorts die Verbindung zu StorageGRID fortgesetzt werden kann.
- Wenn Clients direkt mit Storage Nodes an dem Standort verbunden sind, den Sie entfernen möchten, müssen Sie sicherstellen, dass sie eine Verbindung zu Storage Nodes an anderen Standorten herstellen können, bevor Sie den Vorgang zur Deaktivierung des Standorts starten.
- Sie müssen auf den übrigen Standorten ausreichend Speicherplatz für alle Objektdaten bereitstellen, die aufgrund von Änderungen an der aktiven ILM-Richtlinie verschoben werden. In einigen Fällen müssen Sie dies möglicherweise tun **"Erweitern Sie Ihr Raster"** Indem Sie Storage-Nodes, Storage-Volumes oder neue Standorte hinzufügen, bevor Sie die Deaktivierung eines verbundenen Standorts abschließen können.
- Sie müssen genügend Zeit haben, bis der Stilllegen abgeschlossen ist. Die ILM-Prozesse von StorageGRID dauern möglicherweise Tage, Wochen oder sogar Monate, um Objektdaten vom Standort zu verschieben oder zu löschen, bevor der Standort stillgelegt werden kann.



Das Verschieben oder Löschen von Objektdaten von einem Standort kann Tage, Wochen oder sogar Monate dauern, abhängig von der Datenmenge am Standort, der Systemlast, den Netzwerklatenzen und der Art der erforderlichen ILM-Änderungen.

- Wenn möglich, sollten Sie die Schritte 1-4 des Decommission Site-Assistenten so früh wie möglich abschließen. Die Deaktivierung erfolgt schneller und mit weniger Unterbrechungen und Leistungseinflüssen, wenn Sie zulassen, dass Daten von der Website verschoben werden, bevor Sie die tatsächliche Deaktivierung starten (indem Sie in Schritt 5 des Assistenten **Start Decommission** wählen).

Zusätzliche Anforderungen für die Deaktivierung eines getrennten Standorts

Bevor StorageGRID eine getrennte Site entfernen kann, müssen Sie Folgendes sicherstellen:

- Sie haben sich an Ihren NetApp Ansprechpartner wenden. NetApp überprüft Ihre Anforderungen, bevor Sie alle Schritte im Decommission Site Wizard aktivieren.



Sie sollten keinen Versuch Unternehmen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie der Meinung sind, dass eine Wiederherstellung der Site oder die Wiederherstellung von Objektdaten von der Site möglich wäre. Siehe "[Durchführen der Standortwiederherstellung durch den technischen Support](#)".

- Alle Nodes am Standort müssen einen Verbindungsstatus von einer der folgenden aufweisen:
 - * Unbekannt* (): Aus einem unbekanntem Grund wird ein Knoten getrennt oder Dienste auf dem Knoten sind unerwartet ausgefallen. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren.
 - **Administrativ Down** (): Der Knoten ist aus einem erwarteten Grund nicht mit dem Raster verbunden. Beispielsweise wurde der Node oder die Services auf dem Node ordnungsgemäß heruntergefahren.
- Alle Knoten an allen anderen Standorten müssen über einen Verbindungsstatus von **Connected** (); aber diese anderen Knoten können aktive Warnmeldungen haben.
- Sie müssen wissen, dass Sie mit StorageGRID keine Objektdaten mehr anzeigen oder abrufen können, die auf der Site gespeichert wurden. Wenn StorageGRID dieses Verfahren durchführt, wird nicht versucht, Daten vom getrennten Standort zu bewahren.



Wenn Ihre ILM-Regeln und -Richtlinien zum Schutz vor dem Verlust eines einzelnen Standorts ausgelegt wurden, sind noch Kopien der Objekte auf den übrigen Standorten vorhanden.

- Sie müssen verstehen, dass das Objekt verloren geht und nicht abgerufen werden kann, wenn die Site die einzige Kopie eines Objekts enthielt.

Überlegungen zu Konsistenzkontrollen beim Entfernen eines Standorts

Die Konsistenzstufe für einen S3-Bucket oder Swift-Container bestimmt, ob StorageGRID Objektmetadaten vollständig auf alle Nodes und Standorte repliziert, bevor einem Client mitgeteilt wird, dass die Objektaufnahme erfolgreich war. Konsistenzkontrollen bieten ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg.

Wenn StorageGRID einen Standort entfernt, muss es sicherstellen, dass keine Daten auf den entfernten Standort geschrieben werden. Daher wird das Konsistenzlevel vorübergehend für jeden Bucket oder Container überschrieben. Nach dem Starten der Website-Außerbetriebnahme verwendet StorageGRID vorübergehend eine hohe Standort-Konsistenz, um zu verhindern, dass Objekt-Metadaten auf die Website geschrieben werden.

Aufgrund dieser vorübergehenden Überschreibung ist es nicht bekannt, dass alle während der Außerbetriebnahme eines Standorts laufenden Client-Schreibvorgänge, Updates und Löschvorgänge fehlschlagen können, wenn auf den verbleibenden Standorten nicht mehr mehrere Nodes verfügbar sind.

Sammeln Sie die erforderlichen Materialien

Bevor Sie eine Website ausmustern, sind die folgenden Unterlagen erforderlich.

Element	Hinweise
Wiederherstellungspaket .zip Datei	Sie müssen das neueste Wiederherstellungspaket herunterladen .zip Datei (<code>sgws-recovery-package-id-revision.zip</code>). Sie können die Recovery Package-Datei verwenden, um das System wiederherzustellen, wenn ein Fehler auftritt. "Laden Sie das Recovery Package herunter"
Passwords.txt Datei	Diese Datei enthält die Passwörter, die für den Zugriff auf Grid-Knoten in der Befehlszeile erforderlich sind und im Wiederherstellungspaket enthalten sind.
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im Passwords.txt Datei:
Beschreibung der Topologie des StorageGRID Systems vor der Stilllegung	Falls verfügbar, finden Sie eine Dokumentation, die die aktuelle Topologie des Systems beschreibt.

Verwandte Informationen

["Anforderungen an einen Webbrowser"](#)

Schritt 1: Standort Auswählen

Um zu bestimmen, ob eine Site deaktiviert werden kann, öffnen Sie zunächst den Assistenten zur Deaktivierung der Site.

Bevor Sie beginnen

- Sie haben alle erforderlichen Materialien erhalten.
- Sie haben die Überlegungen zum Entfernen eines Standorts überprüft.
- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie verfügen über die Root-Zugriffsberechtigung oder die Wartungs- und ILM-Berechtigungen.

Schritte

1. Wählen Sie **MAINTENANCE > Tasks > Decommission**.
2. Wählen Sie **Decommission Site**.

Schritt 1 (Standort auswählen) des Assistenten für die Dekommission-Site wird angezeigt. Dieser Schritt enthält eine alphabetische Liste der Sites in Ihrem StorageGRID-System.

Decommission Site

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

Site Name	Used Storage Capacity	Decommission Possible
<input type="radio"/> Raleigh	3.93 MB	
<input type="radio"/> Sunnyvale	3.97 MB	
<input type="radio"/> Vancouver	3.90 MB	No. This site contains the primary Admin Node.

[Next](#)

3. Zeigen Sie die Werte in der Spalte **verwendete Storage-Kapazität** an, um festzustellen, wie viel Storage derzeit für Objektdaten an den einzelnen Standorten verwendet wird.

Die genutzte Storage-Kapazität ist eine Schätzung. Wenn Knoten offline sind, ist die verwendete Speicherkapazität der letzte bekannte Wert für den Standort.

- Um eine zusammenhängende Website außer Betrieb zu nehmen, gibt dieser Wert an, wie viele Objektdaten zu anderen Standorten verschoben oder durch ILM gelöscht werden müssen, bevor Sie diese Website zur sicheren Deaktivierung verwenden können.
- Im Falle einer Deaktivierung einer Website stellt dieser Wert dar, auf welchen Anteil der Datenspeicher Ihres Systems beim Deaktivierung dieser Website nicht mehr zugegriffen werden kann.



Falls Ihre ILM-Richtlinie zum Schutz vor dem Verlust eines einzelnen Standorts ausgelegt wurde, sollten weiterhin Kopien der Objektdaten auf den übrigen Standorten vorhanden sein.

4. Prüfen Sie die Gründe in der Spalte **Dekommission möglich**, um festzustellen, welche Standorte derzeit außer Betrieb genommen werden können.



Wenn es mehr als einen Grund gibt, warum ein Standort nicht stillgelegt werden kann, wird der kritischsten Grund angezeigt.

Möglichen Grund einer Deaktivierung	Beschreibung	Nächster Schritt
Grünes Häkchen ()	Sie können diese Website außer Betrieb nehmen.	Gehen Sie zu Im nächsten Schritt .

Möglichen Grund einer Deaktivierung	Beschreibung	Nächster Schritt
Nein Dieser Standort enthält den primären Admin-Knoten.	Sie können einen Standort, der den primären Admin-Node enthält, nicht stilllegen.	Keine. Sie können diesen Vorgang nicht ausführen.
Nein Diese Site enthält mindestens einen Archiv-Knoten.	Sie können eine Site, die einen Archivknoten enthält, nicht stilllegen.	Keine. Sie können diesen Vorgang nicht ausführen.
Nein Alle Knoten an diesem Standort werden getrennt. Wenden Sie sich an Ihren NetApp Account-Ansprechpartner.	Sie können eine verbundene Website nur dann stilllegen, wenn jeder Knoten im Standort verbunden ist (✓).	Um eine getrennte Website außer Betrieb zu nehmen, müssen Sie sich an Ihren NetApp Ansprechpartner wenden. Dieser überprüft Ihre Anforderungen und aktiviert den Rest des Assistenten zur Decommission Site. WICHTIG: Nehmen Sie niemals Online-Knoten offline, so dass Sie eine Seite entfernen können. Sie verlieren Daten.

Das Beispiel zeigt ein StorageGRID System mit drei Standorten. Das grüne Häkchen (✓) Für die Raleigh und Sunnyvale Seiten bedeutet, dass Sie diese Websites außer Betrieb nehmen können. Sie können die Vancouver-Website jedoch nicht stilllegen, da sie den primären Admin-Knoten enthält.

1. Wenn eine Deaktivierung möglich ist, aktivieren Sie das Optionsfeld für die Website.

Die Schaltfläche **Weiter** ist aktiviert.

2. Wählen Sie **Weiter**.

Schritt 2 (Details anzeigen) wird angezeigt.

Schritt 2: Details Anzeigen

Ab Schritt 2 (Details anzeigen) des Assistenten für die Decommission-Site können Sie überprüfen, welche Knoten auf der Site enthalten sind, sehen, wie viel Speicherplatz auf den einzelnen Speicherknoten verwendet wurde, und bewerten, wie viel freier Speicherplatz auf den anderen Standorten in Ihrem Raster verfügbar ist.

Bevor Sie beginnen

Bevor Sie einen Standort außer Betrieb nehmen, müssen Sie überprüfen, wie viele Objektdaten am Standort vorhanden sind.

- Wenn Sie eine verbundene Website ausmustern, müssen Sie vor der Aktualisierung des ILM die derzeit vorhandene Objektdaten an der Website kennen. Basierend auf den Kapazitäten des Standorts und den Datensicherungsanforderungen können Sie neue ILM-Regeln erstellen, um Daten an andere Standorte zu

verschieben oder Objektdaten vom Standort zu löschen.

- Führen Sie ggf. erforderliche Erweiterungen für Storage-Nodes durch, bevor Sie den Vorgang zur Deaktivierung nach Möglichkeit starten.
- Wenn Sie eine nicht verbundene Website deaktivieren, müssen Sie verstehen, wie viele Objektdaten dauerhaft zugänglich werden, wenn Sie die Website entfernen.

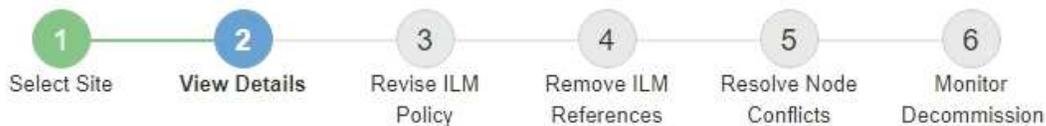


Wenn Sie eine nicht verbundene Website-Stillegung durchführen, kann ILM keine Objektdaten verschieben oder löschen. Alle Daten, die am Standort verbleiben, gehen verloren. Wenn Ihre ILM-Richtlinie jedoch zum Schutz vor dem Verlust eines einzelnen Standorts konzipiert wurde, sind Kopien der Objektdaten weiterhin auf den übrigen Standorten vorhanden. Siehe "[Schutz vor Standortausfällen](#)".

Schritte

1. Überprüfen Sie ab Schritt 2 (Details anzeigen) alle Warnungen im Zusammenhang mit dem zu entfernenden Standort.

Decommission Site



Data Center 2 Details

⚠ This site includes a Gateway Node. If clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before starting the decommission procedure.

⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

In diesen Fällen wird eine Warnung angezeigt:

- Der Standort enthält einen Gateway-Node. Wenn S3- und Swift-Clients derzeit eine Verbindung zu diesem Node herstellen, müssen Sie an einem anderen Standort einen entsprechenden Node konfigurieren. Vergewissern Sie sich, dass Clients eine Verbindung zum Ersatz-Node herstellen können, bevor Sie die Deaktivierung durchführen.
- Der Standort enthält eine Mischung aus verbundenen (✅) und nicht verbundene Knoten (🌙). Oder (🔄). Bevor Sie diesen Standort entfernen können, müssen Sie alle Offline-Nodes wieder in den Online-Modus versetzen.

2. Überprüfen Sie die Details der zu entfernenden Site.

Decommission Site



Raleigh Details

Number of Nodes: 3 Free Space: 475.38 GB
Used Space: 3.93 MB Site Capacity: 475.38 GB

Node Name	Node Type	Connection State	Details
RAL-S1-101-196	Storage Node	✓	1.30 MB used space
RAL-S2-101-197	Storage Node	✓	1.30 MB used space
RAL-S3-101-198	Storage Node	✓	1.34 MB used space

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Previous

Next

Für den ausgewählten Standort sind folgende Informationen enthalten:

- Anzahl der Nodes
- Der insgesamt verwendete Speicherplatz, der freie Speicherplatz und die Kapazität aller Speicherknoten am Standort.
 - Für die Stilllegung einer verbundenen Site gibt der Wert **verwendeter Speicherplatz** an, wie viele Objektdaten auf andere Standorte verschoben oder mit ILM gelöscht werden müssen.
 - Bei einer nicht verbundenen Deaktivierung des Standorts gibt der Wert **verwendeter Speicherplatz** an, auf welche Objektdaten beim Entfernen der Website nicht mehr zugegriffen werden kann.
- Node-Namen, -Typen und -Verbindungsstatus:
 - ✓ (Verbunden)
 - 🌙 (Administrativ Nach Unten)
 - 🔄 (Unbekannt)
- Details zu jedem Node:

- Für jeden Storage-Node die Menge an Speicherplatz, die für Objektdaten verwendet wurde.
- Gibt an, ob der Node derzeit in einer HA-Gruppe (Hochverfügbarkeit) verwendet wird, für Admin-Nodes und Gateway-Nodes. Sie können einen Admin-Node oder einen Gateway-Node, der in einer HA-Gruppe verwendet wird, nicht stilllegen. Bearbeiten Sie vor der Stilllegung HA-Gruppen, um alle Nodes am Standort zu entfernen, oder entfernen Sie die HA-Gruppe, wenn sie nur Nodes von diesem Standort umfasst. Anweisungen hierzu finden Sie unter "[Managen Sie Hochverfügbarkeitsgruppen \(High Availability Groups, HA-Gruppen\)](#)".

3. Bewerten Sie im Abschnitt Details für andere Standorte auf der Seite, wie viel Platz auf den anderen Standorten in Ihrem Raster verfügbar ist.

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
 Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space 	Used Space 	Site Capacity 
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Wenn Sie eine verbundene Website ausmustern und mithilfe von ILM Objektdaten von der ausgewählten Site verschieben (statt sie zu löschen), müssen Sie sicherstellen, dass die anderen Standorte über genügend Kapazität für die verschobenen Daten verfügen und dass genügend Kapazität für zukünftiges Wachstum verfügbar ist.



Eine Warnung wird angezeigt, wenn der **verwendete Platz** für die zu entfernende Website größer als der **gesamte freie Speicherplatz für andere Standorte** ist. Bevor Sie diesen Vorgang durchführen, müssen Sie sicherstellen, dass nach dem Entfernen des Standorts ausreichend Speicherkapazität verfügbar ist.

4. Wählen Sie **Weiter**.

Schritt 3 (ILM-Richtlinie überarbeiten) wird angezeigt.

Schritt 3: ILM-Richtlinie überarbeiten

Ab Schritt 3 (ILM-Richtlinie überarbeiten) des Assistenten für die Dekommission-Site können Sie feststellen, ob die Site von der aktiven ILM-Richtlinie angesprochen wird.

Bevor Sie beginnen

Sie haben gute Kenntnisse der Funktionsweise von ILM und sind mit der Erstellung von Storage-Pools, Profilen zur Fehlerkorrektur, ILM-Regeln sowie der Simulation und Aktivierung einer ILM-Richtlinie vertraut. Siehe "[Objektmanagement mit ILM](#)".

Über diese Aufgabe

StorageGRID kann einen Standort nicht ausmustern, wenn dieser Standort durch eine ILM-Regel der aktiven ILM-Richtlinie referenziert wird.

Wenn sich Ihre aktuelle ILM-Richtlinie auf die Site bezieht, die Sie entfernen möchten, müssen Sie eine neue ILM-Richtlinie aktivieren, die bestimmte Anforderungen erfüllt. Insbesondere die neue ILM-Richtlinie:

- Es kann kein Speicherpool verwendet werden, der sich auf den Standort bezieht oder die Option Alle Standorte verwendet.
- Ein Profil für die Erasure Coding-Verschlüsselung, das auf den Standort verweist, kann nicht verwendet werden.
- Die Regel „2 Kopien erstellen“ kann nicht von StorageGRID 11.6 oder früheren Installationen verwendet werden.
- Muss auf einen vollständigen Schutz aller Objektdaten ausgelegt sein.



Erstellen Sie niemals eine ILM-Regel für eine einzelne Kopie, um die Entfernung eines Standorts aufzunehmen. Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Wenn Sie eine „*connected Site*“-Ausmusterung durchführen, müssen Sie bedenken, wie StorageGRID die Objektdaten, die sich derzeit an der zu entfernenden Site befinden, verwalten sollte. Je nach Datensicherungsanforderungen können vorhandene Objektdaten nach den neuen Regeln auf verschiedene Standorte verschoben oder zusätzliche Objektkopien gelöscht werden, die nicht mehr benötigt werden.

Wenden Sie sich an den technischen Support, wenn Sie Hilfe beim Entwerfen der neuen Richtlinie benötigen.

Schritte

1. Stellen Sie ab Schritt 3 (ILM-Richtlinie überarbeiten) fest, ob ILM-Regeln der aktiven ILM-Richtlinie auf den Standort verweisen, den Sie entfernen möchten.
2. Wenn keine Regeln aufgeführt sind, wählen Sie **Weiter**, um zu gehen "[Schritt 4: Entfernen Sie ILM-Referenzen](#)".
3. Wenn eine oder mehrere ILM-Regeln in der Tabelle aufgeführt sind, wählen Sie den Link neben **Active Policy Name** aus.

Die Seite ILM-Richtlinien wird in einer neuen Browser-Registerkarte angezeigt. Auf dieser Registerkarte können Sie ILM aktualisieren. Die Seite „Decommission Site“ bleibt auf der anderen Registerkarte geöffnet.

- a. Wählen Sie bei Bedarf **ILM > Speicherpools** aus, um einen oder mehrere Speicherpools zu erstellen, die sich nicht auf den Standort beziehen.



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- b. Wenn Sie Erasure Coding verwenden möchten, wählen Sie **ILM > Erasure Coding** aus, um ein oder mehrere Erasure Coding-Profilen zu erstellen.

Sie müssen Speicherpools auswählen, die sich nicht auf den Standort beziehen.



Verwenden Sie nicht den **Alle Speicherknoten** Speicherpool (StorageGRID 11.6 und früher) in den Erasure Coding-Profilen.

4. Wählen Sie **ILM > Regeln** aus, und klonen Sie jede der in der Tabelle für Schritt 3 aufgeführten Regeln (ILM-Richtlinie überarbeiten).



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- a. Verwenden Sie Namen, die die Auswahl dieser Regeln in einer neuen Richtlinie erleichtern.
- b. Aktualisieren Sie die Anweisungen für die Platzierung.

Entfernen Sie alle Storage-Pools oder Profile zur Einhaltung von Erasure Coding, die auf den Standort verweisen, und ersetzen Sie diese durch neue Storage-Pools oder Erasure Coding-Profilen.



Verwenden Sie nicht den Speicherpool **Alle Storage Nodes** in den neuen Regeln.

5. Wählen Sie **ILM > Policies** und erstellen Sie eine neue Richtlinie, die die neuen Regeln verwendet.



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- a. Wählen Sie die aktive Richtlinie aus, und wählen Sie **Clone**.
- b. Geben Sie einen Richtliniennamen und einen Grund für die Änderung an.
- c. Wählen Sie Regeln für die geklonte Richtlinie aus.
 - Löschen Sie alle Regeln, die für Schritt 3 (ILM-Richtlinie überarbeiten) auf der Seite Decommission Site aufgeführt sind.
 - Wählen Sie eine Standardregel aus, die sich nicht auf die Site bezieht.



Wählen Sie nicht die Regel **2 Kopien erstellen** aus, da diese Regel den Speicherpool **Alle Storage Nodes** verwendet, der nicht zulässig ist.

- Wählen Sie die anderen Ersatzregeln aus, die Sie erstellt haben. Diese Regeln sollten sich nicht auf die Website beziehen.

Select Rules for Policy

Select Default Rule

This list shows the rules that do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last. The default rule should retain objects forever.

	Rule Name
<input checked="" type="radio"/>	2 copies at Sunnyvale and Vancouver for smaller objects
<input type="radio"/>	2 copy 2 sites for smaller objects
<input type="radio"/>	Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule and must use at least one filter. Each rule in this list uses at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

	Rule Name	Tenant Account
<input type="checkbox"/>	3 copies for S3 tenant	S3 (61659555232085399385)
<input type="checkbox"/>	EC for larger objects	—
<input checked="" type="checkbox"/>	1-site EC for larger objects	—
<input checked="" type="checkbox"/>	2 copies for S3 tenant	S3 (61659555232085399385)

Cancel

Apply

d. Wählen Sie **Anwenden**.

e. Ziehen Sie die Zeilen, um die Regeln in der Richtlinie neu anzuordnen.

Sie können die Standardregel nicht verschieben.



Sie müssen sich vergewissern, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen.

a. Speichern Sie die vorgeschlagene Richtlinie.

6. Nehmen Sie Testobjekte auf und simulieren Sie die vorgeschlagene Richtlinie, um sicherzustellen, dass die richtigen Regeln angewendet werden.



Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen. Prüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert.



Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommenen Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

7. Aktivieren Sie die neue Richtlinie.

Wenn Sie eine verbundene Website ausmustern, beginnt StorageGRID, Objektdaten von der ausgewählten Site zu entfernen, sobald Sie die neue ILM-Richtlinie aktivieren. Das Verschieben oder

Löschen aller Objektkopien kann Wochen in Anspruch nehmen. Sie können zwar eine Deaktivierung einer Website sicher starten, während noch Objektdaten am Standort vorhanden sind, aber die Deaktivierung erfolgt schneller und mit weniger Unterbrechungen und Performance-Beeinträchtigungen, wenn Daten vom Standort verschoben werden können, bevor Sie mit der tatsächlichen Außerbetriebnahme beginnen (Durch Auswahl von **Start Decommission** in Schritt 5 des Assistenten).

- Zurück zu **Schritt 3 (ILM-Richtlinie überarbeiten)** um sicherzustellen, dass in der neuen aktiven Richtlinie keine ILM-Regeln auf der Site angegeben sind und die Schaltfläche **Weiter** aktiviert ist.

Rules Referring to Raleigh in the Active ILM Policy

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: [Data Protection for Two Sites](#) 

No ILM rules in the active ILM policy refer to Raleigh.

Previous

Next



Wenn Regeln aufgeführt sind, müssen Sie eine neue ILM-Richtlinie erstellen und aktivieren, bevor Sie fortfahren können.

- Wenn keine Regeln aufgeführt sind, wählen Sie **Weiter**.

Schritt 4 (ILM-Referenzen entfernen) wird angezeigt.

Schritt 4: Entfernen Sie ILM-Referenzen

Ab Schritt 4 (Entfernen von ILM-Referenzen) des Decommission Site Wizard können Sie die vorgeschlagene Richtlinie entfernen, wenn diese vorhanden ist, und alle nicht verwendeten ILM-Regeln löschen oder bearbeiten, die sich noch auf die Site beziehen.

Über diese Aufgabe

In den folgenden Fällen können Sie den Ablauf zur Deaktivierung der Website nicht starten:

- Es gibt eine vorgeschlagene ILM-Richtlinie. Wenn Sie über eine vorgeschlagene Richtlinie verfügen, müssen Sie diese löschen.
- Jede ILM-Regel bezieht sich auf den Standort, selbst wenn diese Regel in keiner ILM-Richtlinie verwendet wird. Sie müssen alle Regeln, die sich auf die Website beziehen, löschen oder bearbeiten.

Schritte

- Wenn eine vorgeschlagene Richtlinie aufgeführt ist, entfernen Sie sie.
 - Wählen Sie **Vorgeschlagene Richtlinie Löschen**.
 - Wählen Sie im Bestätigungsdialogfeld * OK* aus.
- Stellen Sie fest, ob sich ungenutzte ILM-Regeln auf den Standort beziehen.

Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

4 ILM rules refer to Data Center 3 ▲

This table lists the unused ILM rules that still refer to the site. For each rule listed, you must do one of the following:

- Edit the rule to remove the Erasure Coding profile or storage pool from the placement instructions.
- Delete the rule.

[Go to the ILM Rules page](#)

Name	EC Profiles	Storage Pools	Delete
Make 2 Copies	—	All Storage Nodes	
3 copies for S3 tenant	—	Raleigh storage pool	
2 copies 2 sites for smaller objects	—	Raleigh storage pool	
EC larger objects	three site EC profile	All 3 Sites	

1 Erasure Coding profile will be deactivated ▼

3 storage pools will be deleted ▼

Alle aufgelisteten ILM-Regeln beziehen sich weiterhin auf den Standort, werden jedoch in keiner Richtlinie verwendet. Im Beispiel:

- Die Regel **2 Kopien erstellen** verwendet den Speicherpool **Alle Speicherknoten** (StorageGRID 11.6 und früher), der den Standort **Alle Standorte** verwendet.
- Die ungenutzte **3 Kopien für S3-Mandanten**-Regel bezieht sich auf den **Raleigh**-Speicherpool.
- Die ungenutzte **2 Copy 2-Seiten für kleinere Objekte**-Regel bezieht sich auf den **Raleigh**-Speicherpool.
- Die unbenutzten **EC larger Objects** Regeln verwenden die Raleigh Site im **All 3 Sites** Erasure Coding Profil.
- Wenn keine ILM-Regeln aufgeführt sind, wählen Sie **Weiter**, um zu gelangen "[Schritt 5: Auflösen von Knotenkonflikten \(und Start der Stilllegung\)](#)".



Wenn StorageGRID die Website dekomprimiert, werden alle ungenutzten Erasure Coding-Profile, die auf diesen Standort verweisen, automatisch deaktiviert und alle nicht verwendeten Storage-Pools, die auf den Standort verweisen, werden automatisch gelöscht. Der Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) wird entfernt, da er den Standort Alle Standorte verwendet.

- Wenn eine oder mehrere ILM-Regeln aufgeführt sind, fahren Sie mit dem nächsten Schritt fort.

3. Bearbeiten oder Löschen jeder nicht verwendeten Regel:

- Um eine Regel zu bearbeiten, aktualisieren Sie auf der ILM-Regelseite alle Platzierungen, die ein Erasure Coding-Profil oder einen Storage-Pool verwenden, das auf den Standort verweist. Kehren Sie dann zu **Schritt 4 (ILM-Referenzen entfernen)** zurück.



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- Um eine Regel zu löschen, wählen Sie das Papierkorb-Symbol aus Und wählen Sie **OK**.



Sie müssen die Regel **make 2 copies** löschen, bevor Sie eine Site stilllegen können.

4. Vergewissern Sie sich, dass keine vorgeschlagene ILM-Richtlinie vorhanden ist, keine ungenutzten ILM-Regeln auf die Site verweisen und die Schaltfläche **Weiter** ist aktiviert.

Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

No ILM rules refer to Raleigh

1 Erasure Coding profile will be deactivated ▼

3 storage pools will be deleted ▼

Previous
Next

5. Wählen Sie **Weiter**.



Alle verbleibenden Speicherpools und Profile für das Erasure Coding, die auf den Standort verweisen, werden ungültig, wenn der Standort entfernt wird. Wenn StorageGRID die Website dekomprimiert, werden alle ungenutzten Erasure Coding-Profile, die auf diesen Standort verweisen, automatisch deaktiviert und alle nicht verwendeten Storage-Pools, die auf den Standort verweisen, werden automatisch gelöscht. Der Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) wird entfernt, da er den Standort Alle Standorte verwendet.

Schritt 5 (Auflösen von Knotenkonflikten) wird angezeigt.

Schritt 5: Auflösen von Knotenkonflikten (und Start der Stilllegung)

Ab Schritt 5 (Auflösen von Knotenkonflikten) des Assistenten für die Dekommission-Website können Sie feststellen, ob Knoten in Ihrem StorageGRID-System getrennt sind oder ob Knoten am ausgewählten Standort zu einer HA-Gruppe gehören. Nachdem Konflikte mit Knoten behoben wurden, starten Sie den Vorgang zur Deaktivierung auf dieser Seite.

Bevor Sie beginnen

Sie müssen sicherstellen, dass alle Nodes in Ihrem StorageGRID System den richtigen Status aufweisen, wie folgt:

- Alle Knoten im StorageGRID-System müssen verbunden sein (✔).
-  Wenn Sie eine getrennte Site außer Betrieb nehmen, müssen alle Nodes an der entfernenden Site getrennt sein. Alle Nodes an allen anderen Standorten müssen verbunden sein.
 -  Die Stilllegung wird nicht gestartet, wenn ein oder mehrere Volumes offline (unmounted) sind oder online (gemountet) sind, sondern sich in einem Fehlerzustand befinden.
 -  Wenn ein oder mehrere Volumes offline geschaltet werden, während eine Deaktivierung durchgeführt wird, wird die Deaktivierung durchgeführt, nachdem diese Volumes wieder online geschaltet wurden.
- Kein Node an dem gerade entfernenden Standort kann eine Schnittstelle besitzen, die zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehört.

Über diese Aufgabe

Wenn ein Knoten für Schritt 5 (Auflösen von Knotenkonflikten) aufgeführt ist, müssen Sie das Problem beheben, bevor Sie den Stilllegen starten können.

Prüfen Sie vor dem Starten des Verfahrens zur Deaktivierung der Website auf dieser Seite die folgenden Aspekte:

- Sie müssen genügend Zeit haben, bis der Stilllegen abgeschlossen ist.
-  Das Verschieben oder Löschen von Objektdaten von einem Standort kann Tage, Wochen oder sogar Monate dauern, abhängig von der Datenmenge am Standort, der Systemlast, den Netzwerklatenzen und der Art der erforderlichen ILM-Änderungen.
- Während die Deaktivierung der Website läuft:
 - Sie können keine ILM-Regeln erstellen, die sich auf den deaktivierten Standort beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf den Standort zu verweisen.
 - Sie können keine anderen Wartungsverfahren wie Erweiterungen oder Upgrades durchführen.



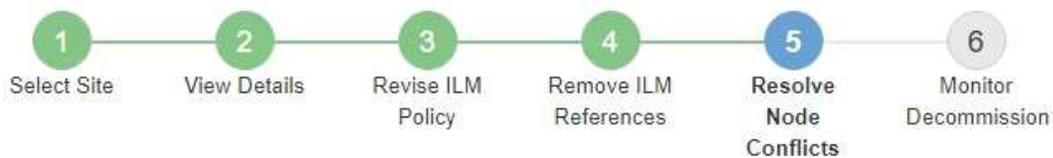
Wenn Sie während der Stilllegung einer verbundenen Site einen weiteren Wartungsvorgang durchführen müssen, können Sie den Vorgang unterbrechen, während die Storage-Nodes entfernt werden. Die Schaltfläche **Pause** ist während der Phase „DEcommissioning Replicated and Erasure coded Data“ aktiviert.

- Falls Nodes nach dem Starten der Deaktivierung der Website wiederhergestellt werden müssen, müssen Sie den Support kontaktieren.

Schritte

1. Überprüfen Sie den Abschnitt „nicht verbundene Knoten“ von Schritt 5 (Auflösen von Knotenkonflikten), um festzustellen, ob Knoten in Ihrem StorageGRID-System einen Verbindungsstatus von Unbekannt () Oder Administrativ Down ().

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

1 disconnected node in the grid ▲

The following nodes have a Connection State of Unknown (blue) or Administratively Down (gray). You must bring these disconnected nodes back online.

For help bringing nodes back online, see the instructions for [monitoring and troubleshooting StorageGRID](#) and the [recovery and maintenance](#) instructions.

Node Name	Connection State	Site	Type
DC1-S3-99-193 	 Administratively Down	Data Center 1	Storage Node

1 node in the selected site belongs to an HA group ▼

Passphrase

Provisioning Passphrase 

Previous

Start Decommission

2. Wenn Knoten getrennt werden, bringen Sie sie wieder in den Online-Modus.

Siehe "[Verfahren für den Grid-Node](#)". Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen.

3. Wenn alle getrennten Nodes wieder in den Online-Modus versetzt wurden, überprüfen Sie den Abschnitt HA-Gruppen in Schritt 5 (Auflösen von Node-Konflikten).

In dieser Tabelle werden alle Nodes am ausgewählten Standort aufgelistet, die zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehören.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

1 node in the selected site belongs to an HA group ▲

The following nodes in the selected site belong to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.

[Go to HA Groups page.](#)

For information about HA groups, see the instructions for [administering StorageGRID](#)

HA Group Name	Node Name	Node Type
HA group	DC1-GW1-99-190	API Gateway Node

Passphrase

Provisioning Passphrase

Previous

Start Decommission

4. Wenn alle Knoten aufgelistet sind, führen Sie einen der folgenden Schritte aus:

- Bearbeiten Sie jede betroffene HA-Gruppe, um die Node-Schnittstelle zu entfernen.
- Entfernen Sie eine HA-Gruppe, die nur Nodes aus diesem Standort enthält. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Wenn alle Nodes verbunden sind und keine Nodes am ausgewählten Standort in einer HA-Gruppe verwendet werden, ist das Feld **Provisioning-Passphrase** aktiviert.

5. Geben Sie die Provisionierungs-Passphrase ein.

Die Schaltfläche **Start Decommission** wird aktiviert.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be offline.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

No nodes in the selected site belong to an HA group

Passphrase

Provisioning Passphrase 

Previous

Start Decommission

6. Wenn Sie bereit sind, den Vorgang zur Deaktivierung der Website zu starten, wählen Sie **Start Decommission**.

Eine Warnung zeigt den Standort und die Knoten, die entfernt werden. Sie werden daran erinnert, dass es Tage, Wochen oder sogar Monate dauern kann, die Website vollständig zu entfernen.

⚠ Warning

The following site and its nodes have been selected for decommissioning and will be permanently removed from the StorageGRID system:

Data Center 3

- DC3-S1
- DC3-S2
- DC3-S3

When StorageGRID removes a site, it temporarily uses strong-site consistency to prevent object metadata from being written to the site being removed. Client write and delete operations can fail if multiple nodes become unavailable at the remaining sites.

This procedure might take days, weeks, or even months to complete. Select **Maintenance > Decommission** to monitor the decommission progress.

Do you want to continue?

Cancel

OK

7. Überprüfen Sie die Warnung. Wenn Sie bereit sind, zu beginnen, wählen Sie **OK**.

Beim Generieren der neuen Grid-Konfiguration wird eine Meldung angezeigt. Dieser Prozess kann je nach Typ und Anzahl der nicht mehr verwendeten Grid-Nodes einige Zeit in Anspruch nehmen.

Passphrase

Provisioning Passphrase ⓘ

.....

ⓘ Generating grid configuration. This may take some time depending on the type and the number of decommissioned grid nodes.

Previous

Start Decommission



Wenn die neue Grid-Konfiguration generiert wurde, wird Schritt 6 (Monitor Decommission) angezeigt.



Die Schaltfläche * Previous* bleibt deaktiviert, bis die Stilllegung abgeschlossen ist.

Schritt 6: Überwachung Der Dekommission

Ab Schritt 6 (Überwachung der Dekommission) des Seitenassistenten der Decommission-Website können Sie den Fortschritt überwachen, während die Site entfernt wird.

Über diese Aufgabe

Wenn StorageGRID einen verbundenen Standort entfernt, werden Nodes in dieser Reihenfolge entfernt:

1. Gateway-Nodes
2. Admin-Nodes
3. Storage-Nodes

Wenn StorageGRID einen getrennten Standort entfernt, werden Nodes in dieser Reihenfolge entfernt:

1. Gateway-Nodes
2. Storage-Nodes
3. Admin-Nodes

Jeder Gateway-Node oder Admin-Node kann möglicherweise nur ein paar Minuten oder eine Stunde entfernt werden. Storage-Nodes können jedoch Tage oder Wochen in Anspruch nehmen.

Schritte

1. Sobald ein neues Wiederherstellungspaket erstellt wurde, laden Sie die Datei herunter.

Decommission Site



i A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.



Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Grid wiederherstellen können, wenn während des Stillfalls etwas schief geht.

- a. Wählen Sie den Link in der Nachricht aus, oder wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
- b. Laden Sie die herunter .zip Datei:

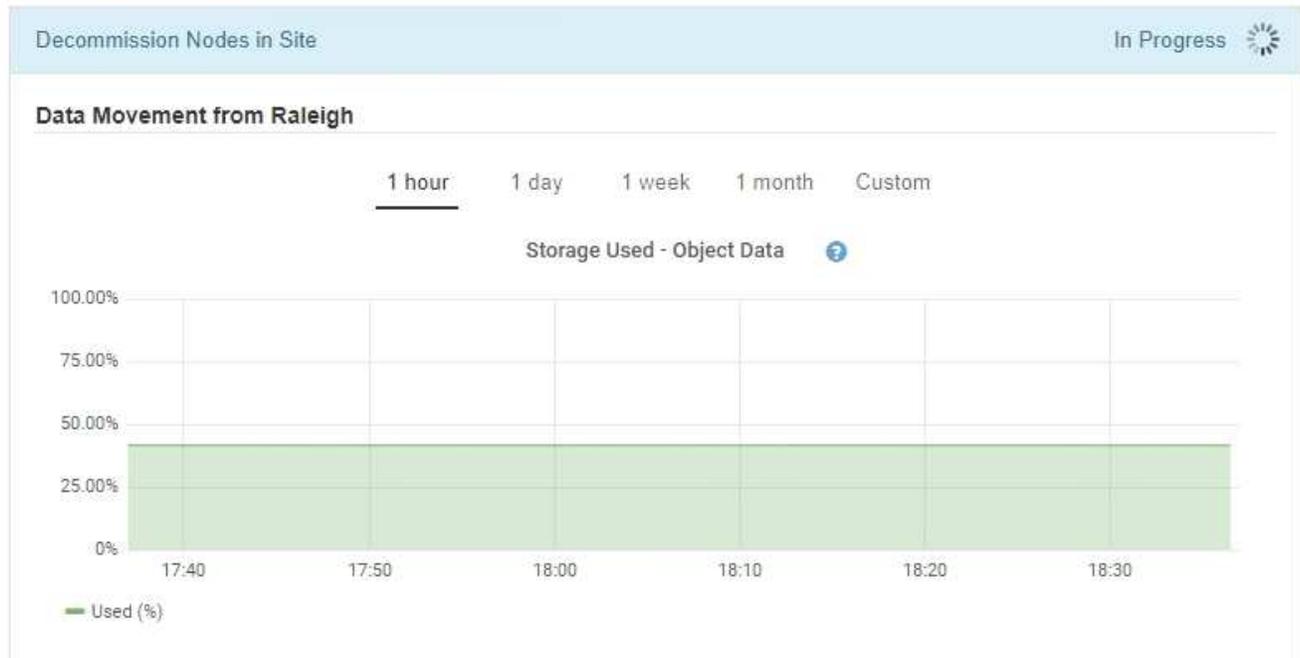
Siehe Anweisungen für "[Herunterladen des Wiederherstellungspakets](#)".



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

2. Überwachen Sie mithilfe des Diagramms für die Datenverschiebung das Verschieben von Objektdaten von dieser Seite zu anderen Standorten.

Datenverschiebung gestartet, als Sie die neue ILM-Richtlinie in Schritt 3 aktiviert haben (ILM-Richtlinie überarbeiten). Die Datenverschiebung findet während der gesamten Außerbetriebnahme statt.



3. Überwachen Sie im Abschnitt Status des Knotens der Seite den Fortschritt des Stillstandsvorgangs, wenn Nodes entfernt werden.

Wenn ein Speicherknoten entfernt wird, durchläuft jeder Knoten eine Reihe von Phasen. Obwohl die meisten dieser Phasen schnell oder sogar unmerklich auftreten, müssen Sie möglicherweise Tage oder sogar Wochen warten, bis andere Phasen abgeschlossen sind, je nachdem, wie viele Daten verschoben werden müssen. Zur Verwaltung von Daten, die mit Erasure Coding versehen sind, und zur Neubewertung von ILM-Verfahren ist zusätzlicher Zeit erforderlich.

Node Progress

 Depending on the number of objects stored, Storage Nodes might take significantly longer to decommission. Extra time is needed to manage erasure coded data and re-evaluate ILM.

The progress for each node is displayed while the decommission procedure is running. If you need to perform another maintenance procedure, select **Pause** to suspend the decommission (only allowed during certain stages).



Name 	Type 	Progress 	Stage 
RAL-S1-101-196	Storage Node	<div style="width: 20px; height: 10px; background-color: #00a0e3; border: 1px solid #ccc;"></div>	Decommissioning Replicated and Erasure Coded Data
RAL-S2-101-197	Storage Node	<div style="width: 20px; height: 10px; background-color: #00a0e3; border: 1px solid #ccc;"></div>	Decommissioning Replicated and Erasure Coded Data
RAL-S3-101-198	Storage Node	<div style="width: 20px; height: 10px; background-color: #00a0e3; border: 1px solid #ccc;"></div>	Decommissioning Replicated and Erasure Coded Data

Wenn Sie den Fortschritt der Deaktivierung einer verbundenen Site überwachen, lesen Sie diese Tabelle, um die Phasen zur Ausmusterung eines Storage Node zu verstehen:

Stufe	Geschätzte Dauer
Ausstehend	Minuten oder weniger
Warten Sie auf Sperren	Minuten
Aufgabe Vorbereiten	Minuten oder weniger
Markieren von LDR deaktiviert	Minuten
Stilllegung replizierter und Erasure Coding von Daten	Stunden, Tage oder Wochen, basierend auf der Datenmenge Hinweis: Wenn Sie weitere Wartungsarbeiten durchführen müssen, können Sie die Deaktivierung der Website während dieser Phase unterbrechen.
LDR-Status gesetzt	Minuten
Audit-Warteschlangen Leeren	Minuten bis Stunden, basierend auf der Anzahl der Nachrichten und der Netzwerklatenz.
Vollständig	Minuten

Wenn Sie den Fortschritt der Deaktivierung einer getrennten Site überwachen, lesen Sie diese Tabelle, um weitere Informationen zur Ausmusterung von Storage Nodes zu erhalten:

Stufe	Geschätzte Dauer
Ausstehend	Minuten oder weniger
Warten Sie auf Sperren	Minuten
Aufgabe Vorbereiten	Minuten oder weniger
Externe Dienste Deaktivieren	Minuten
Widerruf Des Zertifikats	Minuten
Knoten Nicht Registrieren	Minuten
Storage-Klasse Nicht Registrieren	Minuten
Entfernung Von Speichergruppen	Minuten

Stufe	Geschätzte Dauer
Entfernen Der Einheit	Minuten
Vollständig	Minuten

4. Sobald alle Nodes abgeschlossen sind, warten Sie, bis der restliche Standort außer Betrieb ist.
- Im Schritt **Cassandra reparieren** führt StorageGRID alle erforderlichen Reparaturen an den Cassandra-Clustern durch, die in Ihrem Grid verbleiben. Je nachdem, wie viele Speicherknoten im Raster verbleiben, kann diese Reparaturen mehrere Tage oder länger dauern.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	In Progress 
StorageGRID is repairing the remaining Cassandra clusters after removing the site. This might take several days or more, depending on how many Storage Nodes remain in your grid.	
Overall Progress	<div style="width: 0%;"><div></div></div> 0%
Deactivate EC Profiles & Delete Storage Pools	Pending
Remove Configurations	Pending

- Während des Schritts **EC-Profil deaktivieren & Speicherpools löschen** werden folgende ILM-Änderungen vorgenommen:
 - Alle Löschkennzeichnungsprofile, die auf die Site verwiesen werden, werden deaktiviert.
 - Alle Speicherpools, die auf den Standort verwiesen werden gelöscht.



Der Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) wird ebenfalls entfernt, da er den Standort Alle Standorte verwendet.

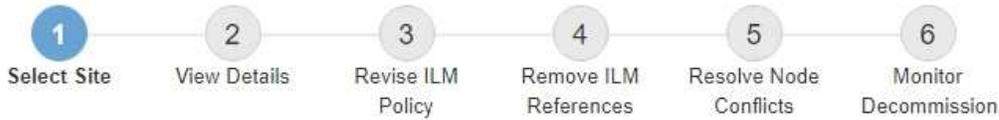
- Schließlich werden im Schritt **Konfiguration entfernen** alle verbleibenden Verweise auf die Site und ihre Knoten aus dem Rest des Rasters entfernt.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	Completed
Deactivate EC Profiles & Delete Storage Pools	Completed
Remove Configurations	In Progress 
StorageGRID is removing the site and node configurations from the rest of the grid.	

5. Nach Abschluss des Stilllegen-Verfahrens wird auf der Seite Decommission Site eine Meldung angezeigt, die den entfernten Standort nicht mehr anzeigt.

Decommission Site



The previous decommission procedure completed successfully at 2021-01-12 14:28:32 MST.

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity	Decommission Possible
<input checked="" type="radio"/>	Sunnyvale	4.79 MB	
<input type="radio"/>	Vancouver	4.90 MB	No. This site contains the primary Admin Node.

Next

Nachdem Sie fertig sind

Führen Sie diese Aufgaben nach Abschluss des Verfahrens zur Deaktivierung der Website durch:

- Stellen Sie sicher, dass die Laufwerke aller Storage-Nodes am ausgemusterten Standort sauber gelöscht werden. Verwenden Sie ein handelsübliches Datenwischwerkzeug oder einen Dienst, um die Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn die Site einen oder mehrere Admin-Nodes enthält und Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, entfernen Sie alle Vertrauensstellen für die Site aus Active Directory Federation Services (AD FS).
- Nachdem die Knoten im Rahmen der Deaktivierung des angeschlossenen Standorts automatisch ausgeschaltet wurden, entfernen Sie die zugehörigen virtuellen Maschinen.

Benennen Sie Raster, Standorte und Nodes um

Raster, Standorte und Knoten umbenennen: Übersicht

Bei Bedarf können Sie die Anzeigenamen ändern, die im Grid Manager für das gesamte Raster, jeden Standort und jeden Node angezeigt werden. Sie können Anzeigenamen sicher und jederzeit aktualisieren.

Wie lautet das Umbenennungsverfahren?

Wenn Sie StorageGRID von Anfang an installieren, geben Sie einen Namen für das Grid, jeden Standort und

jeden Node an. Diese Anfangsnamen werden als *System names* bezeichnet, und sie sind die Namen, die ursprünglich 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, jeden Standort und jeden Node zu definieren. Diese Anzeigenamen werden an verschiedenen StorageGRID-Speicherorten anstelle (oder in einigen Fällen zusätzlich zu) der zugrunde liegenden Systemnamen angezeigt.

Verwenden Sie das Umbenennungsverfahren, um Tippfehler zu korrigieren, eine andere Benennungskonvention zu implementieren oder um anzuzeigen, dass ein Standort und alle seine Knoten verschoben wurden. Im Gegensatz zu Systemnamen können Anzeigenamen bei Bedarf und ohne Beeinträchtigung der StorageGRID-Vorgänge aktualisiert werden.

Wo werden System- und Anzeigenamen angezeigt?

Die folgende Tabelle fasst zusammen, wo Systemnamen und Anzeigenamen in der StorageGRID-Benutzeroberfläche und in StorageGRID-Dateien angezeigt werden.

Standort	Systemname	Anzeigename
Seiten von Grid Manager	Wird angezeigt, sofern das Element nicht umbenannt wird	<p>Wenn ein Element umbenannt wird, wird anstelle des Systemnamens an diesen Speicherorten angezeigt:</p> <ul style="list-style-type: none"> • Dashboard • Knoten Seite • Konfigurationsseiten für Hochverfügbarkeitsgruppen, Load Balancer-Endpunkte, VLAN-Schnittstellen, Verschlüsselungsmanagement-Server, Grid-Passwörter, Und Firewall-Kontrolle • Meldungen • Speicherpooldefinitionen • Seite zur Objekt-Metadaten-Suche • Seiten im Zusammenhang mit Wartungsverfahren, einschließlich Upgrade, Hotfix, SANtricity-Betriebssystem-Upgrade, Stilllegung, Erweiterung, Wiederherstellung und Prüfung des Objektbestandes • Support-Seiten (Protokolle und Diagnose) • Seite für die einfache Anmeldung neben dem Hostnamen des Admin-Knotens in der Tabelle für Details zum Admin-Knoten
NODES > Übersicht Tab für einen Knoten	Immer angezeigt	Wird nur angezeigt, wenn das Element umbenannt wurde

Standort	Systemname	Anzeigename
Legacy-Seiten im Grid Manager (z. B. SUPPORT > Grid Topology)	Angezeigt	Nicht abgebildet
Node-Health API	Immer zurückgekehrt	Dieser Wert wird nur zurückgegeben, wenn das Element umbenannt wurde
Eingabeaufforderung beim Verwenden von SSH zum Zugriff auf einen Node	Wird als Primärname angezeigt, sofern das Element nicht umbenannt wurde: admin@SYSTEM-NAME: ~ \$ Wenn das Element umbenannt wird, wird es in Klammern aufgenommen: admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$	Wird als Primärname angezeigt, wenn das Element umbenannt wird: admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$
Passwords.txt Datei im Wiederherstellungspaket	Angezeigt als Server Name	Angezeigt 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	Immer in der zweiten Spalte angezeigt	Wenn das Element umbenannt wird, wird es in der vierten Spalte angezeigt
topology-display-names.json, In AutoSupport-Daten enthalten	Nicht enthalten	Leer, es sei denn, Elemente wurden umbenannt; andernfalls werden Raster-, Standort- und Knoten-IDs ihren Anzeigenamen zugeordnet.

Anforderungen für Anzeigenamen

Bevor Sie dieses Verfahren verwenden, überprüfen Sie die Anforderungen für Anzeigenamen.

Namen für Nodes anzeigen

Anzeigenamen für Nodes müssen folgende Regeln einhalten:

- Muss für Ihr StorageGRID System eindeutig sein.
- Darf nicht mit dem Systemnamen eines anderen Elements in Ihrem StorageGRID-System identisch sein.
- Muss mindestens 1 und nicht mehr als 32 Zeichen enthalten.
- Kann Zahlen, Bindestriche (-) sowie Groß- und Kleinbuchstaben enthalten.
- Kann mit einem Buchstaben oder einer Zahl beginnen oder enden, aber nicht mit einem Bindestrich beginnen oder enden.
- Es können nicht alle Zahlen sein.
- Die Groß-/Kleinschreibung muss nicht beachtet werden. Beispiel: DC1-ADM Und dc1-adm Werden als Duplikate betrachtet.

Sie können einen Node mit einem Anzeigenamen umbenennen, der zuvor von einem anderen Node verwendet wurde, solange die Umbenennung nicht zu einem doppelten Anzeigenamen oder Systemnamen führt.

Namen für Raster und Standorte anzeigen

Anzeigenamen für das Raster und Standorte folgen denselben Regeln mit diesen Ausnahmen:

- Kann Leerzeichen enthalten.
- Folgende Sonderzeichen sind zulässig: = - _ : , . @ !
- Kann mit den Sonderzeichen einschließlich Bindestrichen beginnen und enden.
- Kann aus allen Zahlen oder Sonderzeichen bestehen.

Best Practices für Anzeigenamen

Wenn Sie mehrere Elemente umbenennen möchten, dokumentieren Sie Ihr allgemeines Benennungsschema, bevor Sie dieses Verfahren verwenden. Ein System, das dafür sorgt, dass die Namen eindeutig, konsistent und auf einen Blick verständlich sind.

Sie können beliebige Namenskonventionen verwenden, die Ihren Unternehmensanforderungen entsprechen. Berücksichtigen Sie diese grundlegenden Vorschläge hinsichtlich der folgenden Punkte:

- **Standortkennzeichen:** Wenn Sie mehrere Standorte haben, fügen Sie jedem Knotennamen einen Standortcode hinzu.
- **Knotentyp:** Knotennamen geben in der Regel den Knotentyp an. Sie können Abkürzungen wie verwenden `s`, `adm`, `gw`, und `arc` (Storage Node, Admin Node, Gateway Node und Archive Node).
- **Knotennummer:** Wenn ein Standort mehr als einen bestimmten Knotentyp enthält, fügen Sie dem Namen jedes Knotens eine eindeutige Nummer hinzu.

Überlegen Sie sich zweimal, bevor Sie den Namen, die sich wahrscheinlich im Laufe der Zeit ändern, spezifische Details hinzufügen. Nehmen Sie beispielsweise keine IP-Adressen in Node-Namen auf, da diese Adressen geändert werden können. Ebenso können sich die Rack-Standorte oder die Modellnummern der Appliance ändern, wenn Sie Geräte verlagern oder die Hardware aktualisieren.

Beispiel für Anzeigenamen

Angenommen, Ihr StorageGRID System hat drei Datacenter und verfügt in jedem Datacenter über unterschiedliche Nodes. Ihre Anzeigenamen können so einfach sein wie diese:

- **Raster:** StorageGRID Deployment
- **Erste Seite:** Data Center 1
 - dc1-adm1
 - dc1-s1
 - dc1-s2
 - dc1-s3
 - dc1-gw1
- **Zweiter Standort:** Data Center 2
 - dc2-adm2
 - dc2-s1
 - dc2-s2
 - dc2-s3
- **Dritter Standort:** Data Center 3
 - dc3-s1
 - dc3-s2
 - dc3-s3

Anzeigenamen hinzufügen oder aktualisieren

Mit diesem Verfahren können Sie die Anzeigenamen für Ihr Raster, Ihre Standorte und Knoten 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 sind Sie mit einem beim Grid-Manager angemeldet "[Unterstützter Webbrowser](#)".



Sie können Anzeigenamen von einem nicht-primären Admin-Node hinzufügen oder aktualisieren, müssen jedoch beim primären Admin-Node angemeldet sein, um ein Wiederherstellungspaket herunterzuladen.

- Sie haben die Berechtigung `Wartung` oder `Stammzugriff`.
- Sie haben die Provisionierungs-Passphrase.
- Sie kennen die Anforderungen und Best Practices für Anzeigenamen. Siehe "[Raster, Standorte und Knoten umbenennen: Übersicht](#)".

Umbenennen von Rastergittern, Standorten oder Nodes

Sie können das StorageGRID-System, einen oder mehrere Standorte oder einen oder mehrere Nodes umbenennen.

Sie können einen Anzeigenamen verwenden, der zuvor von einem anderen Node verwendet wurde, solange die Umbenennung nicht zu einem doppelten Anzeigenamen oder Systemnamen führt.

Wählen Sie die umzubennenden Elemente aus

Wählen Sie zum Starten die Elemente aus, die Sie umbenennen möchten.

Schritte

1. Wählen Sie **MAINTENANCE > Tasks > Raster, Standorte und Knoten umbenennen**.
2. Wählen Sie im Schritt **Namen auswählen** die Elemente aus, die Sie umbenennen möchten.

Zu ändernde Position	Anweisung
Namen von allem (oder fast allem) in Ihrem System	<ol style="list-style-type: none">a. Wählen Sie Alle auswählen.b. Löschen Sie optional alle Elemente, die Sie nicht umbenennen möchten.
Name des Rasters	Aktivieren Sie das Kontrollkästchen für das Raster.
Name eines Standorts und einige oder alle seiner Knoten	<ol style="list-style-type: none">a. Aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift für den Standort.b. Löschen Sie optional alle Nodes, die Sie nicht umbenennen möchten.
Name einer Site	Aktivieren Sie das Kontrollkästchen für den Standort.
Name eines Node	Aktivieren Sie das Kontrollkästchen für den Knoten.

3. Wählen Sie **Weiter**.
4. Überprüfen Sie die Tabelle, die die ausgewählten Elemente enthält.
 - Die Spalte **Anzeigename** zeigt den aktuellen Namen für jedes Element an. Wenn das Element nie umbenannt wurde, ist sein Anzeigename mit dem Systemnamen identisch.
 - Die Spalte **Systemname** zeigt den Namen an, den Sie für jedes Element während der Installation eingegeben haben. Systemnamen werden für interne StorageGRID-Vorgänge verwendet und können nicht geändert werden. Beispielsweise kann der Systemname für einen Node sein Hostname sein.
 - Die Spalte **Typ** gibt den Typ des Elements an: Grid, Site oder den spezifischen Typ des Knotens.

Schlagen Sie neue Namen vor

Für den Schritt **Neue Namen vorschlagen** können Sie einen Anzeigenamen für jedes Element einzeln eingeben oder Elemente in großen Mengen umbenennen.

Benennen Sie Elemente einzeln um

Führen Sie die folgenden Schritte aus, um für jedes Element, das Sie umbenennen möchten, einen Anzeigenamen einzugeben.

Schritte

1. Geben Sie in das Feld **Anzeigename** einen vorgeschlagenen Anzeigenamen für jedes Element in der Liste ein.

Siehe "[Raster, Standorte und Knoten umbenennen: Übersicht](#)" Um die Namensanforderungen zu erlernen.

2. Um Elemente zu entfernen, die Sie nicht umbenennen möchten, wählen Sie aus  In der Spalte **aus Liste entfernen**.

Wenn Sie keinen neuen Namen für ein Element vorschlagen, müssen Sie es aus der Tabelle entfernen.

3. Wenn Sie neue Namen für alle Elemente in der Tabelle vorgeschlagen haben, wählen Sie **Umbenennen**.

Eine Erfolgsmeldung wird angezeigt. Die neuen Anzeigenamen werden nun im gesamten Grid Manager verwendet.

Umbenennen von Elementen in Massen

Verwenden Sie das Tool zum Umbenennen mehrerer Elemente, wenn Elementnamen eine gemeinsame Zeichenfolge verwenden, die Sie durch eine andere Zeichenfolge ersetzen möchten.

Schritte

1. Wählen Sie für den Schritt **Neue Namen vorschlagen Bulk Rename Tool verwenden**.

Die Vorschau **Umbenennen** enthält 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 **existing string** den freigegebenen String ein, den Sie ersetzen möchten. Beispiel: Wenn die Zeichenfolge, die Sie ersetzen möchten, lautet `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 zu finden ist.

3. Wählen Sie  Um alle Elemente zu entfernen, die Sie mit diesem Tool nicht umbenennen möchten.

Angenommen, Sie möchten alle Nodes umbenennen, die den String enthalten `Data-Center-1`, Aber Sie möchten das nicht umbenennen `Data-Center-1` Standort selbst. Wählen Sie  So entfernen Sie die Site aus der Vorschau zum Umbenennen.

Bulk rename tool

Rename preview 

<i>Data-Center-1</i> 
<i>Data-Center-1-ADM1</i> 
<i>Data-Center-1-ARC1</i> 
<i>Data-Center-1-G1</i> 
<i>Data-Center-1-S1</i> 
<i>Data-Center-1-S2</i> 
<i>Data-Center-1-S3</i> 
<i>Data-Center-1-S4</i> 

Cancel 

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

The string you want to replace. Represented by *italicized text* in the preview section.

New string

The string you want to use instead. Represented by **bolded text** in the preview section.

4. Geben Sie im Feld **New string** den Ersatzstring ein, den Sie stattdessen verwenden möchten. Geben Sie beispielsweise **DC1** ein.

Siehe "[Raster, Standorte und Knoten umbenennen: Übersicht](#)" Um die Namensanforderungen zu erlernen.

Wenn Sie die Ersatzzeichenfolge eingeben, werden die Namen auf der linken Seite aktualisiert, sodass Sie überprüfen können, ob die neuen Namen korrekt sind.

Bulk rename tool

Rename preview ⓘ

DC1-ADM1	✕
DC1-ARC1	✕
DC1-G1	✕
DC1-S1	✕
DC1-S2	✕
DC1-S3	✕
DC1-S4	✕

Cancel **Add names**

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

The string you want to replace. Represented by *italicized text* in the preview section.

New string

The string you want to use instead. Represented by **bolded text** in the preview section.

5. Wenn Sie mit den in der Vorschau angezeigten Namen zufrieden sind, wählen Sie **Namen hinzufügen**, um die Namen der Tabelle für den Schritt **Neue Namen vorschlagen** hinzuzufügen.
6. Nehmen Sie alle erforderlichen zusätzlichen Änderungen vor, oder wählen Sie ✕ Um alle Elemente zu entfernen, die Sie nicht umbenennen möchten.
7. Wenn Sie alle Elemente in der Tabelle umbenennen möchten, wählen Sie **Umbenennen**.

Eine Erfolgsmeldung wird angezeigt. Die neuen Anzeigenamen werden nun im gesamten Grid Manager verwendet.

Laden Sie das Wiederherstellungspaket herunter

Wenn Sie die Umbenennung der Elemente abgeschlossen haben, laden Sie ein neues Wiederherstellungspaket herunter und speichern Sie es. Die neuen Anzeigenamen für die Elemente, die Sie umbenannt haben, sind in der enthaltenen `Passwords.txt` Datei:

Schritte

1. Geben Sie die Provisionierungs-Passphrase ein.
2. Wählen Sie **Download Recovery Package**.

Der Download startet sofort.

3. Wenn der Download abgeschlossen ist, öffnen Sie das `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 separate Speicherorte.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

5. Wählen Sie **Fertig**, um zum ersten Schritt zurückzukehren.

Zurücksetzen der Anzeigenamen auf Systemnamen

Sie können ein umbenanntes Raster, eine Site oder einen Node auf den ursprünglichen Systemnamen zurücksetzen. Wenn Sie ein Element auf seinen Systemnamen zurücksetzen, werden auf den Seiten des Grid-Managers und anderen StorageGRID-Speicherorten kein **Anzeigename** für dieses Element mehr angezeigt. Es wird nur der Systemname des Elements angezeigt.

Schritte

1. Wählen Sie **MAINTENANCE > Tasks > Raster, Standorte und Knoten umbenennen**.
2. Wählen Sie im Schritt **Namen auswählen** alle Elemente aus, die Sie auf Systemnamen zurücksetzen möchten.
3. Wählen Sie **Weiter**.
4. Für den Schritt **Neue Namen vorschlagen**, stellen Sie Anzeigenamen einzeln oder in Massen zurück auf Systemnamen.

Individuelle Wiederherstellung auf Systemnamen

- 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 nicht rückgängig gemacht werden sollen.

Um einen Anzeigenamen rückgängig zu machen, muss der Systemname im Feld **Anzeigename** angezeigt werden, der Name muss jedoch nicht zwischen Groß- und Kleinschreibung unterschieden werden.

- b. Wählen Sie **Umbenennen**.

Eine Erfolgsmeldung wird angezeigt. Die Anzeigenamen für diese Elemente werden nicht mehr verwendet.

Zurücksetzen auf Systemnamen in Massen

- a. Wählen Sie für den Schritt **Neue Namen vorschlagen Bulk Rename Tool verwenden**.
- b. Geben Sie in das Feld **existing string** den anzuzeigenden Namensstring ein, den Sie ersetzen möchten.
- c. Geben Sie im Feld **New string** den Systemnamen ein, den Sie stattdessen verwenden möchten.
- d. Wählen Sie **Namen hinzufügen**, um die Namen der Tabelle für den Schritt **Neue Namen vorschlagen** hinzuzufügen.
- e. Bestätigen Sie, dass jeder Eintrag im Feld **Anzeigename** mit dem Namen im Feld **Systemname** übereinstimmt. Nehmen Sie Änderungen vor oder wählen Sie aus Um alle Elemente zu entfernen, die nicht rückgängig gemacht werden sollen.

Um einen Anzeigenamen rückgängig zu machen, muss der Systemname im Feld **Anzeigename** angezeigt werden, der Name muss jedoch nicht zwischen Groß- und Kleinschreibung unterschieden werden.

- f. Wählen Sie **Umbenennen**.

Eine Erfolgsmeldung wird angezeigt. Die Anzeigenamen für diese Elemente werden nicht mehr verwendet.

5. [Laden Sie ein neues Wiederherstellungspaket herunter und speichern Sie es](#).

Anzeigenamen für die zurückgesenkten Elemente sind nicht mehr in der enthalten `Passwords.txt` Datei:

Netzwerkwartungsverfahren

Subnetze für Grid Network aktualisieren

StorageGRID pflegt eine Liste der für die Kommunikation zwischen den Grid-Nodes im Grid-Netzwerk (eth0) verwendeten Subnetze. Zu diesen Einträgen gehören die Subnetze, die von jedem Standort im StorageGRID-System für das Grid-Netzwerk verwendet werden, sowie alle Subnetze, die für NTP, DNS, LDAP oder andere externe Server verwendet werden, auf die über das Grid-Netzwerk-Gateway zugegriffen wird. Wenn Sie

Grid-Nodes oder einen neuen Standort in einer Erweiterung hinzufügen, müssen Sie möglicherweise Subnetze zum Grid-Netzwerk aktualisieren oder hinzufügen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Berechtigung für Wartung oder Root-Zugriff](#)".
- Sie haben die Provisionierungs-Passphrase.
- Sie haben die Netzwerkadressen in CIDR-Notation der Subnetze, die Sie konfigurieren möchten.

Über diese Aufgabe

Wenn Sie eine Erweiterungsaktivität durchführen, die das Hinzufügen eines neuen Subnetzes einschließt, müssen Sie der Netznetznetznetznetznetznetznetznetznetznetznetznetznetznetznetznetznetzliste ein neues Subnetz hinzufügen, bevor Sie mit dem Erweiterungsverfahren beginnen. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und die Erweiterung erneut starten.

Fügen Sie ein Subnetz hinzu

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > Grid-Netzwerk**.
2. Wählen Sie **Add another subnet**, um ein neues Subnetz in CIDR-Notation hinzuzufügen.

Geben Sie beispielsweise ein 10.96.104.0/22.

3. Geben Sie die Provisionierungs-Passphrase 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 **Provisioning-Passphrase** ein.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können. Er wird auch zur Wiederherstellung des primären Admin-Knotens verwendet.

Die angegebenen Subnetze werden automatisch für Ihr StorageGRID System konfiguriert.

Bearbeiten Sie ein Subnetz

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 Provisionierungs-Passphrase 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 **Provisioning-Passphrase** ein.

Löschen Sie ein Subnetz

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > Grid-Netzwerk**.
2. Klicken Sie auf das Löschsymboll  Neben dem Subnetz.
3. Geben Sie die Provisionierungs-Passphrase 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 **Provisioning-Passphrase** ein.

Konfigurieren Sie IP-Adressen

Konfigurieren Sie IP-Adressen

Sie können eine Netzwerkkonfiguration durchführen, indem Sie IP-Adressen für Grid-Nodes mithilfe des Tools IP ändern konfigurieren.

Sie müssen das Change IP-Tool verwenden, um die meisten Änderungen an der Netzwerkkonfiguration vorzunehmen, die ursprünglich während der Grid-Implementierung festgelegt wurde. Manuelle Änderungen unter Verwendung von standardmäßigen Linux-Netzwerkbefehlen und Dateien werden möglicherweise nicht an allen StorageGRID-Diensten weitergegeben. Dabei bleiben Upgrades, Neustarts oder Recovery-Verfahren für Knoten nicht erhalten.



Das IP-Änderungsverfahren kann eine Unterbrechungsmaßnahme sein. Teile des Rasters sind möglicherweise erst verfügbar, wenn die neue Konfiguration angewendet wird.



Wenn Sie nur Änderungen an der Netznetzwerksubnetz-Liste vornehmen, verwenden Sie den Grid-Manager, um die Netzwerkkonfiguration hinzuzufügen oder zu ändern. Verwenden Sie andernfalls das Change IP-Tool, wenn der Grid Manager aufgrund eines Netzwerkkonfigurationsproblem nicht erreichbar ist, oder Sie führen gleichzeitig eine Änderung des Grid Network Routing und andere Netzwerkänderungen durch.



Wenn Sie die Grid-Netzwerk-IP-Adresse für alle Knoten im Raster ändern möchten, verwenden Sie den "[Sonderverfahren für netzweite Änderungen](#)".

Ethernet-Schnittstellen

Die eth0 zugewiesene IP-Adresse ist immer die Grid-Netzwerk-IP-Adresse des Grid-Node. Die eth1 zugewiesene IP-Adresse ist immer die Admin-Netzwerk-IP-Adresse des Grid-Node. Die eth2 zugewiesene IP-Adresse ist immer die Client-Netzwerk-IP-Adresse des Grid-Node.

Beachten Sie, dass auf einigen Plattformen, z. B. StorageGRID Appliances, eth0, eth1 und eth2, aggregierte Schnittstellen bestehen, die aus untergeordneten Bridges oder Bindungen von physischen oder VLAN-Schnittstellen bestehen. Auf diesen Plattformen zeigt die Registerkarte **SSM > Resources** möglicherweise die Grid-, Admin- und Client-Netzwerk-IP-Adresse an, die anderen Schnittstellen zusätzlich zu eth0, eth1 oder

eth2 zugewiesen ist.

DHCP

Sie können DHCP nur während der Bereitstellungsphase einrichten. DHCP kann während der Konfiguration nicht eingerichtet werden. Sie müssen die Änderungsverfahren für die IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmaske und Standard-Gateways für einen Grid-Node ändern möchten. Wenn Sie das Tool IP ändern verwenden, werden DHCP-Adressen statisch.

Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen)

- 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 sich außerhalb des für die HA-Gruppe konfigurierten Subnetzes befindet.
- Sie können die Client-Netzwerk-IP-Adresse nicht in den Wert einer vorhandenen virtuellen IP-Adresse ändern, die einer HA-Gruppe zugewiesen ist, die auf der Client-Netzwerk-Schnittstelle konfiguriert ist.
- Wenn eine Grid-Netzwerkschnittstelle in einer HA-Gruppe vorhanden ist, können Sie die Grid-Netzwerk-IP-Adresse für diese Schnittstelle nicht in eine Adresse ändern, die sich außerhalb des für die HA-Gruppe konfigurierten Subnetzes befindet.
- 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.

Ändern der Node-Netzwerkconfiguration

Mit dem Change IP-Tool können Sie die Netzwerkkonfiguration für einen oder mehrere Knoten ändern. Sie können die Konfiguration des Grid-Netzwerks ändern oder den Administrator- oder Client-Netzwerk hinzufügen, ändern oder entfernen.

Bevor Sie beginnen

Sie haben die `passwords.txt` Datei:

Über diese Aufgabe

Linux: Wenn Sie zum ersten Mal einen Grid-Knoten zum Admin-Netzwerk oder Client-Netzwerk hinzufügen und SIE IN der Node-Konfigurationsdatei NOCH nicht `ADMIN_NETWORK_TARGET` oder `CLIENT_NETWORK_TARGET` konfiguriert haben, müssen Sie dies jetzt tun.

Weitere Informationen finden Sie in der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem:

- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)

Appliances: bei StorageGRID Appliances, wenn das Client- oder Admin-Netzwerk während der Erstinstallation nicht im StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann das Netzwerk nicht nur mit dem Change IP-Tool hinzugefügt werden. Zunächst müssen Sie ["Stellen Sie das Gerät in den Wartungsmodus"](#), Konfigurieren Sie die Links, stellen Sie die Appliance in den normalen Betriebsmodus zurück, und verwenden Sie dann das Change IP-Tool, um die Netzwerkkonfiguration zu ändern. Siehe ["Verfahren zum Konfigurieren von Netzwerkverbindungen"](#).

Sie können die IP-Adresse, die Subnetzmaske, das Gateway oder den MTU-Wert für einen oder mehrere Knoten in einem Netzwerk ändern.

Sie können auch einen Knoten aus einem Client-Netzwerk oder aus einem Admin-Netzwerk hinzufügen oder

entfernen:

- Sie können einem Client-Netzwerk oder einem Admin-Netzwerk einen Knoten hinzufügen, indem Sie dem Knoten eine IP-Adresse/Subnetzmaske hinzufügen.
- Sie können einen Knoten aus einem Client-Netzwerk oder aus 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.



Das Austauschen von IP-Adressen ist nicht zulässig. Wenn Sie IP-Adressen zwischen Grid-Nodes austauschen müssen, müssen Sie eine temporäre IP-Adresse verwenden.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist und Sie die IP-Adresse eines Admin-Knotens ändern, ist zu beachten, dass jedes Vertrauen, das mit der IP-Adresse des Admin-Knotens konfiguriert wurde (anstelle des vollständig qualifizierten Domännennamens, wie empfohlen), ungültig wird. Sie können sich nicht mehr bei dem Node anmelden. Unmittelbar nach dem Ändern der IP-Adresse müssen Sie das Vertrauen des Knotens in Active Directory Federation Services (AD FS) mit der neuen IP-Adresse aktualisieren oder neu konfigurieren. Siehe Anweisungen für "[SSO wird konfiguriert](#)".



Alle Änderungen, die Sie mit dem Change IP-Tool an das Netzwerk vornehmen, werden an die Installer-Firmware für die StorageGRID-Appliances übertragen. Auf diese Weise wird bei einer erneuten Installation der StorageGRID Software auf einer Appliance oder beim Einsatz einer Appliance in den Wartungsmodus die Netzwerkkonfiguration korrekt ausgeführt.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie das Change IP-Tool mit folgendem Befehl: `change-ip`
3. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase 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 optional **1** aus, um die zu aktualisierenden Knoten auszuwählen. Wählen Sie dann eine der folgenden Optionen aus:

- **1:** Einzelner Knoten — nach Namen auswählen
- **2:** Single Node — Wählen Sie nach Standort, dann nach Name
- **3:** Single Node — Wählen Sie 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 bleiben.

Nachdem Sie Ihre Auswahl getroffen haben, wird das Hauptmenü angezeigt, wobei das Feld **Ausgewählte Knoten** aktualisiert wird, um Ihre Auswahl zu berücksichtigen. Alle nachfolgenden Aktionen werden nur auf den angezeigten Nodes ausgeführt.

5. Wählen Sie im Hauptmenü die 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:** Netznetz
- **2:** Admin-Netzwerk
- **3:** Client-Netzwerk
- **4:** Alle Netzwerke nach der Auswahl zeigt die Eingabeaufforderung den Knotennamen, den Netzwerknamen (Grid, Admin oder Client), den Datentyp (IP/Maske, Gateway oder MTU) und aktueller Wert.

Wenn Sie die IP-Adresse, die Präfixlänge, das Gateway oder die MTU einer DHCP-konfigurierten Schnittstelle bearbeiten, wird die Schnittstelle zu statisch geändert. Wenn Sie eine durch DHCP konfigurierte Schnittstelle ändern möchten, wird eine Warnung angezeigt, die Sie darüber informiert, dass sich die Schnittstelle in statisch ändert.

Als konfigurierte Schnittstellen `fixed` Kann nicht bearbeitet werden.

- b. Um einen neuen Wert festzulegen, geben Sie ihn in das für den aktuellen Wert angezeigte Format ein.
- c. Um den aktuellen Wert unverändert zu lassen, drücken Sie **Enter**.
- d. Wenn der Datentyp ist `IP/mask`, Sie können 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 so lange gespeichert, bis sie gelöscht oder angewendet wurden.

- 6. Überprüfen Sie Ihre Änderungen, indem Sie eine der folgenden Optionen auswählen:

- **5**: Zeigt Edits in der Ausgabe an, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe dargestellt:
- **6**: Zeigt Änderungen in der Ausgabe an, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert.



Bestimmte Befehlszeilenschnittstellen zeigen möglicherweise Ergänzungen und Löschungen mithilfe von durchgestrichelter Formatierung. Die richtige Anzeige hängt von Ihrem Terminalclient ab, der die erforderlichen VT100-Escape-Sequenzen unterstützt.

- 7. Wählen Sie Option **7**, um alle Änderungen zu validieren.

Durch diese Validierung wird sichergestellt, dass die Regeln für Grid-, Admin- und Client-Netzwerke, z. B. die Verwendung überlappender Subnetze, nicht verletzt werden.

In diesem Beispiel ergab die Validierung Fehler.

In diesem Beispiel wurde die Validierung erfolgreich bestanden.

- 8. Wenn die Validierung erfolgreich abgeschlossen ist, wählen Sie eine der folgenden Optionen:

- **8**: Speichern Sie nicht angewendete Änderungen.

Mit dieser Option können Sie das Tool IP ändern beenden und es später erneut starten, ohne dabei unangewendete Änderungen zu verlieren.

- **10**: Die neue Netzwerkkonfiguration anwenden.

- 9. Wenn Sie die Option **10** ausgewählt haben, wählen Sie eine der folgenden Optionen:

- **Apply**: Die Änderungen sofort anwenden und bei Bedarf automatisch jeden Knoten neu starten.

Wenn für die neue Netzwerkkonfiguration keine Änderungen am physischen Netzwerk erforderlich sind, können Sie **Apply** auswählen, um die Änderungen sofort anzuwenden. Nodes werden bei Bedarf automatisch neu gestartet. Knoten, die neu gestartet werden müssen, werden angezeigt.

- **Stufe**: Beim nächsten manuellen Neustart der Knoten die Änderungen anwenden.

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 Änderungen am physischen Netzwerk vornehmen und die betroffenen Knoten neu starten. Wenn Sie **Apply** wählen, ohne zuvor diese Netzwerkänderungen vornehmen zu müssen, schlagen die Änderungen normalerweise fehl.



Wenn Sie die Option **Stage** verwenden, müssen Sie den Knoten nach der Staging so schnell wie möglich neu starten, um Störungen zu minimieren.

- **Cancel:** Nehmen Sie zu diesem Zeitpunkt keine Netzwerkänderungen vor.

Wenn Sie nicht wissen, dass für die vorgeschlagenen Änderungen ein Neustart von Nodes erforderlich ist, können Sie die Änderungen verschieben, um die Auswirkungen für den Benutzer zu minimieren. Mit der Option **Cancel** gelangen Sie zurück zum Hauptmenü und erhalten Ihre Änderungen, damit Sie sie später anwenden können.

Wenn Sie **Apply** oder **Stage** auswählen, wird eine neue Netzwerkkonfigurationsdatei generiert, die Bereitstellung durchgeführt und Knoten mit neuen Arbeitsinformationen aktualisiert.

Während der Bereitstellung wird der Status bei der Anwendung von Aktualisierungen angezeigt.

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

Nach dem Anwenden oder Staging von Änderungen wird ein neues Wiederherstellungspaket als Ergebnis der Änderung der Grid-Konfiguration generiert.

10. Wenn Sie **Phase** ausgewählt haben, führen Sie nach Abschluss der Bereitstellung folgende Schritte aus:
 - a. Nehmen Sie die erforderlichen Änderungen am physischen oder virtuellen Netzwerk vor.

Physische Netzwerkänderungen: Nehmen Sie die erforderlichen Änderungen an der physischen Netzwerkumgebung vor, und fahren Sie den Knoten bei Bedarf sicher herunter.

Linux: Wenn Sie den Knoten zum ersten Mal einem Admin-Netzwerk oder Client-Netzwerk hinzufügen, stellen Sie sicher, dass Sie die Schnittstelle wie unter beschrieben hinzugefügt haben "[Linux: Hinzufügen von Schnittstellen zu vorhandenem Node](#)".

- a. Starten Sie die betroffenen Knoten neu.

11. Wählen Sie **0** aus, um das Change IP-Tool nach Abschluss der Änderungen zu beenden.
12. Laden Sie ein neues Wiederherstellungspaket aus dem Grid Manager herunter.
 - a. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
 - b. Geben Sie die Provisionierungs-Passphrase ein.

Verwandte Informationen

["SGF6112 Storage Appliances"](#)

["SG6000 Storage-Appliances"](#)

["SG5700 Storage-Appliances"](#)

["SG100- und SG1000-Services-Appliances"](#)

Fügen Sie zu Subnetzlisten im Admin-Netzwerk hinzu oder ändern Sie diese

Sie können die Subnetze in der Subnetz-Liste Admin-Netzwerk eines oder mehrerer Nodes hinzufügen, löschen oder ändern.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei:

Sie können Subnetze zu allen Nodes in der Subnetz-Liste des Admin-Netzwerks hinzufügen, löschen oder ändern.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie das Change IP-Tool mit folgendem Befehl: `change-ip`
3. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase 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. Optional können Sie auch die Netzwerke/Nodes begrenzen, auf denen Vorgänge ausgeführt werden. Folgenden Optionen wählbar:
 - Wählen Sie die Knoten aus, die Sie bearbeiten möchten, indem Sie **1** wählen, wenn Sie bestimmte Knoten filtern möchten, auf denen der Vorgang ausgeführt werden soll. Wählen Sie eine der folgenden Optionen:
 - **1:** Einzelner Knoten (nach Namen auswählen)
 - **2:** Einzelner Knoten (nach Standort auswählen, dann nach Name)
 - **3:** Einzelner Knoten (nach aktueller IP auswählen)
 - **4:** Alle Knoten an einem Standort

- **5**: Alle Knoten im Raster
- **0**: Zurück

◦ Die Option „all“ bleibt aktiviert. Nach der Auswahl wird der Hauptmenü-Bildschirm angezeigt. Das Feld „Ausgewählte Knoten“ gibt Ihre neue Auswahl wieder. Nun 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. Folgenden Optionen wählbar:

- 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 mit diesem Format mehrere Adressen eingeben: `add CIDR, CIDR`

Beispiel: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Sie können den erforderlichen Tippaufwand reduzieren, indem Sie „Pfeil nach oben“ verwenden, um zuvor eingegebene Werte an die aktuelle Eingabeaufforderung abzurufen und diese gegebenenfalls zu bearbeiten.

Im folgenden Beispiel werden Subnetze zur Subnetz-Liste des Admin-Netzwerks hinzugefügt:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

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

DK-10-224-5-20-G1
 10.0.0.0/8
 172.19.0.0/16
 172.21.0.0/16
 172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. Wenn Sie bereit sind, geben Sie **q** ein, um zum Hauptmenü-Bildschirm zurückzukehren. Ihre Änderungen werden so lange gespeichert, bis sie gelöscht oder angewendet wurden.



Wenn Sie in Schritt 2 einen der "alle" Knotenauswahlmodi ausgewählt haben, drücken Sie **Enter** (ohne **q**), um zum nächsten Knoten in der Liste zu gelangen.

8. Folgenden Optionen wählbar:

- Wählen Sie die Option **5**, um Änderungen in der Ausgabe anzuzeigen, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Zusätze) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe unten gezeigt:

- Wählen Sie die Option **6**, um Änderungen in der Ausgabe anzuzeigen, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert. **Hinweis:** bestimmte Terminalemulatoren könnten Ergänzungen und Löschungen mit durchgestrichelter Formatierung anzeigen.

Wenn Sie versuchen, die Subnetz-Liste 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-Servernetze nicht speziell einem Netzwerk zugewiesen haben, erstellt StorageGRID automatisch eine Host-Route (/32) für die Verbindung. Wenn Sie beispielsweise eine /16- oder /24-Route für eine ausgehende Verbindung zu einem DNS- oder NTP-Server verwenden möchten, sollten Sie die automatisch erstellte /32-Route löschen und die gewünschten Routen hinzufügen. Wenn Sie die automatisch erstellte Hostroute nicht löschen, wird sie nach der Anwendung von Änderungen an der Subnetzliste erhalten.



Sie können diese automatisch erkannten Host-Routen verwenden, aber im Allgemeinen sollten Sie die DNS- und NTP-Routen manuell konfigurieren, um die Konnektivität zu gewährleisten.

9. Wählen Sie Option **7**, um alle stufenweisen Änderungen zu validieren.

Diese Validierung stellt sicher, dass die Regeln für Grid, Admin und Client-Netzwerke befolgt werden, z. B. die Verwendung überlappender Subnetze.

10. Wählen Sie optional die Option **8**, um alle Änderungen in der Stufenschicht zu speichern und später zurückzukehren, um die Änderungen fortzusetzen.

Mit dieser Option können Sie das Tool IP ändern beenden und es später erneut starten, ohne dabei unangewendete Änderungen zu verlieren.

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 des Provisioning wird der Status als Aktualisierung angezeigt, 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 aus dem Grid Manager herunter.
 - a. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
 - b. Geben Sie die Provisionierungs-Passphrase ein.

Fügen Sie zu Subnetzlisten im Grid-Netzwerk hinzu oder ändern Sie diese

Mithilfe des Tools IP ändern können Sie Subnetze im Grid Network hinzufügen oder ändern.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei:

Sie können Subnetze in der Netznetznetznetznetznetznetzsubnetzliste hinzufügen, löschen oder ändern. Änderungen wirken sich auf das Routing aller Knoten im Raster aus.



Wenn Sie nur Änderungen an der Netznetzwerksubnetz-Liste vornehmen, verwenden Sie den Grid-Manager, um die Netzwerkkonfiguration hinzuzufügen oder zu ändern. Verwenden Sie andernfalls das Change IP-Tool, wenn der Grid Manager aufgrund eines Netzwerkkonfigurationsproblem nicht erreichbar ist, oder Sie führen gleichzeitig eine Änderung des Grid Network Routing und andere Netzwerkänderungen durch.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

2. Starten Sie das Change IP-Tool mit folgendem Befehl: `change-ip`
3. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase 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 Netznetzwerksubnetz-Liste sind im gesamten Grid verfügbar.

5. Folgenden Optionen wählbar:

- 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 mit diesem Format mehrere Adressen eingeben: `add CIDR, CIDR`

Beispiel: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Sie können den erforderlichen Tippaufwand reduzieren, indem Sie „Pfeil nach oben“ verwenden, um zuvor eingegebene Werte an die aktuelle Eingabeaufforderung abzurufen und diese gegebenenfalls zu bearbeiten.

Die unten stehende Beispieleingabe zeigt das Festlegen von Subnetzen für die Netzsubnetz-Liste:

6. Wenn Sie bereit sind, geben Sie `q` ein, um zum Hauptmenü-Bildschirm zurückzukehren. Ihre Änderungen werden so lange gespeichert, bis sie gelöscht oder angewendet wurden.

7. Folgenden Optionen wählbar:

- Wählen Sie die Option 5, um Änderungen in der Ausgabe anzuzeigen, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Zusätze) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe unten gezeigt:
- Wählen Sie die Option 6, um Änderungen in der Ausgabe anzuzeigen, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert.



Bestimmte Befehlszeilenschnittstellen zeigen möglicherweise Ergänzungen und Löschungen mithilfe von durchgestrichelter Formatierung.

8. Wählen Sie Option **7**, um alle stufenweisen Änderungen zu validieren.

Diese Validierung stellt sicher, dass die Regeln für Grid, Admin und Client-Netzwerke befolgt werden, z. B. die Verwendung überlappender Subnetze.

9. Wählen Sie optional die Option **8**, um alle Änderungen in der Stufenschicht zu speichern und später zurückzukehren, um die Änderungen fortzusetzen.

Mit dieser Option können Sie das Tool IP ändern beenden und es später erneut starten, ohne dabei unangewendete Änderungen zu verlieren.

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 des Provisioning wird der Status als Aktualisierung angezeigt, wie in der folgenden Beispielausgabe dargestellt:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

11. Wenn Sie beim Ändern des Grid-Netzwerks die Option **10** ausgewählt haben, wählen Sie eine der folgenden Optionen aus:

- **Apply**: Die Änderungen sofort anwenden und bei Bedarf automatisch jeden Knoten neu starten.

Wenn die neue Netzwerkkonfiguration ohne externe Änderungen gleichzeitig mit der alten Netzwerkkonfiguration funktioniert, können Sie die Option **Apply** für eine vollautomatische Konfigurationsänderung verwenden.

- **Stufe**: Beim nächsten Neustart der Knoten die Änderungen anwenden.

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 Änderungen am physischen Netzwerk vornehmen und die betroffenen Knoten neu starten.



Wenn Sie die Option **Stage** verwenden, starten Sie den Knoten so schnell wie möglich nach dem Staging neu, um Unterbrechungen zu minimieren.

- **Cancel**: Nehmen Sie zu diesem Zeitpunkt keine Netzwerkänderungen vor.

Wenn Sie nicht wissen, dass für die vorgeschlagenen Änderungen ein Neustart von Nodes erforderlich ist, können Sie die Änderungen verschieben, um die Auswirkungen für den Benutzer zu minimieren. Mit der Option **Cancel** gelangen Sie zurück zum Hauptmenü und erhalten Ihre Änderungen, damit Sie sie später anwenden können.

Nach dem Anwenden oder Staging von Änderungen wird ein neues Wiederherstellungspaket als Ergebnis

der Änderung der Grid-Konfiguration generiert.

12. Wenn die Konfiguration aufgrund von Fehlern angehalten wird, stehen folgende Optionen zur Verfügung:
- Um das IP-Änderungsverfahren zu beenden 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 erneut versucht werden, indem Sie im Hauptmenü die Option **10** (Änderungen übernehmen) wählen. Das IP-Änderungsverfahren wird erst abgeschlossen, wenn alle Vorgänge erfolgreich abgeschlossen wurden.

- Wenn Sie manuell eingreifen mussten (zum Beispiel um einen Knoten neu zu starten) und sich sicher sind, dass die Aktion, die das Tool für erfolgreich hält, tatsächlich erfolgreich abgeschlossen wurde, geben Sie **f** ein, um sie als erfolgreich zu markieren und zum nächsten Vorgang zu wechseln.

13. Laden Sie ein neues Wiederherstellungspaket aus dem Grid Manager herunter.

- Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
- Geben Sie die Provisionierungs-Passphrase ein.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

Ändern Sie die IP-Adressen für alle Nodes im Grid

Wenn Sie die Grid-Netzwerk-IP-Adresse für alle Knoten im Raster ändern müssen, müssen Sie dieses spezielle Verfahren befolgen. Sie können keine IP-Änderung für das Grid-weite Netzwerk durchführen, indem Sie das Verfahren zum Ändern einzelner Knoten verwenden.

Bevor Sie beginnen

- Sie haben die `passwords.txt` Datei:

Um sicherzustellen, dass das Raster erfolgreich gestartet wird, müssen Sie alle Änderungen gleichzeitig vornehmen.



Dieses Verfahren gilt nur für das Grid-Netzwerk. Sie können dieses Verfahren nicht zum Ändern von IP-Adressen in Admin- oder Client-Netzwerken verwenden.

Wenn Sie die IP-Adressen und die MTU nur für die Nodes an einem Standort ändern möchten, folgen Sie den "[Ändern der Node-Netzwerkkonfiguration](#)" Anweisungen.

Schritte

1. Planen Sie im Voraus, wenn Änderungen außerhalb des Tools zur Änderung der IP vorgenommen werden müssen, z. B. Änderungen an DNS oder NTP oder Änderungen an der SSO-Konfiguration (Single Sign On).



Wenn auf den neuen IP-Adressen nicht auf die vorhandenen NTP-Server für das Grid zugegriffen werden kann, fügen Sie die neuen NTP-Server hinzu, bevor Sie das Change-ip-Verfahren durchführen.



Wenn auf den neuen IP-Adressen nicht auf die vorhandenen DNS-Server für das Grid zugegriffen werden kann, fügen Sie die neuen DNS-Server hinzu, bevor Sie das Change-ip-Verfahren durchführen.



Wenn SSO für Ihr StorageGRID-System aktiviert ist und alle Vertrauensstellen, die sich auf Administratorknoten-IP-Adressen befinden, konfiguriert wurden (anstelle von vollständig qualifizierten Domännennamen, wie empfohlen), müssen Sie diese Vertrauensstellungen der betreffenden Partei in Active Directory Federation Services (AD FS) aktualisieren oder neu konfigurieren. Unmittelbar nach dem Ändern der IP-Adressen. Siehe "[Konfigurieren Sie Single Sign-On](#)".



Fügen Sie bei Bedarf das neue Subnetz für die neuen IP-Adressen hinzu.

2. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Starten Sie das Change IP-Tool mit folgendem Befehl: `change-ip`

4. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase ein.

Das Hauptmenü wird angezeigt. Standardmäßig wird der verwendet `Selected nodes` Feld ist auf festgelegt `all`.

```
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: █
```

5. Wählen Sie im Hauptmenü **2** aus, um IP/Subnetzmaske, Gateway und MTU-Informationen für alle Knoten zu bearbeiten.

- a. Wählen Sie **1**, um Änderungen am Grid-Netzwerk vorzunehmen.

Nach der Auswahl werden in der Eingabeaufforderung die Node-Namen, Grid Network Name, Datentyp (IP/Maske, Gateway oder MTU) angezeigt. Und aktuellen Werten.

Wenn Sie die IP-Adresse, die Präfixlänge, das Gateway oder die MTU einer DHCP-konfigurierten

Schnittstelle bearbeiten, wird die Schnittstelle zu statisch geändert. Vor jeder über DHCP konfigurierten Schnittstelle wird eine Warnung angezeigt.

Als konfigurierte Schnittstellen `fixed` Kann nicht bearbeitet werden.

- a. Um einen neuen Wert festzulegen, geben Sie ihn in das für den aktuellen Wert angezeigte Format ein.
- b. Nachdem Sie alle Knoten bearbeitet haben, die Sie ändern möchten, geben Sie **q** ein, um zum Hauptmenü zurückzukehren.

Ihre Änderungen werden so lange gespeichert, bis sie gelöscht oder angewendet wurden.

6. Überprüfen Sie Ihre Änderungen, indem Sie eine der folgenden Optionen auswählen:

- **5:** Zeigt Edits in der Ausgabe an, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe dargestellt:
- **6:** Zeigt Änderungen in der Ausgabe an, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert.



Bestimmte Befehlszeilenschnittstellen zeigen möglicherweise Ergänzungen und Löschungen mithilfe von durchgestrichelter Formatierung. Die richtige Anzeige hängt von Ihrem Terminalclient ab, der die erforderlichen VT100-Escape-Sequenzen unterstützt.

7. Wählen Sie Option **7**, um alle Änderungen zu validieren.

Diese Validierung stellt sicher, dass die Regeln für das Grid-Netzwerk, wie z. B. die Verwendung überlappender Subnetze, nicht verletzt werden.

In diesem Beispiel ergab die Validierung Fehler.

In diesem Beispiel wurde die Validierung erfolgreich bestanden.

8. Wenn die Validierung erfolgreich abgeschlossen ist, wählen Sie **10** aus, um die neue Netzwerkkonfiguration anzuwenden.

9. Wählen Sie **Stufe**, um die Änderungen beim nächsten Neustart der Knoten anzuwenden.



Sie müssen **Stufe** wählen. Führen Sie keinen Rolling-Neustart durch, entweder manuell oder durch Auswahl von **Apply** anstelle von **Stage**; das Raster wird nicht erfolgreich gestartet.

10. Wenn die Änderungen abgeschlossen sind, wählen Sie **0** aus, um das Change IP-Tool zu verlassen.

11. Fahren Sie alle Nodes gleichzeitig herunter.



Das gesamte Grid muss gleichzeitig heruntergefahren werden, um alle Nodes gleichzeitig ausgefallen zu sein.

12. Nehmen Sie die erforderlichen Änderungen am physischen oder virtuellen Netzwerk vor.

13. Vergewissern Sie sich, dass alle Grid-Nodes ausgefallen sind.

14. Schalten Sie alle Knoten ein.
15. Sobald das Raster erfolgreich gestartet wurde:
 - 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 aus dem Grid Manager herunter.
 - a. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
 - b. Geben Sie die Provisionierungs-Passphrase ein.

Verwandte Informationen

- ["Fügen Sie zu Subnetzlisten im Grid-Netzwerk hinzu oder ändern Sie diese"](#)
- ["Fahren Sie den Grid-Node herunter"](#)

Fügen Sie Schnittstellen zum vorhandenen Node hinzu

Linux: Hinzufügen von Admin- oder Client-Schnittstellen zu einem bestehenden Knoten

Führen Sie diese Schritte aus, um einen Linux-Knoten nach der Installation eine Schnittstelle im Admin-Netzwerk oder im Client-Netzwerk hinzuzufügen.

Wenn SIE WÄHREND der Installation IN der Node-Konfigurationsdatei auf dem Linux-Host NICHT ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET konfiguriert haben, verwenden Sie dieses Verfahren, um die Schnittstelle hinzuzufügen. Weitere Informationen zur Node-Konfigurationsdatei finden Sie in den Anweisungen für Ihr Linux-Betriebssystem:

- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)

Sie führen diese Schritte auf dem Linux-Server durch, der den Node hostet, der die neue Netzwerkzuweisung benötigt, nicht innerhalb des Nodes. Bei diesem Vorgang wird die Schnittstelle nur dem Knoten hinzugefügt. Ein Validierungsfehler tritt auf, wenn Sie versuchen, andere Netzwerkparameter anzugeben.

Um Adressinformationen bereitzustellen, müssen Sie das Werkzeug IP ändern verwenden. Siehe ["Ändern der Node-Netzwerkconfiguration"](#).

Schritte

1. Melden Sie sich beim Linux-Server an, auf dem der Node gehostet wird.
2. Bearbeiten Sie die Konfigurationsdatei des Knotens: `/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 Node-Validier-Befehl aus:

```
sudo storagegrid node validate node-name
```

4. Beheben Sie alle Validierungsfehler.
5. Führen Sie den Befehl zum erneuten Laden des Node aus:

```
sudo storagegrid node reload node-name
```

Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node

Nach der Installation können Sie einem Linux-Knoten zusätzliche Trunk- oder Zugangsschnittstellen hinzufügen. Die fügen Sie Schnittstellen hinzu, werden auf der Seite VLAN-Schnittstellen und auf der Seite HA-Gruppen angezeigt.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anweisungen für die Installation von StorageGRID auf Ihrer Linux-Plattform.
 - ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
 - ["Installieren Sie Ubuntu oder Debian"](#)
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, einem Node Schnittstellen hinzuzufügen, während ein Software-Upgrade, ein Recovery-Verfahren oder ein Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Verwenden Sie diese Schritte, um einem Linux-Knoten eine oder mehrere zusätzliche Schnittstellen hinzuzufügen, nachdem der Knoten installiert wurde. Beispielsweise möchten Sie einem Admin oder Gateway Node eine Trunk-Schnittstelle hinzufügen, sodass Sie den Datenverkehr zwischen verschiedenen Applikationen oder Mandanten über VLAN-Schnittstellen trennen können. Oder auch, wenn Sie eine Access-Schnittstelle hinzufügen möchten, um sie in einer HA-Gruppe (High Availability, Hochverfügbarkeit) zu verwenden.

Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.

Der Node ist für kurze Zeit nicht verfügbar, wenn Sie Schnittstellen hinzufügen. Sie sollten dieses Verfahren auf jeweils einem Knoten durchführen.

Schritte

1. Melden Sie sich beim Linux-Server an, auf dem der Node gehostet wird.
2. Bearbeiten Sie mit einem Texteditor wie vim oder pico die Konfigurationsdatei des Knotens:

```
/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 Node hinzufügen möchten. Verwenden Sie dieses Format.

```
INTERFACE_TARGET_nnnn=value
```

Geben Sie für *nnnn* eine eindeutige Zahl für jede ein `INTERFACE_TARGET` Eintrag, den Sie hinzufügen.

Geben Sie unter *value* 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 an, 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 Node-Konfigurationsdatei zu validieren:

```
sudo storagegrid node validate node-name
```

Beheben Sie Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

5. Führen Sie den folgenden Befehl aus, um die Konfiguration des Node zu aktualisieren:

```
sudo storagegrid node reload node-name
```

Nachdem Sie fertig sind

- Wenn Sie eine oder mehrere Trunk-Schnittstellen hinzugefügt haben, gehen Sie zu ["Konfigurieren Sie die VLAN-Schnittstellen"](#) So konfigurieren Sie eine oder mehrere VLAN-Schnittstellen für jede neue übergeordnete Schnittstelle:
- Wenn Sie eine oder mehrere Access Interfaces hinzugefügt haben, gehen Sie zu ["Konfigurieren Sie Hochverfügbarkeitsgruppen"](#) Um die neuen Schnittstellen direkt zu HA-Gruppen hinzuzufügen.

VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node

Nach der Installation des Node können Sie einem VM-Node eine Trunk- oder Zugriffsschnittstelle hinzufügen. Die fügen Sie Schnittstellen hinzu, werden auf der Seite VLAN-Schnittstellen und auf der Seite HA-Gruppen angezeigt.

Bevor Sie beginnen

- Sie haben Zugriff auf die Anweisungen für ["Installation von StorageGRID auf Ihrer VMware-Plattform"](#).
- Sie haben virtuelle Admin-Node- und Gateway-Node-VMware-Maschinen.
- Sie haben ein Netzwerk-Subnetz, das nicht als Grid, Admin oder Client-Netzwerk verwendet wird.
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, einem Node Schnittstellen hinzuzufügen, während ein Software-Upgrade, ein Recovery-Verfahren oder ein Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Verwenden Sie diese Schritte, um einem VMware Node nach der Installation des Node mindestens eine zusätzliche Schnittstelle hinzuzufügen. Beispielsweise möchten Sie einem Admin oder Gateway Node eine Trunk-Schnittstelle hinzufügen, sodass Sie den Datenverkehr zwischen verschiedenen Applikationen oder

Mandanten über VLAN-Schnittstellen trennen können. Oder Sie möchten vielleicht eine Zugriffsoberfläche hinzufügen, die in einer HA-Gruppe (High Availability, Hochverfügbarkeit) verwendet werden soll.

Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsschnittstelle hinzufügen, können Sie die Schnittstelle direkt einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.

Der Node ist möglicherweise für einen kurzen Zeitraum nicht verfügbar, wenn Sie Schnittstellen hinzufügen.

Schritte

1. Fügen Sie in vCenter einen neuen Netzwerkadapter (Typ VMXNET3) zu einer Admin-Node- und Gateway-Node-VM hinzu. Aktivieren Sie die Kontrollkästchen * Verbunden* und * Verbinden beim Einschalten*.

Network adapter 4 *	CLIENT683_old_vlan	Connected
Status	<input checked="" type="checkbox"/> Connect At Power On	
Adapter Type	VMXNET 3	
DirectPath I/O	<input checked="" type="checkbox"/> Enable	

2. Verwenden Sie SSH, um sich beim Admin-Node oder Gateway-Node anzumelden.
3. Nutzung `ip link show` Um zu überprüfen, ob 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
```

Nachdem Sie fertig sind

- Wenn Sie eine oder mehrere Trunk-Schnittstellen hinzugefügt haben, gehen Sie zu ["Konfigurieren Sie die VLAN-Schnittstellen"](#) So konfigurieren Sie eine oder mehrere VLAN-Schnittstellen für jede neue übergeordnete Schnittstelle:
- Wenn Sie eine oder mehrere Access Interfaces hinzugefügt haben, gehen Sie zu ["Konfigurieren Sie Hochverfügbarkeitsgruppen"](#) Um die neuen Schnittstellen direkt zu HA-Gruppen hinzuzufügen.

Konfigurieren Sie DNS-Server

Sie können DNS-Server hinzufügen, aktualisieren und entfernen, sodass Sie statt IP-Adressen vollständig qualifizierte Domännennamen (FQDN) verwenden können.

Wenn Sie bei der Angabe von Hostnamen für externe Ziele vollständig qualifizierte Domännennamen (FQDNs) anstelle von IP-Adressen verwenden möchten, geben Sie die IP-Adresse jedes DNS-Servers an, den Sie verwenden möchten. Diese Einträge werden für AutoSupport, Warn-E-Mails, SNMP-Benachrichtigungen, Plattform-Services-Endpunkte, Cloud-Storage-Pools, Und vieles mehr.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Berechtigung für Wartung oder Root-Zugriff](#)".
- Sie haben die IP-Adressen der zu konfigurierenden DNS-Server.

Über diese Aufgabe

Um einen ordnungsgemäßen Betrieb zu gewährleisten, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, können aufgrund bekannter Einschränkungen des Betriebssystems auf einigen Plattformen nur drei verwendet werden. Wenn in Ihrer Umgebung Routing-Einschränkungen bestehen, können Sie dies tun "[Passen Sie die DNS-Serverliste an](#)" Für einzelne Knoten (in der Regel alle Knoten an einem Standort) einen anderen Satz von bis zu drei DNS-Servern verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein Inselstandort die FQDNs für externe Ziele auflösen kann.

Fügen Sie einen DNS-Server hinzu

Führen Sie die folgenden Schritte aus, um einen DNS-Server hinzuzufügen.

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > DNS-Server**.
2. Wählen Sie **Add another Server**, um einen DNS-Server hinzuzufügen.
3. Wählen Sie **Speichern**.

Ändern Sie einen DNS-Server

Führen Sie die folgenden Schritte aus, 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 Sie einen DNS-Server

Gehen Sie wie folgt vor, um eine IP-Adresse eines DNS-Servers zu löschen.

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > DNS-Server**.

2. Klicken Sie auf das Löschsymbol  Neben der IP-Adresse.
3. Wählen Sie **Speichern**.

Ändern der DNS-Konfiguration für einen einzelnen Grid-Node

Anstatt den DNS global für die gesamte Bereitstellung zu konfigurieren, können Sie ein Skript ausführen, um DNS für jeden Grid-Knoten anders zu konfigurieren.

Im Allgemeinen sollten Sie die Option **MAINTENANCE > Network > DNS Servers** im Grid Manager verwenden, um DNS-Server zu konfigurieren. Verwenden Sie das folgende Skript nur, wenn Sie unterschiedliche DNS-Server für unterschiedliche Grid-Nodes verwenden müssen.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.
 - e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
 - f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
2. Melden Sie sich beim 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 einen Domänennamendienst für Ihr Netzwerk bereitstellt: `add <nameserver IP_address>`
5. Wiederholen Sie den `add nameserver` Befehl zum Hinzufügen von Nameserver.
6. Befolgen Sie die Anweisungen, wenn Sie dazu aufgefordert werden, weitere Befehle einzugeben.
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 Grid-Node die Schritte von [Anmeldung beim Node](#) Bis [Schließen der Befehlsshell](#).

10. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein: `ssh-add -D`

Managen von NTP-Servern

Sie können NTP-Server (Network Time Protocol) hinzufügen, aktualisieren oder entfernen, um sicherzustellen, dass die Daten zwischen den Grid-Nodes im StorageGRID-System genau synchronisiert werden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Berechtigung für Wartung oder Root-Zugriff](#)".
- Sie haben die Provisionierungs-Passphrase.
- Sie verfügen über die IPv4-Adressen der zu konfigurierenden NTP-Server.

Verwendung von NTP durch StorageGRID

Das StorageGRID System verwendet das Network Time Protocol (NTP) zur Synchronisierung der Zeit zwischen allen Grid-Nodes im Grid.

Jedem Standort werden mindestens zwei Nodes im StorageGRID-System die primäre NTP-Rolle zugewiesen. Sie synchronisieren sich mit einem vorgeschlagenen Minimum von vier und maximal sechs externen Zeitquellen und miteinander. Jeder Node im StorageGRID System, der kein primärer NTP-Node ist, fungiert als NTP-Client und synchronisiert mit diesen primären NTP-Nodes.

Die externen NTP-Server stellen eine Verbindung zu den Nodes her, mit denen Sie zuvor primäre NTP-Rollen zugewiesen haben. Aus diesem Grund wird empfohlen, mindestens zwei Nodes mit primären NTP-Rollen anzugeben.

NTP-Server-Richtlinien

Beachten Sie die folgenden Richtlinien, um sich vor Zeitproblemen zu schützen:

- Die externen NTP-Server stellen eine Verbindung zu den Nodes her, mit denen Sie zuvor primäre NTP-Rollen zugewiesen haben. Aus diesem Grund wird empfohlen, mindestens zwei Nodes mit primären NTP-Rollen anzugeben.
- Stellen Sie sicher, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid 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 Zeitdrift zu vermeiden.



Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer älteren Windows-Version als Windows Server 2016. Der Zeitservice früherer Versionen von Windows ist nicht ausreichend genau und wird von Microsoft nicht für den Einsatz in hochgenauen Umgebungen, einschließlich StorageGRID, unterstützt. Weitere Informationen finden Sie unter "[Begrenzung des Supports, um Windows Time Service für hochpräzise Umgebungen zu konfigurieren](#)".

Konfigurieren Sie NTP-Server

Führen Sie die folgenden Schritte aus, um NTP-Server hinzuzufügen, zu aktualisieren oder zu entfernen.

Schritte

1. Wählen Sie **MAINTENANCE > Network > NTP-Server**.
2. Fügen Sie im Abschnitt Server bei Bedarf NTP-Servereinträge hinzu, aktualisieren oder entfernen Sie sie.

Sie sollten mindestens vier NTP-Server angeben, und Sie können bis zu sechs Server angeben.

3. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System ein, und wählen Sie dann **Speichern**.

Die Seite wird deaktiviert, bis die Konfigurationsaktualisierungen abgeschlossen sind.



Wenn alle NTP-Server den Verbindungstest nach dem Speichern der neuen NTP-Server nicht bestehen, fahren Sie nicht fort. Wenden Sie sich an den technischen Support.

Beheben von Problemen mit dem NTP-Server

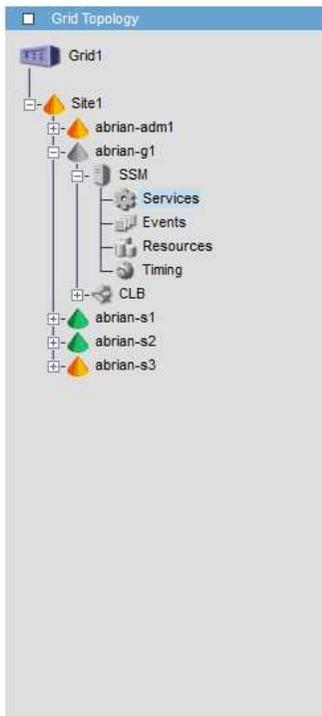
Wenn Probleme mit der Stabilität oder Verfügbarkeit der NTP-Server auftreten, die ursprünglich während der Installation angegeben wurden, können Sie die Liste der externen NTP-Quellen, die das StorageGRID-System verwendet, aktualisieren oder entfernen Sie vorhandene Server.

Stellt die Netzwerkverbindung für isolierte Knoten wieder her

Unter bestimmten Umständen, z. B. Änderungen an der IP-Adresse für Standort oder das gesamte Grid, kann sich eine oder mehrere Node-Gruppen möglicherweise nicht an den Rest des Grid wenden.

Über diese Aufgabe

Wenn im Grid Manager (**SUPPORT > Tools > Grid Topology**) ein Knoten grau ist oder wenn ein Knoten blau ist und viele seiner Dienste einen anderen Status als ausgeführt aufweisen, sollten Sie nach einer Knotenisolierung suchen.



Overview
Alarms
Reports
Configuration

Main

Overview: SSM (abrian-g1) - Services
Updated: 2018-01-23 15:03:45 MST

Operating System: Linux 4.9.0-3-amd64

Services

Service	Version	Status	Threads	Load	Memory
ADE Exporter Service	11.1.0-20171214.1441.c29e2f8	Running	11	0.011 %	7.87 MB
Connection Load Balancer (CLB)	11.1.0-20180120.011f.02137fe	Running	61	0.07 %	39.3 MB
Dynamic IP Service	11.1.0-20180123.1919.deeeba7.abrian	Not Running	0	0 %	0 B
Nginx Service	1.10.3-1+deb9u1	Running	5	0.002 %	20 MB
Node Exporter Service	0.13.0+ds-1+b2	Running	5	0 %	8.58 MB
Persistence Service	11.1.0-20180123.1919.deeeba7.abrian	Running	6	0.064 %	17.1 MB
Server Manager	11.1.0-20171214.1441.c29e2f8	Running	4	2.116 %	18.7 MB
Server Status Monitor (SSM)	11.1.0-20180120.011f.02137fe	Running	61	0.288 %	45.8 MB
System Logging	3.8.1-10	Running	3	0.006 %	8.27 MB
Time Synchronization	1:4.2.8p10+dfsg-3+deb9u1	Running	2	0.007 %	4.54 MB

Packages

Package	Installed	Version
storage-grid-release	Installed	11.1.0-20180123.1919.deeeba7.abrian

Isolierte Nodes haben einige der Folgen:

- Wenn mehrere Knoten isoliert sind, können Sie sich möglicherweise nicht bei Grid Manager anmelden oder auf diesen zugreifen.
- Wenn mehrere Nodes isoliert sind, sind möglicherweise die im Dashboard für den Mandanten-Manager angezeigten Werte für Speichernutzung und Kontingent nicht mehr aktuell. Die Gesamtwerte 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-Node enthält) ein Befehlszeilen-Dienstprogramm aus, das vom Raster isoliert ist. Das Dienstprogramm stellt den Knoten die IP-Adresse eines nicht isolierten Knotens im Raster zur Verfügung, sodass der isolierte Knoten oder die Gruppe der Knoten das gesamte Raster erneut kontaktieren kann.



Wenn das Multicast-Domännennamensystem (mDNS) in den Netzwerken deaktiviert ist, muss das Befehlszeilendienstprogramm möglicherweise auf jedem isolierten Knoten ausgeführt werden.

Schritte

1. Auf den Knoten zugreifen und überprüfen `/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 sie eine Meldung, dass der Node möglicherweise isoliert ist.

Bei Linux-Bereitstellungen werden in Isolationsmeldungen angezeigt
/var/log/storagegrid/node/<nodename>.log Dateien:

2. Wenn die Isolationsmeldungen immer wieder und dauerhaft sind, führen Sie den folgenden Befehl aus:

```
add_node_ip.py <address>
```

Wo <address> Ist die IP-Adresse eines Remote-Node, 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 zuvor isolierten Node:

- Die Services des Knotens wurden gestartet.
- Der Status des Dynamic IP-Dienstes lautet „running“, nachdem Sie den ausgeführt haben `storagegrid-status` Befehl.
- In der Struktur Grid Topology erscheint der Knoten nicht mehr vom Rest des Rasters getrennt.



Wenn Sie den ausführen `add_node_ip.py` Der Befehl löst das Problem nicht, es können weitere Netzwerkprobleme auftreten, die gelöst werden müssen.

Verfahren auf Host-Ebene und Middleware

Linux: Migrieren des Grid-Node zu neuem Host

Sie können einen oder mehrere StorageGRID-Knoten von einem Linux-Host (dem *source-Host*) zu einem anderen Linux-Host (dem *target-Host*) migrieren, um die Hostwartung durchzuführen, ohne die Funktionalität oder Verfügbarkeit Ihres Grids zu beeinträchtigen.

Angenommen, Sie möchten einen Node migrieren, um Patching und Neubooten des Betriebssystems durchzuführen.

Bevor Sie beginnen

- Sie planen Ihre StorageGRID-Implementierung, um den Migrations-Support einzubeziehen.
 - ["Anforderungen für die Migration von Node-Containern für Red hat Enterprise Linux oder CentOS"](#)
 - ["Node Container Migration Anforderungen für Ubuntu oder Debian"](#)
- Der Zielhost ist bereits für die Verwendung mit StorageGRID vorbereitet.
- Shared Storage wird für alle Storage Volumes pro Node verwendet
- Netzwerkschnittstellen verfügen über konsistente Namen aller Hosts.



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Storage Node auf einem einzelnen Host aus. Die Verwendung eines dedizierten Hosts für jeden Speicherknoten stellt eine isolierte Ausfalldomäne zur Verfügung.

Andere Node-Typen, wie beispielsweise Admin-Nodes oder Gateway-Nodes, können auf demselben Host implementiert werden. Wenn Sie jedoch mehrere Nodes desselben Typs (z. B. zwei Gateway-Nodes) haben, installieren Sie nicht alle Instanzen auf demselben Host.

Knoten vom Quellhost exportieren

Fahren Sie zunächst den Grid-Knoten herunter und exportieren Sie ihn vom Linux-Quellhost.

Führen Sie die folgenden Befehle auf dem *source Host* aus.

Schritte

1. Abrufen des Status aller derzeit auf dem Quell-Host ausgeführten Nodes

```
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. Geben Sie den Namen des Node an, den Sie migrieren möchten, und beenden Sie ihn, wenn sein Ausführungsstatus ausgeführt wird.

```
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 Quell-Host.

```
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.

Im nächsten Schritt führen Sie diesen Befehl auf dem Zielhost aus.

Knoten auf Zielhost importieren

Nachdem Sie den Node vom Quellhost exportiert haben, importieren und validieren Sie den Node auf dem Zielhost. Die Validierung bestätigt, dass der Knoten Zugriff auf denselben Block-Speicher und Netzwerkschnittstellengeräte hat, wie er auf dem Quell-Host hatte.

Führen Sie die folgenden Befehle auf dem *target Host* 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 der Node-Konfiguration 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 der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem.

- ["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)
- ["Installieren Sie Ubuntu oder Debian"](#)

Migrierten Knoten starten

Nachdem Sie den migrierten Node validiert haben, starten Sie den Node, indem Sie einen Befehl auf dem *target Host* ausführen.

Schritte

1. Starten Sie den Knoten auf dem neuen Host.

```
sudo storagegrid node start DC1-S3
```

2. Melden Sie sich beim Grid-Manager an, und überprüfen Sie, ob der Status des Node grün ist, ohne dass eine Warnmeldung ausgegeben wird.



Überprüfen, ob der Status des Node grün lautet, stellt sicher, dass der migrierte Node vollständig neu gestartet und wieder dem Grid beigetreten ist. Wenn der Status nicht grün lautet, migrieren Sie keine zusätzlichen Nodes, damit nicht mehr als ein Node außer Betrieb ist.

3. Wenn Sie nicht auf den Grid Manager zugreifen können, warten Sie 10 Minuten, und führen Sie den folgenden Befehl aus:

```
sudo storagegrid node status _node-name
```

Vergewissern Sie sich, dass der migrierte Node den Status „Ausführen“ hat.

Wartung von Archivierungs-Nodes für TSM Middleware

Archive Nodes sind möglicherweise für Tapes über einen TSM Middleware-Server oder die Cloud über die S3-API konfiguriert. Nach der Konfiguration kann das Ziel eines Archive Node nicht mehr geändert werden.

Wenn der Server, der den Archivknoten hostet, ausfällt, ersetzen Sie den Server, und befolgen Sie den entsprechenden Wiederherstellungsvorgang.

Fehler bei Archivgeräten

Wenn Sie feststellen, dass ein Fehler beim Archivspeichergerät vorliegt, auf das der Archivknoten über Tivoli Storage Manager (TSM) zugreift, schalten Sie den Archivknoten offline, um die Anzahl der im StorageGRID-System angezeigten Alarme zu begrenzen. Anschließend können Sie das Problem mit den administrativen Tools des TSM-Servers, des Speichergeräts oder beidem weiter diagnostizieren und lösen.

Versetzen Sie die Zielkomponente in den Offline-Modus

Bevor Sie eine Wartung des TSM Middleware-Servers durchführen, der dazu führen kann, dass der Knoten „Archiv“ nicht mehr verfügbar ist, nehmen Sie die Zielkomponente offline, um die Anzahl der Alarme zu begrenzen, die ausgelöst werden, wenn der TSM Middleware-Server nicht mehr verfügbar ist.

Bevor Sie beginnen

Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.

2. Wählen Sie **Archivknoten > ARC > Ziel > Konfiguration > Haupt**.
3. Ändern Sie den Wert für Tivoli Storage Manager Status in **Offline** und klicken Sie auf **Änderungen anwenden**.
4. Nachdem die Wartung abgeschlossen ist, ändern Sie den Wert des Tivoli Storage Manager-Status in **Online** und klicken Sie auf **Änderungen übernehmen**.

Administrative Tools für Tivoli Storage Manager

Das dsmadm Tool ist die Administrationskonsole für den TSM Middleware-Server, der auf dem Archiv-Knoten installiert ist. Sie können auf das Tool zugreifen, indem Sie eingeben `dsmadm` In der Befehlszeile des Servers. Melden Sie sich an der Verwaltungskonsole mit demselben administrativen Benutzernamen und Kennwort an, das für den ARC-Dienst konfiguriert ist.

Der `tsmquery.rb` Skript wurde erstellt, um Statusinformationen aus `dsmadm` in lesbarer Form zu generieren. Sie können dieses Skript ausführen, indem Sie den folgenden Befehl in der Befehlszeile des Archiv-Knotens eingeben: `/usr/local/arc/tsmquery.rb status`

Weitere Informationen zur TSM Administrationskonsole `dsmadm` finden Sie im *Tivoli Storage Manager für Linux: Administrator's Reference*.

Objekt dauerhaft nicht verfügbar

Wenn der Archivknoten ein Objekt vom Tivoli Storage Manager (TSM)-Server anfordert und der Abruf fehlschlägt, versucht der Archivknoten die Anforderung nach einem Intervall von 10 Sekunden erneut. Wenn das Objekt dauerhaft nicht verfügbar ist (z. B. weil das Objekt auf Band beschädigt ist), kann die TSM-API dies nicht auf den Archiv-Node hinweisen, sodass der Archivknoten die Anforderung weiterhin erneut versucht.

Wenn diese Situation eintritt, wird ein Alarm ausgelöst, und der Wert steigt weiter. Um den Alarm anzuzeigen, wählen Sie **SUPPORT > Tools > Gittertopologie**. Wählen Sie dann **Archivknoten > ARC > Retrieve > Fehler anfordern**.

Wenn das Objekt dauerhaft nicht verfügbar ist, müssen Sie das Objekt identifizieren und die Anfrage des Archivierungs-Nodes manuell abbrechen, wie in der Prozedur beschrieben. [Bestimmen, ob Objekte dauerhaft nicht verfügbar sind](#).

Ein Abruf kann auch fehlschlagen, wenn das Objekt vorübergehend nicht verfügbar ist. In diesem Fall sollten nachfolgende Abrufanfragen erfolgreich sein.

Wenn das StorageGRID System für die Verwendung einer ILM-Regel konfiguriert ist, die eine einzelne Objektkopie erstellt und diese Kopie nicht abgerufen werden kann, geht das Objekt verloren und kann nicht wiederhergestellt werden. Sie müssen jedoch weiterhin das Verfahren befolgen, um festzustellen, ob das Objekt zum Entfernen von `` zum StorageGRID-System dauerhaft nicht verfügbar ist, zum Abbrechen der Anfrage des Archivknotens und zum Löschen von Metadaten für das verlorene Objekt.

Bestimmen, ob Objekte dauerhaft nicht verfügbar sind

Sie können feststellen, ob Objekte dauerhaft nicht verfügbar sind, indem Sie eine Anforderung über die TSM-Administrationskonsole erstellen.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die `Passwords.txt` Datei:

- Sie haben die IP-Adresse eines Admin-Knotens.

Über diese Aufgabe

Dieses Beispiel dient als Informationsmaterial. Mit diesem Verfahren können Sie nicht alle Fehlerbedingungen identifizieren, die zu nicht verfügbaren Objekten oder Bandvolumen führen können. Informationen zur TSM-Administration finden Sie in der TSM-Server-Dokumentation.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Identifizieren Sie das Objekt oder die Objekte, die nicht vom Archiv-Node abgerufen werden konnten:
 - a. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält: `cd /var/local/audit/export`

Die aktive Audit-Log-Datei heißt `Audit.log`. Einmal am Tag, die aktive `audit.log` Die 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`. Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt `yyyy-mm-dd.txt.gz`, Die das ursprüngliche Datum bewahrt.

- b. Durchsuchen Sie die entsprechende Audit-Log-Datei nach Meldungen, die darauf hinweisen, dass ein archiviertes Objekt nicht abgerufen werden konnte. Geben Sie beispielsweise Folgendes ein: `grep ARCE audit.log | less -n`

Wenn ein Objekt nicht von einem Archivknoten abgerufen werden kann, wird in DER ARCE-Überwachungsmeldung (Archivobjekt abrufen Ende) ARUN (ArchivMiddleware nicht verfügbar) oder GERR (allgemeiner Fehler) im Ergebnisfeld angezeigt. Die folgende Beispielzeile aus dem Audit-Protokoll zeigt, dass die ARCE-Meldung mit dem Ergebnis ARUN für CBID 498D8A1F681F05B3 beendet wurde.

```
[AUDT: [CBID (UI64) :0x498D8A1F681F05B3] [VLID (UI64) :□20091127] [RSLT (FC32) : ARUN] [AVER (UI32) : 7]
[ATIM (UI64) :1350613602969243] [ATYP (FC32) :ARCE] [ANID (UI32) :13959984] [AMID (FC32) :ARCI]
[ATID (UI64) :4560349751312520631]]
```

Weitere Informationen finden Sie in den Anweisungen zum Verständnis von Überwachungsmeldungen.

- c. Notieren Sie die CBID jedes Objekts, bei dem ein Anforderungsfehler auftritt.

Möglicherweise möchten Sie auch die folgenden zusätzlichen Informationen aufzeichnen, die vom TSM zur Identifizierung von Objekten verwendet werden, die vom Archiv-Node gespeichert wurden:

- **Dateiplatzname:** Entspricht der Archiv-Knoten-ID. Um die Archiv-Knoten-ID zu finden, wählen Sie **SUPPORT > Tools > Grid Topology**. Wählen Sie dann **Archivknoten > ARC > Ziel > Übersicht**.
- **Hoher Level Name:** Entspricht der Volume-ID, die dem Objekt durch den Archiv-Node zugewiesen wurde. Die Volume-ID hat die Form eines Datums (z. B. 20091127), und wird als VLID des Objekts in Archiv-Audit-Nachrichten aufgezeichnet.

- **Name der unteren Ebene:** Entspricht der CBID, die einem Objekt vom StorageGRID-System zugewiesen wurde.

d. Melden Sie sich aus der Befehlsshell ab: `exit`

3. Überprüfen Sie den TSM-Server, ob die in Schritt 2 identifizierten Objekte dauerhaft nicht verfügbar sind:

a. Melden Sie sich bei der Administrationskonsole des TSM-Servers an: `dsmadmc`

Verwenden Sie den für den ARC-Dienst konfigurierten administrativen Benutzernamen und das für den ARC-Dienst konfigurierte Passwort. Geben Sie den Benutzernamen und das Kennwort in den Grid Manager ein. (Um den Benutzernamen anzuzeigen, wählen Sie **SUPPORT > Tools > Grid Topology**. Wählen Sie dann **Archivknoten > ARC > Ziel > Konfiguration**.)

b. Stellen Sie fest, ob das Objekt dauerhaft nicht verfügbar ist.

Beispielsweise können Sie im TSM-Aktivitätsprotokoll nach einem Datenintegritätsfehler für das Objekt suchen. Das folgende Beispiel zeigt eine Suche des Aktivitätsprotokolls für den letzten Tag nach einem Objekt mit CBID 498D8A1F681F05B3.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

Je nach Art des Fehlers kann die CBID nicht im TSM-Aktivitätsprotokoll aufgezeichnet werden. Zum Zeitpunkt des Fehlers der Anforderung müssen Sie möglicherweise das Protokoll nach anderen TSM-Fehlern durchsuchen.

c. Wenn ein ganzes Band dauerhaft nicht verfügbar ist, identifizieren Sie die CBIDs für alle Objekte, die auf diesem Volume gespeichert sind: `query content TSM_Volume_Name`

Wo `TSM_Volume_Name` ist der TSM-Name für das nicht verfügbare Band. Im Folgenden finden Sie ein Beispiel für die Ausgabe dieses Befehls:

```
> query content TSM-Volume-Name
Node Name      Type Filespace  FSID Client's Name for File Name
-----
DEV-ARC-20     Arch /19130020    216 /20081201/ C1D172940E6C7E12
DEV-ARC-20     Arch /19130020    216 /20081201/ F1D7FBC2B4B0779E
```

Der `Client's Name for File Name` Entspricht der Archiv-Node-Volume-ID (oder TSM „High-Level Name“), gefolgt von der CBID des Objekts (oder TSM „Low-Level-Name“). Das ist, das `Client's Name for File Name` Nimmt das Formular an `/Archive Node volume ID /CBID`. In der ersten Zeile der Beispielausgabe wird der angezeigt `Client's Name for File Name` ist `/20081201/ C1D172940E6C7E12`.

Erinnern Sie sich auch daran, dass die `Filespace` Ist die Knoten-ID des Archiv-Knotens.

Sie benötigen die CBID jedes auf dem Volume gespeicherten Objekts und die Node-ID des Archiv-Node, um die Anforderung zum Abrufen abzubrechen.

4. Brechen Sie bei jedem Objekt, das dauerhaft nicht verfügbar ist, die Abfrage ab, und geben Sie einen Befehl ein, um das StorageGRID System über den Verlust der Objektkopie zu informieren:



Verwenden Sie die ADE-Konsole vorsichtig. Wenn die Konsole nicht ordnungsgemäß verwendet wird, können Systemvorgänge und beschädigte Daten unterbrochen werden. Geben Sie Befehle sorgfältig ein, und verwenden Sie nur die in diesem Verfahren dokumentierten Befehle.

- a. Wenn Sie noch nicht beim Archivknoten angemeldet sind, melden Sie sich wie folgt an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

- b. Zugriff auf die ADE-Konsole des ARC-Dienstes: `telnet localhost 1409`

- c. Abbrechen der Anfrage für das Objekt: `/proc/BRTR/cancel -c CBID`

Wo `CBID` Ist die Kennung des Objekts, das nicht vom TSM abgerufen werden kann.

Wenn sich die einzigen Kopien des Objekts auf Band befinden, wird die Anforderung „Bulk refrain“ mit einer Nachricht abgebrochen, „1 Requests stornierte“. Wenn Kopien des Objekts an anderer Stelle im System vorhanden sind, wird der Objektabruf durch ein anderes Modul verarbeitet, sodass die Antwort auf die Nachricht „0 Requests stornierte“ lautet.

- d. Geben Sie einen Befehl ein, um das StorageGRID System darüber zu informieren, dass eine Objektkopie verloren gegangen ist und dass weitere Kopien erstellt werden müssen:

`/proc/CMSI/Object_Lost CBID node_ID`

Wo `CBID` Ist die Kennung des Objekts, das nicht vom TSM-Server abgerufen werden kann, und `node_ID` Ist die Knoten-ID des Archiv-Knotens, bei dem der Abruf fehlgeschlagen ist.

Sie müssen einen separaten Befehl für jede verlorene Objektkopie eingeben: Die Eingabe eines Bereichs von CBIDs wird nicht unterstützt.

In den meisten Fällen erstellt das StorageGRID System sofort zusätzliche Kopien von Objektdaten, um sicherzustellen, dass die ILM-Richtlinie des Systems befolgt wird.

Wenn jedoch in der ILM-Regel für das Objekt angegeben wurde, dass nur eine Kopie erstellt wurde und diese Kopie jetzt verloren gegangen ist, kann das Objekt nicht wiederhergestellt werden. In diesem Fall die ausführen `Object_Lost` Der Befehl bereinigt die Metadaten des verlorenen Objekts aus dem StorageGRID System.

Wenn der `Object_Lost` Befehl wurde erfolgreich abgeschlossen, die folgende Meldung wird zurückgegeben:

```
CLOC_LOST_ANS returned result 'SUCS'
```

+



Der `/proc/CMSI/Object_Lost` Der Befehl ist nur für verlorene Objekte gültig, die auf Archiv-Knoten gespeichert sind.

- a. Verlassen Sie die ADE-Konsole: `exit`
 - b. Melden Sie sich vom Archiv-Knoten ab: `exit`
5. Zurücksetzen des Werts von Anfragefehlern im StorageGRID System:
- a. Gehen Sie zu **Archivknoten > ARC > Retrieve > Konfiguration**, und wählen Sie **Fehleranzahl der Anfrage zurücksetzen**.
 - b. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

["StorageGRID verwalten"](#)

["Prüfung von Audit-Protokollen"](#)

VMware: Virtuelle Maschine für automatischen Neustart konfigurieren

Wenn die virtuelle Maschine nach dem Neustart des VMware vSphere-Hypervisors nicht neu gestartet wird, müssen Sie die virtuelle Maschine möglicherweise für den automatischen Neustart konfigurieren.

Führen Sie diese Schritte aus, wenn Sie bemerken, dass eine virtuelle Maschine nicht neu gestartet wird, während Sie einen Grid-Knoten wiederherstellen oder einen anderen Wartungsvorgang ausführen.

Schritte

1. Wählen Sie in der VMware vSphere Client-Struktur die virtuelle Maschine aus, die nicht gestartet wurde.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, und wählen Sie **Einschalten**.
3. Konfigurieren Sie den VMware vSphere Hypervisor, um die virtuelle Maschine in Zukunft automatisch neu zu starten.

Verfahren für den Grid-Node

Grid Node Procedures: Übersicht

Möglicherweise müssen Sie auf einem bestimmten Grid-Node Verfahren durchführen. Sie können zwar einige dieser Verfahren im Grid Manager ausführen, jedoch müssen Sie bei den meisten Verfahren von der Befehlszeile des Knotens aus auf Server Manager zugreifen.

Server Manager wird auf jedem Grid-Knoten ausgeführt, um das Starten und Beenden von Diensten zu überwachen und sicherzustellen, dass Dienste problemlos dem StorageGRID-System beitreten und das System verlassen. Server Manager überwacht auch die Dienste auf jedem Grid-Knoten und versucht automatisch, alle Services, die Fehler melden, neu zu starten.



Sie sollten auf Server Manager zugreifen, wenn Sie von technischem Support dazu aufgefordert wurden.



Sie müssen die aktuelle Shell-Sitzung des Befehls schließen und sich ausloggen, nachdem Sie mit Server Manager fertig sind. Geben Sie Ein: `exit`

Zeigen Sie den Status und die Version von Server Manager an

Für jeden Grid-Node können Sie den aktuellen Status und die Version des auf diesem Grid-Node ausgeführten Server Managers anzeigen. Zudem erhalten Sie den aktuellen Status aller auf diesem Grid-Node ausgeführten Services.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als `root` angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Anzeigen des aktuellen Status von Server Manager, der auf dem Grid-Node ausgeführt wird: **`service servermanager status`**

Der aktuelle Status von Server Manager, der auf dem Grid-Knoten ausgeführt wird, wird gemeldet (wird ausgeführt oder nicht). Wenn der Status von Server Manager lautet `running`, Die Zeit, die es seit dem letzten Start läuft, ist aufgelistet. Beispiel:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Zeigen Sie die aktuelle Version von Server Manager an, der auf einem Grid-Node ausgeführt wird: **`service servermanager version`**

Die aktuelle Version wird aufgelistet. Beispiel:

```
11.1.0-20180425.1905.39c9493
```

4. Melden Sie sich aus der Befehlshell ab: **`exit`**

Den aktuellen Status aller Dienste anzeigen

Sie können jederzeit den aktuellen Status aller auf einem Grid-Node ausgeführten

Services anzeigen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

Beispielsweise zeigt die Ausgabe für den primären Admin-Node den aktuellen Status der AMS-, CMN- und NMS-Dienste als ausgeführt an. Diese Ausgabe wird sofort aktualisiert, wenn sich der Status eines Dienstes ändert.

```
Host Name          190-ADM1
IP Address
Operating System Kernel  4.9.0      Verified
Operating System Environment  Debian 9.4  Verified
StorageGRID Webscale Release  11.1.0     Verified
Networking          Verified
Storage Subsystem    Verified
Database Engine      5.5.9999+default Running
Network Monitoring   11.1.0     Running
Time Synchronization  1:4.2.8p10+dfsg Running
ams                  11.1.0     Running
cmn                  11.1.0     Running
nms                  11.1.0     Running
ssm                  11.1.0     Running
mi                   11.1.0     Running
dynip                11.1.0     Running
nginx                1.10.3     Running
tomcat               8.5.14     Running
grafana              4.2.0      Running
mgmt api             11.1.0     Running
prometheus           1.5.2+ds   Running
persistence          11.1.0     Running
ade exporter         11.1.0     Running
attrDownPurge        11.1.0     Running
attrDownSamp1        11.1.0     Running
attrDownSamp2        11.1.0     Running
node exporter        0.13.0+ds  Running
```

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Optional können Sie einen statischen Bericht für alle Dienste anzeigen, die auf dem Grid-Node ausgeführt werden: `/usr/local/servermanager/reader.rb`

Dieser Bericht enthält dieselben Informationen wie der ständig aktualisierte Bericht, wird jedoch nicht aktualisiert, wenn sich der Status eines Dienstes ändert.

5. Melden Sie sich aus der Befehlsshell ab: `exit`

Starten Sie Server Manager und alle Dienste

Möglicherweise müssen Sie Server Manager starten, der auch alle Dienste auf dem Grid-Knoten startet.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Der Start von Server Manager auf einem Grid-Knoten, auf dem er bereits ausgeführt wird, führt zu einem Neustart des Server-Managers und aller Dienste auf dem Grid-Knoten.

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Server Manager Starten: `service servermanager start`
3. Melden Sie sich aus der Befehlsshell ab: `exit`

Starten Sie Server Manager und alle Services neu

Möglicherweise müssen Sie den Server-Manager und alle Dienste, die auf einem Grid-Knoten ausgeführt werden, neu starten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie Server Manager und alle Services auf dem Grid-Knoten neu: `service servermanager restart`

Server Manager und alle Dienste auf dem Grid-Knoten werden angehalten und dann neu gestartet.



Verwenden der `restart` Der Befehl ist der gleiche wie mit dem `stop` Befehl gefolgt vom `start` Befehl.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Beenden Sie Server Manager und alle Dienste

Server Manager ist dafür gedacht, immer ausgeführt zu werden, aber möglicherweise müssen Sie Server Manager und alle Dienste, die auf einem Grid-Knoten ausgeführt werden, anhalten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Stoppen Sie Server Manager und alle Services, die auf dem Grid-Knoten ausgeführt werden: `service servermanager stop`

Server Manager und alle auf dem Grid-Knoten ausgeführten Dienste werden ordnungsgemäß beendet. Das Herunterfahren des Services kann bis zu 15 Minuten dauern.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Zeigt den aktuellen Servicestatus an

Sie können jederzeit den aktuellen Status einer auf einem Grid-Node ausgeführten Services anzeigen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als `root` angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Den aktuellen Status eines Dienstes anzeigen, der auf einem Grid-Knoten ausgeführt wird:
``Service_servicename_ Status` der aktuelle Status des angeforderten Dienstes, der auf dem Grid-Knoten ausgeführt wird, wird gemeldet (wird ausgeführt oder nicht). Beispiel:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Dienst stoppen

Einige Wartungsvorgänge erfordern, dass Sie einen einzelnen Service beenden und gleichzeitig andere Services auf dem Grid-Node ausgeführt werden. Stoppen Sie nur einzelne Dienste, wenn Sie dazu durch ein Wartungsverfahren angewiesen werden.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Wenn Sie mit diesen Schritten einen Dienst „administrativ stoppen“ beenden, startet der Server Manager den Dienst nicht automatisch neu. Sie müssen entweder den einzelnen Dienst manuell starten oder Server Manager neu starten.

Wenn Sie den LDR-Dienst auf einem Speicherknoten anhalten müssen, beachten Sie, dass es möglicherweise eine Weile dauern kann, bis der Dienst beendet wird, wenn aktive Verbindungen vorhanden sind.

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als `root` angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Beenden eines einzelnen Dienstes: `service servicename stop`

Beispiel:

```
service ldr stop
```



Der Service kann bis zu 11 Minuten dauern.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

["Dienst zum Beenden erzwingen"](#)

Stellen Sie das Gerät in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Berechtigung `Wartung` oder `Stammzugriff`. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Über diese Aufgabe

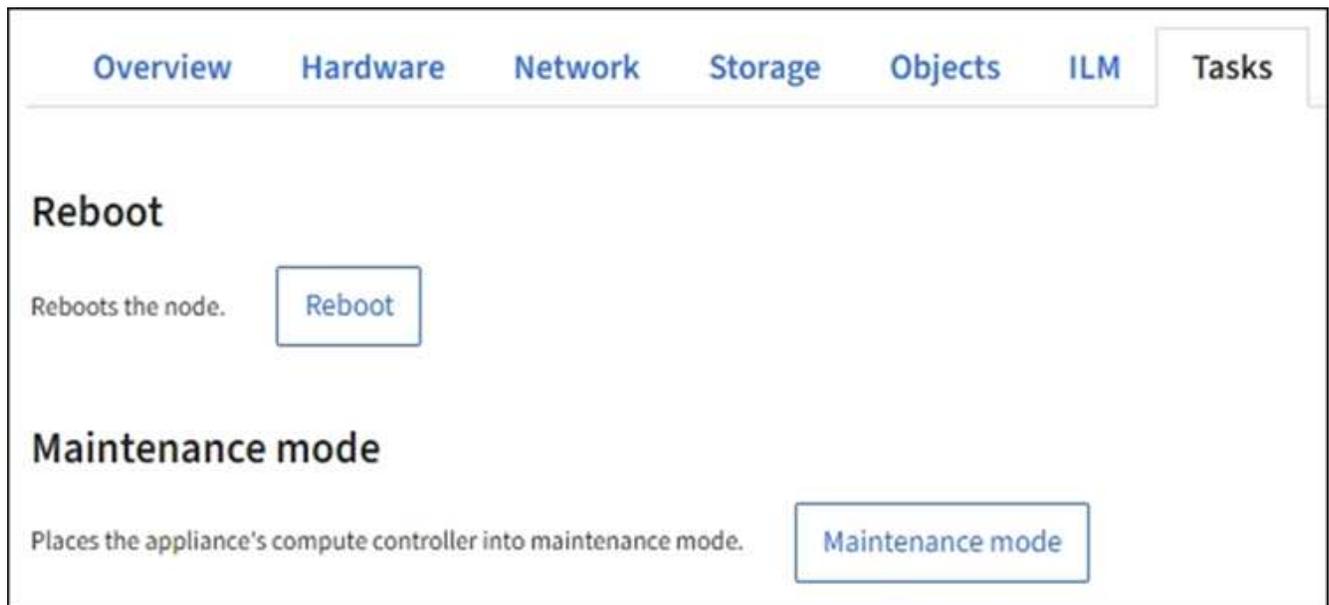
In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den Wartungsmodus versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.



Das Passwort des Admin-Kontos und die SSH-Host-Schlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem Kennwort, das zum Zeitpunkt der Wartung der Appliance vorhanden war.

Schritte

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie in der Strukturansicht der Seite Knoten den Appliance Storage Node aus.
3. Wählen Sie **Aufgaben**.



4. Wählen Sie **Wartungsmodus**. Ein Bestätigungsdialogfeld wird angezeigt.
5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

Eine Fortschrittsleiste und eine Reihe von Meldungen, darunter „Anfrage gesendet“, „StorageGRID

stoppen“ und „neu booten“, geben an, dass die Appliance die Schritte zum Eintritt in den Wartungsmodus abschließt.

Wenn sich die Appliance im Wartungsmodus befindet, wird in einer Bestätigungsmeldung die URLs aufgeführt, mit denen Sie auf das Installationsprogramm der StorageGRID-Appliance zugreifen können.

i This node is currently in maintenance mode. Navigate to one of the URLs listed below and perform any necessary maintenance procedures.

- <https://172.16.2.24:8443>
- <https://10.224.2.24:8443>

When you are done with any required maintenance procedures, you must exit maintenance mode by selecting Reboot Controller from the StorageGRID Appliance Installer.

6. Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.



Zugriff Auf <https://169.254.0.1:8443> Erfordert eine direkte Verbindung zum lokalen Management-Port.

7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im Wartungsmodus befindet.

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to [reboot](#) the controller.

8. Führen Sie alle erforderlichen Wartungsaufgaben durch.

9. Beenden Sie nach Abschluss der Wartungsaufgaben den Wartungsmodus und fahren Sie den normalen Node-Betrieb fort. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Controller neu starten** aus, und wählen Sie dann **Neustart in StorageGRID** aus.

NetApp® StorageGRID® Appliance Installer

Home	Configure Networking ▾	Configure Hardware ▾	Monitor Installation	Advanced ▾
------	------------------------	----------------------	----------------------	------------

Reboot Controller
Request a controller reboot.

RAID Mode

Upgrade Firmware

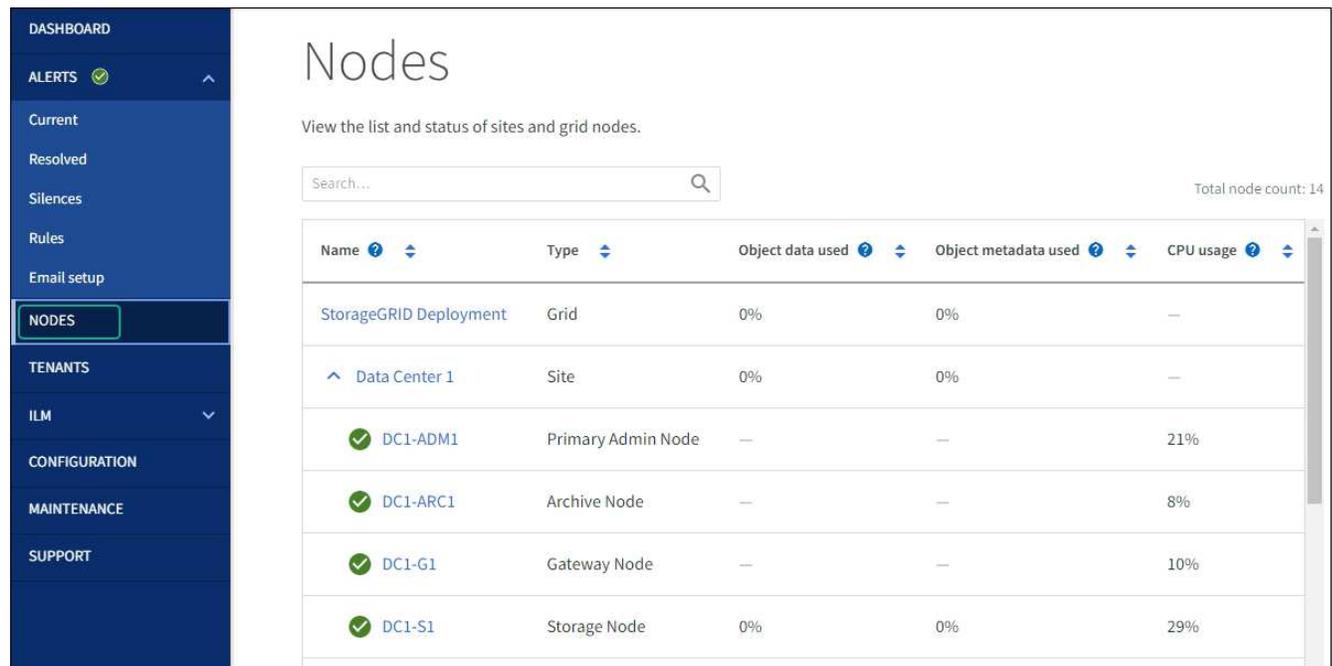
Reboot Controller

Reboot into StorageGRID

Reboot into Maintenance Mode

Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird.

Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **Knoten** sollte ein normaler Status angezeigt werden (grünes Häkchen-Symbol  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.



Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	21%
 DC1-ARC1	Archive Node	—	—	8%
 DC1-G1	Gateway Node	—	—	10%
 DC1-S1	Storage Node	0%	0%	29%

Dienst zum Beenden erzwingen

Wenn Sie einen Dienst sofort beenden müssen, können Sie den `force-stop` Befehl.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Erzwingen Sie den Dienst manuell zum Beenden: `service servicename force-stop`

Beispiel:

```
service ldr force-stop
```

Das System wartet 30 Sekunden, bevor der Dienst beendet wird.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Dienst starten oder neu starten

Möglicherweise müssen Sie einen Dienst starten, der angehalten wurde, oder Sie müssen einen Dienst anhalten und neu starten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Entscheiden Sie, welcher Befehl das Problem verursacht, basierend darauf, ob der Service derzeit ausgeführt oder angehalten ist.

- Wenn der Dienst derzeit angehalten ist, verwenden Sie das `start` Befehl zum manuellen Starten des Dienstes: `service servicename start`

Beispiel:

```
service ldr start
```

- Wenn der Dienst derzeit ausgeführt wird, verwenden Sie das `restart` Befehl, um den Dienst zu beenden und ihn dann neu zu starten: `service servicename restart`

Beispiel:

```
service ldr restart
```

+



Verwenden der `restart` Der Befehl ist der gleiche wie mit dem `stop` Befehl gefolgt vom `start` Befehl. Sie können ein Problem lösen `restart` Selbst wenn der Dienst derzeit angehalten ist.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Entfernen Sie die Port-Remaps

Wenn Sie einen Endpunkt für den Load Balancer-Dienst konfigurieren möchten und einen Port verwenden möchten, der bereits als Port mit dem Port einer Port-Remap konfiguriert wurde, müssen Sie zunächst die vorhandene Port-Remap entfernen, oder der Endpunkt ist nicht wirksam. Sie müssen auf jedem Admin-Node und Gateway-Node ein Skript ausführen, das über widersprüchliche neu zugeordnete Ports verfügt, um alle Port-Remaps des Node zu entfernen.

Über diese Aufgabe

Durch dieses Verfahren werden alle Port-Remaps entfernt. Wenden Sie sich an den technischen Support, wenn Sie einige der Rückpläne aufbewahren müssen.

Informationen zum Konfigurieren von Endpunkten für den Load Balancer finden Sie unter "[Konfigurieren von Load Balancer-Endpunkten](#)".



Wenn die Port-Neuzuordnung Client-Zugriff ermöglicht, konfigurieren Sie den Client neu, damit er einen anderen Port als Load-Balancer-Endpunkt verwendet, um einen Dienstausfall zu vermeiden. Andernfalls führt das Entfernen der Port-Zuordnung zum Verlust des Client-Zugriffs und sollte entsprechend geplant werden.



Dieses Verfahren ist bei einem StorageGRID System, das als Container auf Bare-Metal-Hosts bereitgestellt wird, nicht möglich. Siehe Anweisungen für "[Entfernen von Port-Remaps auf Bare-Metal-Hosts](#)".

Schritte

1. Melden Sie sich bei dem Node an.

a. Geben Sie den folgenden Befehl ein: `ssh -p 8022 admin@node_IP`

Port 8022 ist der SSH-Port des Basis-OS, während Port 22 der SSH-Port der Container-Engine ist, auf der StorageGRID ausgeführt wird.

b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Führen Sie das folgende Skript aus: `remove-port-remap.sh`

3. Booten Sie den Node neu.

Befolgen Sie die Anweisungen für "[Neubooten eines Grid-Node](#)".

4. Wiederholen Sie diese Schritte auf jedem Admin-Node und Gateway-Node mit gegensätzlichen neu zugeordneten Ports.

Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts

Wenn Sie einen Endpunkt für den Load Balancer-Dienst konfigurieren möchten und einen

Port verwenden möchten, der bereits als Port mit dem Port einer Port-Remap konfiguriert wurde, müssen Sie zunächst die vorhandene Port-Remap entfernen, oder der Endpunkt ist nicht wirksam.

Über diese Aufgabe

Wenn Sie StorageGRID auf Bare-Metal-Hosts ausführen, führen Sie dieses Verfahren anstelle des allgemeinen Verfahrens zum Entfernen von Port-Remaps durch. Sie müssen die Node-Konfigurationsdatei für jeden Admin-Node und Gateway-Node bearbeiten, der über widersprüchliche neu zugeordnete Ports verfügt, um alle Port-Neuzuordnungen des Node zu entfernen und den Node neu zu starten.



Durch dieses Verfahren werden alle Port-Remaps entfernt. Wenden Sie sich an den technischen Support, wenn Sie einige der Rückpläne aufbewahren müssen.

Informationen über das Konfigurieren von Endpunkten für den Load Balancer finden Sie in den Anweisungen zur Verwaltung von StorageGRID.



Dieses Verfahren kann zu einem vorübergehenden Serviceverlust führen, wenn Knoten neu gestartet werden.

Schritte

1. Melden Sie sich bei dem Host an, der den Node unterstützt. Melden Sie sich als root oder mit einem Konto an, das über sudo-Berechtigung verfügt.
2. Führen Sie den folgenden Befehl aus, um den Node vorübergehend zu deaktivieren: `sudo storagegrid node stop node-name`
3. Bearbeiten Sie mithilfe eines Texteditors wie vim oder pico die Konfigurationsdatei des Knotens für den Knoten.

Die Konfigurationsdatei des Knotens ist unter zu finden `/etc/storagegrid/nodes/node-name.conf`.

4. Suchen Sie den Abschnitt der Node-Konfigurationsdatei, die die Port-Zuordnungen 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-Remaps zu entfernen.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Führen Sie den folgenden Befehl aus, um Ihre Änderungen an der Node-Konfigurationsdatei für den Node zu validieren: `sudo storagegrid node validate node-name`

Beheben Sie Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

7. Führen Sie den folgenden Befehl aus, um den Node ohne Port-Zuordnungen neu zu starten: `sudo storagegrid node start node-name`
8. Loggen Sie sich als Administrator beim Node mit dem im angegebenen Passwort ein `Passwords.txt` Datei:
9. Überprüfen Sie, ob die Dienste richtig starten.
- Anzeigen einer Liste der Status aller Dienste auf dem Server: `sudo storagegrid-status`

Der Status wird automatisch aktualisiert.

b. Warten Sie, bis alle Dienste den Status „wird ausgeführt“ oder „verifiziert“ aufweisen.

c. Statusbildschirm verlassen:Ctrl+C

10. Wiederholen Sie diese Schritte auf jedem Admin-Node und Gateway-Node mit gegensätzlichen neu zugeordneten Ports.

Grid-Node neu booten

Grid Node neu booten: Übersicht

Sie können einen Grid-Node aus dem Grid Manager oder aus der Befehlshaber des Node neu booten.

Beim Neubooten eines Grid-Node wird der Node heruntergefahren und neu gestartet. Alle Dienste werden automatisch neu gestartet.

Wenn Sie Storage-Nodes neu starten möchten, beachten Sie Folgendes:

- Wenn eine ILM-Regel das Aufnahmeverhalten von zwei Commits oder Balanced angibt und es nicht möglich ist, sofort alle erforderlichen Kopien zu erstellen, überträgt StorageGRID alle neu aufgenommenen Objekte sofort auf zwei Storage-Nodes an derselben Site und wertet ILM später aus. Wenn Sie zwei oder mehr Storage-Nodes an einem bestimmten Standort neu starten möchten, können Sie während des Neustarts möglicherweise nicht auf diese Objekte zugreifen.
- Um sicherzustellen, dass Sie während des Neubootens eines Storage-Node auf alle Objekte zugreifen können, beenden Sie die Verarbeitung von Objekten an einem Standort etwa eine Stunde lang, bevor Sie den Node neu booten.

Grid-Node aus Grid Manager neu booten

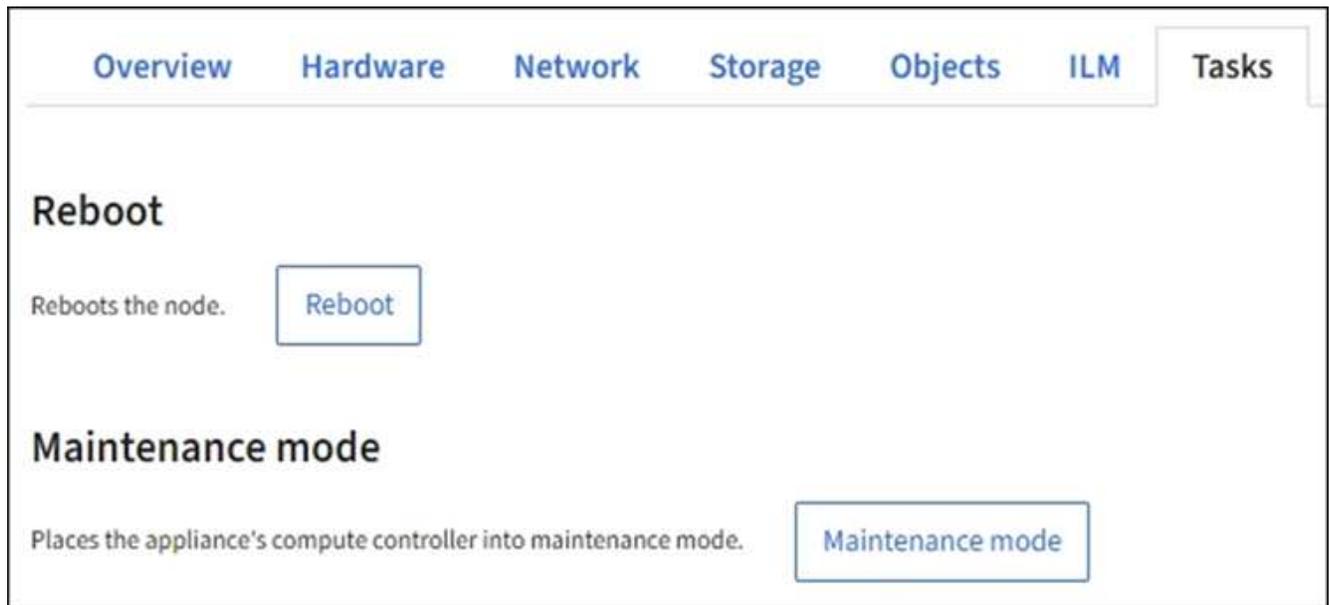
Beim Neubooten eines Grid-Node aus dem Grid Manager wird der Probleme auftreten `reboot` Befehl auf dem Ziel-Node.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben die Provisionierungs-Passphrase.

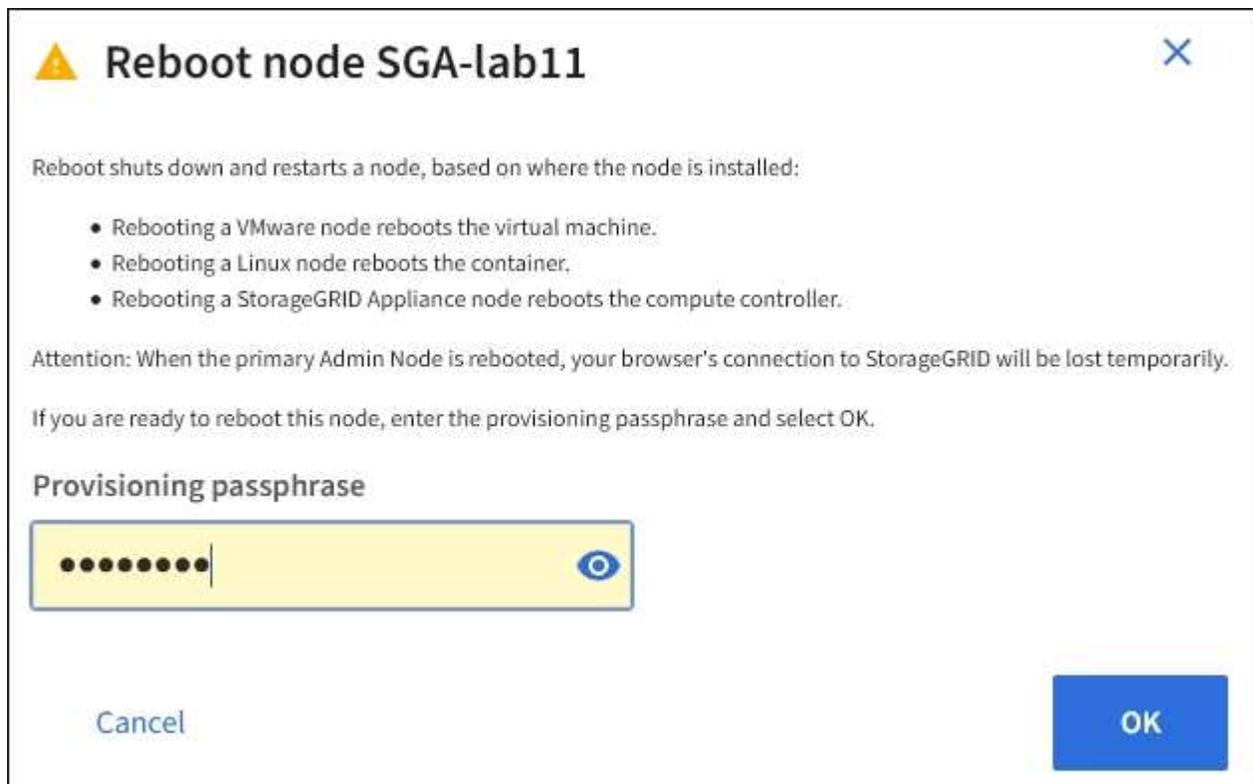
Schritte

1. Wählen Sie **KNOTEN**.
2. Wählen Sie den Grid-Node aus, den Sie neu booten möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.



4. Wählen Sie **Neustart**.

Ein Bestätigungsdialogfeld wird angezeigt.



Wenn Sie den primären Admin-Knoten neu starten, wird im Bestätigungsdialogfeld darauf hingewiesen, dass die Verbindung Ihres Browsers zum Grid Manager vorübergehend verloren geht, wenn Dienste beendet werden.

5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

6. Warten Sie, bis der Node neu gebootet wird.

Es kann einige Zeit dauern, bis Dienste heruntergefahren werden.

Wenn der Knoten neu gestartet wird, wird das graue Symbol (Administrativ Down) auf der linken Seite der Seite **Nodes** angezeigt. Wenn alle Dienste wieder gestartet wurden und der Knoten erfolgreich mit dem Raster verbunden ist, sollte die Seite **Nodes** einen normalen Status anzeigen (keine Symbole links neben dem Knotennamen), was darauf hinweist, dass keine Alarme aktiv sind und der Knoten mit dem Raster verbunden ist.

Grid-Node aus der Eingabeaufforderung neu booten

Wenn Sie den Neustartvorgang genauer überwachen müssen oder wenn Sie nicht auf den Grid Manager zugreifen können, können Sie sich am Grid-Knoten anmelden und den Befehl `Server Manager reboot` über die Befehlsshell ausführen.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Optional Dienste beenden: `service servermanager stop`

Das Beenden von Diensten ist ein optionaler, aber empfohlener Schritt. Die Services können bis zu 15 Minuten zum Herunterfahren dauern. Möglicherweise möchten Sie sich beim System per Remote-Zugriff anmelden, um den Shutdown-Prozess zu überwachen, bevor Sie im nächsten Schritt den Node neu booten.

3. Booten Sie den Grid-Node neu: `reboot`
4. Melden Sie sich aus der Befehlsshell ab: `exit`

Fahren Sie den Grid-Node herunter

Sie können einen Grid-Node über die Befehlshaber des Node herunterfahren.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Bevor Sie dieses Verfahren durchführen, sollten Sie folgende Punkte beachten:

- Im Allgemeinen sollten Sie nicht mehr als einen Node gleichzeitig herunterfahren, um Unterbrechungen zu vermeiden.

- Fahren Sie einen Node während eines Wartungsverfahrens nicht herunter, es sei denn, Sie werden in der Dokumentation oder vom technischen Support ausdrücklich dazu aufgefordert.
- Das Herunterfahren basiert auf dem Installationsort des Node, wie folgt:
 - Durch das Herunterfahren eines VMware-Knotens wird die virtuelle Maschine heruntergefahren.
 - Durch das Herunterfahren eines Linux-Node wird der Container heruntergefahren.
 - Durch das Herunterfahren eines StorageGRID-Appliance-Node wird der Computing-Controller heruntergefahren.
- Wenn Sie planen, mehr als einen Storage-Node an einem Standort herunterzufahren, beenden Sie die Aufnahme von Objekten an diesem Standort ca. eine Stunde lang, bevor Sie die Nodes herunterfahren.

Wenn eine ILM-Regel die Option **Dual Commit** Ingest verwendet (oder wenn eine Regel die Option **Balanced** verwendet und alle erforderlichen Kopien nicht sofort erstellt werden können), überträgt StorageGRID alle neu aufgenommenen Objekte sofort auf zwei Speicher-Nodes auf derselben Seite und wartet ILM später aus. Wenn mehr als ein Storage-Node an einem Standort heruntergefahren wird, sind Sie möglicherweise während des Herunterfahrens nicht in der Lage, auf neu aufgenommene Objekte zuzugreifen. Schreibvorgänge können auch fehlschlagen, wenn am Standort zu wenige Speicherknoten verfügbar bleiben. Siehe "[Objektmanagement mit ILM](#)".

Schritte

1. Melden Sie sich beim Grid-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Beenden Sie alle Dienste: `service servermanager stop`

Die Dienste können bis zu 15 Minuten zum Herunterfahren dauern. Außerdem können Sie sich möglicherweise per Remote-Zugriff beim System anmelden, um den Shutdown-Prozess zu überwachen.

3. Wenn der Node auf einer virtuellen VMware-Maschine ausgeführt wird oder er ein Appliance-Node ist, geben Sie den Befehl zum Herunterfahren aus: `shutdown -h now`

Führen Sie diesen Schritt unabhängig vom Ergebnis des aus `service servermanager stop` Befehl.



Nachdem Sie das ausstellen `shutdown -h now` Befehl auf einem Appliance-Node müssen Sie die Appliance aus- und wieder einschalten, um den Node neu zu starten.

Bei diesem Befehl wird der Controller heruntergefahren, das Gerät ist jedoch weiterhin eingeschaltet. Sie müssen den nächsten Schritt abschließen.

4. Wenn Sie einen Appliance-Node herunterfahren, befolgen Sie die Schritte für Ihre Appliance.

SGF6112

- a. Schalten Sie das Gerät aus.
- b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG6000

- a. Warten Sie, bis die grüne LED Cache Active auf der Rückseite der Storage Controller ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- b. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.

SG5700

- a. Warten Sie, bis die grüne LED Cache Active auf der Rückseite des Storage Controllers ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- b. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und siebensegmentreichen Anzeigeaktivitäten angehalten sind.

SG100 oder SG1000

- a. Schalten Sie das Gerät aus.
- b. Warten Sie, bis die blaue Betriebs-LED erlischt.

Schalten Sie den Host aus

Bevor Sie einen Host herunterfahren, müssen Sie Dienste auf allen Grid-Nodes auf diesem Host anhalten.

Schritte

1. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

2. Beenden Sie alle auf dem Knoten ausgeführten Services: `service servermanager stop`

Die Dienste können bis zu 15 Minuten zum Herunterfahren dauern. Außerdem können Sie sich möglicherweise per Remote-Zugriff beim System anmelden, um den Shutdown-Prozess 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 Node auf einer virtuellen VMware-Maschine ausgeführt wird oder er ein Appliance-Node ist, geben Sie den Befehl zum Herunterfahren aus: `shutdown -h now`

Führen Sie diesen Schritt unabhängig vom Ergebnis des `service servermanager stop` Befehl.



Nachdem Sie das ausstellen `shutdown -h now` Befehl auf einem Appliance-Node müssen Sie die Appliance aus- und wieder einschalten, um den Node neu zu starten.

Bei diesem Befehl wird der Controller heruntergefahren, das Gerät ist jedoch weiterhin eingeschaltet. Sie müssen den nächsten Schritt abschließen.

6. Wenn Sie einen Appliance-Node herunterfahren, befolgen Sie die Schritte für Ihre Appliance.

SGF6112

- a. Schalten Sie das Gerät aus.
- b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG6000

- a. Warten Sie, bis die grüne LED Cache Active auf der Rückseite der Storage Controller ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- b. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.

SG5700

- a. Warten Sie, bis die grüne LED Cache Active auf der Rückseite des Storage Controllers ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- b. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und siebensegmentreichen Anzeigeaktivitäten angehalten sind.

SG100 oder SG1000

- a. Schalten Sie das Gerät aus.
- b. Warten Sie, bis die blaue Betriebs-LED erlischt.

7. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

["SGF6112 Storage Appliances"](#)

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG100- und SG1000-Services-Appliances"

Schalten Sie alle Knoten im Grid aus und wieder ein

Möglicherweise müssen Sie Ihr gesamtes StorageGRID System herunterfahren, wenn Sie ein Datacenter verschieben. Diese Schritte bieten einen allgemeinen Überblick über die empfohlene Sequenz für ein kontrolliertes Herunterfahren und Starten.

Wenn Sie alle Nodes an einem Standort oder Grid ausschalten, können Sie nicht auf aufgenommene Objekte zugreifen, während die Storage-Nodes offline sind.

Stoppen Sie Services und fahren Sie die Grid-Nodes herunter

Bevor Sie ein StorageGRID System ausschalten können, müssen Sie alle Services, die auf jedem Grid-Node ausgeführt werden, anhalten und anschließend alle VMware Virtual Machines, Container-Engines und StorageGRID Appliances herunterfahren.

Über diese Aufgabe

Beenden Sie zuerst Dienste auf Admin-Nodes und Gateway-Nodes, und beenden Sie dann Dienste auf Storage-Nodes.

Dieser Ansatz ermöglicht Ihnen, den primären Admin-Knoten so lange wie möglich zu verwenden, um den Status der anderen Grid-Knoten zu überwachen.



Wenn ein einzelner Host mehr als einen Grid-Node enthält, fahren Sie den Host erst herunter, wenn Sie alle Nodes auf diesem Host angehalten haben. Wenn der Host den primären Admin-Node enthält, fahren Sie diesen Host zuletzt herunter.



Bei Bedarf können Sie dies tun "[Migrieren Sie Nodes von einem Linux-Host zu einem anderen](#)" Hostwartung ohne Auswirkungen auf die Funktionalität oder Verfügbarkeit des Grids durchführen.

Schritte

1. Beenden Sie alle Client-Applikationen vom Zugriff auf das Grid.
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 im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Beenden Sie alle Dienste, die auf dem Knoten ausgeführt werden: `service servermanager stop`

Die Dienste können bis zu 15 Minuten zum Herunterfahren dauern. Außerdem können Sie sich

möglicherweise per Remote-Zugriff beim System anmelden, um den Shutdown-Prozess zu überwachen.

4. Wiederholen Sie die beiden vorherigen Schritte, um die Dienste auf allen Speicherknoten, den Knoten Archiv und nicht-primären Admin-Knoten anzuhalten.

Sie können die Dienste auf diesen Knoten in beliebiger Reihenfolge anhalten.



Wenn Sie das ausgegeben `service servermanager stop` Befehl zum Beenden der Dienste auf einem Appliance-Speicherknoten müssen Sie die Appliance aus- und wieder einschalten, um den Node neu zu starten.

5. Wiederholen Sie für den primären Admin-Knoten die Schritte für [Anmeldung beim Node](#) Und [Anhalten 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 VMware Virtual Machines und für Appliance Storage Nodes ausgeführt werden, den Befehl `shutdown aus: shutdown -h now`

Führen Sie diesen Schritt unabhängig vom Ergebnis des `aus service servermanager stop` Befehl.

Bei diesem Befehl wird der Compute-Controller heruntergefahren, das Gerät ist jedoch weiterhin eingeschaltet. Sie müssen den nächsten Schritt abschließen.

8. Wenn Sie über Geräteknöten verfügen, befolgen Sie die Schritte für Ihre Appliance.

SG100 oder SG1000

- a. Schalten Sie das Gerät aus.
- b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SGF6112

- a. Schalten Sie das Gerät aus.
- b. Warten Sie, bis die blaue Betriebs-LED erlischt.

SG6000

- a. Warten Sie, bis die grüne LED Cache Active auf der Rückseite der Storage Controller ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- b. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.

SG5700

- a. Warten Sie, bis die grüne LED Cache Active auf der Rückseite des Storage Controllers ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- b. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und siebensegmentreichen Anzeigeaktivitäten angehalten sind.

9. Melden Sie sich bei Bedarf von der Eingabeaufforderung ab: `exit`

Das StorageGRID-Grid wurde jetzt heruntergefahren.

Grid-Nodes starten

Wenn das gesamte Grid seit mehr als 15 Tagen heruntergefahren wurde, müssen Sie sich an den technischen Support wenden, bevor Sie die Grid-Nodes starten. Versuchen Sie nicht, die Wiederherstellungsverfahren zu verwenden, mit denen Cassandra-Daten wiederhergestellt werden. Dies kann zu Datenverlust führen.

Schalten Sie die Netzknoten nach Möglichkeit in dieser Reihenfolge ein:

- Zuerst die Administratorknoten mit Strom versorgen.
- Strom auf Gateway-Knoten zuletzt anwenden.



Wenn ein Host mehrere Grid-Nodes enthält, werden die Nodes automatisch wieder online geschaltet, wenn Sie den Host einschalten.

Schritte

1. Schalten Sie die Hosts für den primären Admin-Node und alle nicht-primären Admin-Nodes ein.



Sie können sich erst bei den Admin-Knoten anmelden, wenn die Speicherknoten neu gestartet wurden.

2. Schalten Sie die Hosts für alle Archiv-Nodes und Speicherknoten ein.

Sie können diese Knoten in beliebiger Reihenfolge einschalten.

3. Schalten Sie die Hosts für alle Gateway-Nodes ein.

4. Melden Sie sich beim Grid Manager an.

5. Wählen Sie **NODES** aus, und überwachen Sie den Status der Grid-Knoten. Vergewissern Sie sich, dass neben den Node-Namen keine Warnsymbole vorhanden sind.

Verwandte Informationen

- ["SG100- und SG1000-Services-Appliances"](#)
- ["SG6000 Storage-Appliances"](#)
- ["SG5700 Storage-Appliances"](#)

Verwenden Sie eine DoNotStart-Datei

Wenn Sie unter Anleitung des technischen Supports verschiedene Wartungs- oder Konfigurationsverfahren ausführen, werden Sie möglicherweise aufgefordert, eine DoNotStart-Datei zu verwenden, um zu verhindern, dass Dienste beim Starten von Server Manager gestartet oder neu gestartet werden.



Sie sollten eine DoNotStart-Datei nur hinzufügen oder entfernen, wenn Sie vom technischen Support dazu aufgefordert wurden.

Um den Start eines Dienstes zu verhindern, legen Sie eine DoNotStart-Datei in das Verzeichnis des Dienstes, den Sie verhindern möchten, dass dieser gestartet wird. Beim Start sucht der Server Manager nach der DoNotStart-Datei. Wenn die Datei vorhanden ist, wird der Dienst (und alle Services, die davon abhängig sind) nicht gestartet. Wenn die DoNotStart-Datei entfernt wird, wird der zuvor angefangene Dienst beim nächsten Start oder Neustart von Server Manager gestartet. Dienste werden nicht automatisch gestartet, wenn die DoNotStart-Datei entfernt wird.

Der effizienteste Weg, um einen Neustart aller Dienste zu verhindern, ist, dass der NTP-Dienst nicht gestartet wird. Alle Services sind vom NTP-Service abhängig und können nicht ausgeführt werden, wenn der NTP-Service nicht ausgeführt wird.

Fügen Sie die DoNotStart-Datei für den Dienst hinzu

Sie können verhindern, dass ein einzelner Dienst gestartet wird, indem Sie dem Verzeichnis dieses Dienstes auf einem Grid-Node eine DoNotStart-Datei hinzufügen.

Bevor Sie beginnen

Sie haben die `passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Fügen Sie eine DoNotStart-Datei hinzu: `touch /etc/sv/service/DoNotStart`

Wo `service` Ist der Name des Dienstes, der verhindert werden soll, dass der Dienst gestartet wird.
Beispiel:

```
touch /etc/sv/ldr/DoNotStart
```

Eine DoNotStart-Datei wird erstellt. Es werden keine Dateiinhalte benötigt.

Wenn Server Manager oder der Grid-Node neu gestartet wird, wird der Server Manager neu gestartet, der Service jedoch nicht.

3. Melden Sie sich aus der Befehlshell ab: `exit`

Entfernen Sie DoNotStart-Datei für den Dienst

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-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Entfernen Sie die DoNotStart-Datei aus dem Service-Verzeichnis: `rm /etc/sv/service/DoNotStart`

Wo `service` Ist der Name des Service. Beispiel:

```
rm /etc/sv/ldr/DoNotStart
```

3. Starten Sie den Service: `service servicename start`
4. Melden Sie sich aus der Befehlshell ab: `exit`

Fehlerbehebung Für Server Manager

Wenn bei der Verwendung von Server Manager ein Problem auftritt, überprüfen Sie dessen Protokolldatei.

Fehlermeldungen im Zusammenhang mit Server Manager werden in der Server Manager-Protokolldatei erfasst, die sich unter befindet: `/var/local/log/servermanager.log`

Prüfen Sie diese Datei auf Fehlermeldungen zu Fehlern. Eskalieren des Problems gegebenenfalls an den technischen Support. Möglicherweise werden Sie aufgefordert, Protokolldateien an den technischen Support weiterzuleiten.

Dienst mit Fehlerstatus

Wenn Sie feststellen, dass ein Dienst einen Fehlerstatus eingegeben hat, versuchen Sie, den Dienst neu zu starten.

Bevor Sie beginnen

Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Server Manager überwacht Dienste und startet alle, die unerwartet angehalten haben. Wenn ein Dienst ausfällt, versucht der Server Manager, ihn neu zu starten. Wenn drei fehlgeschlagene Versuche bestehen, einen Dienst innerhalb von fünf Minuten zu starten, wechselt der Dienst in einen Fehlerzustand. Server Manager versucht keinen anderen Neustart.

Schritte

1. Melden Sie sich beim Grid-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

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 Servicestatus lautet `disabled`, Siehe die Anweisungen für "[Entfernen einer DoNotStart-Datei für einen Dienst](#)".

3. Versuchen Sie, den Fehlerstatus durch Neustart des Dienstes zu entfernen: `service servicename restart`

Wenn der Service nicht neu gestartet werden kann, wenden Sie sich an den technischen Support.

4. Melden Sie sich aus der Befehlsshell ab: `exit`

Halten Sie die Appliance-Konfiguration aufrecht

Allgemeine Verfahren für die Knotenwartung: Übersicht

Befolgen Sie diese Anweisungen, um Ihr StorageGRID-System zu warten.

Informationen zu diesen Anweisungen

In diesen Anweisungen werden die für alle Knoten üblichen Verfahren beschrieben, z. B. die Anwendung eines Software-Hotfix, die Wiederherstellung von Grid-Nodes, die Wiederherstellung eines ausgefallenen Standorts, die Stilllegung von Grid-Nodes oder eines gesamten Standorts, die Durchführung von Netzwerkwartungen, die Durchführung von Wartungsverfahren auf Host-Ebene und Middleware sowie die Durchführung von Grid Node-Verfahren.



In diesen Anweisungen bezieht sich „Linux“ auf eine Bereitstellung von Red hat® Enterprise Linux®, Ubuntu®, CentOS oder Debian®. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um eine Liste der unterstützten Versionen zu erhalten.

Bevor Sie beginnen

- Sie verfügen über ein umfassendes Verständnis des StorageGRID Systems.
- Sie haben die Topologie Ihres StorageGRID Systems überprüft und sich mit der Grid-Konfiguration vertraut gemacht.
- Ihr versteht, dass ihr alle Anweisungen genau befolgen und alle Warnungen beachten müsst.
- Sie wissen, dass nicht beschriebene Wartungsverfahren nicht unterstützt werden oder eine Serviceerbringung erfordern.

Wartungsverfahren für Geräte

Spezifische Wartungsverfahren für jeden StorageGRID-Gerätetyp finden Sie in den Abschnitten zur Gerätewartung:

- "[SGF6112-Appliance warten](#)"
- "[Warten Sie die SG6000-Appliance](#)"
- "[SG5700 Appliance warten](#)"
- "[Wartung von SG100 und SG1000 Appliances](#)"

Stellen Sie das Gerät in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Berechtigung **Wartung** oder **Stammzugriff**. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Über diese Aufgabe

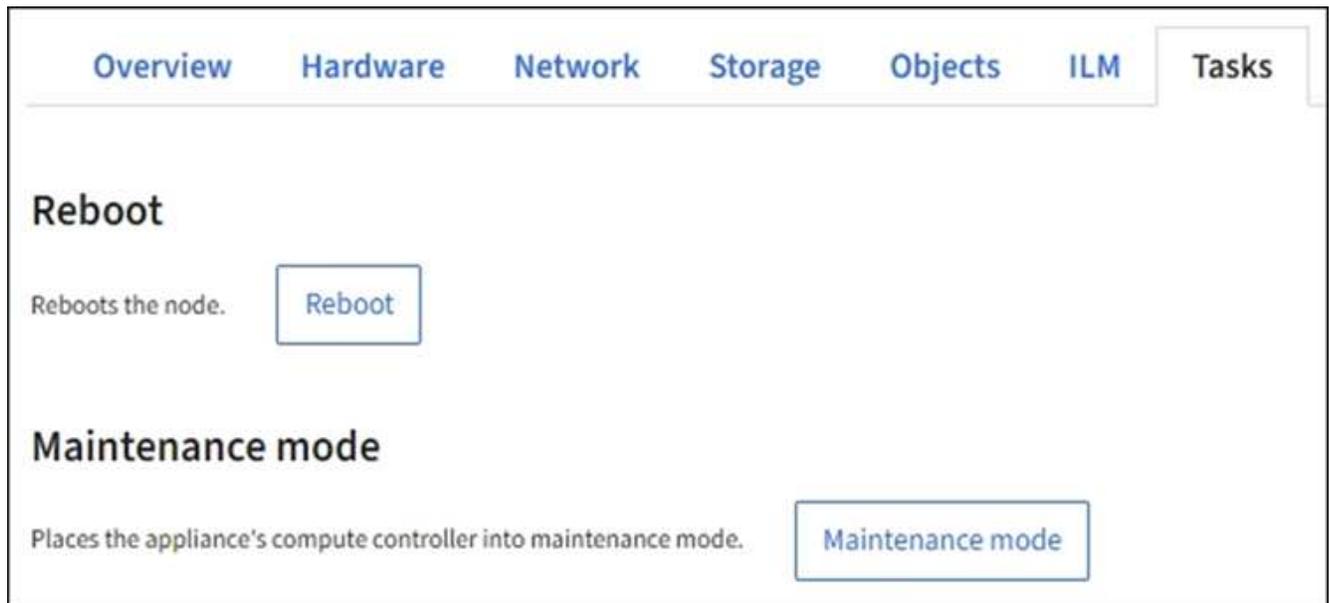
In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den Wartungsmodus versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.



Das Passwort des Admin-Kontos und die SSH-Host-Schlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem Kennwort, das zum Zeitpunkt der Wartung der Appliance vorhanden war.

Schritte

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie in der Strukturansicht der Seite Knoten den Appliance Storage Node aus.
3. Wählen Sie **Aufgaben**.



4. Wählen Sie **Wartungsmodus**. Ein Bestätigungsdialogfeld wird angezeigt.
5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

Eine Fortschrittsleiste und eine Reihe von Meldungen, darunter „Anfrage gesendet“, „StorageGRID stoppen“ und „neu booten“, geben an, dass die Appliance die Schritte zum Eintritt in den Wartungsmodus abschließt.

Wenn sich die Appliance im Wartungsmodus befindet, wird in einer Bestätigungsmeldung die URLs aufgeführt, mit denen Sie auf das Installationsprogramm der StorageGRID-Appliance zugreifen können.

i This node is currently in maintenance mode. Navigate to one of the URLs listed below and perform any necessary maintenance procedures.

- <https://172.16.2.24:8443>
- <https://10.224.2.24:8443>

When you are done with any required maintenance procedures, you must exit maintenance mode by selecting Reboot Controller from the StorageGRID Appliance Installer.

6. Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.



Wenn Sie über eine direkte Verbindung zum Management-Port der Appliance verfügen, verwenden Sie `https://169.254.0.1:8443`. So greifen Sie auf die Seite StorageGRID-Appliance-Installationsprogramm zu.

7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im Wartungsmodus befindet.

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

8. Führen Sie alle erforderlichen Wartungsaufgaben durch.

9. Beenden Sie nach Abschluss der Wartungsaufgaben den Wartungsmodus und fahren Sie den normalen Node-Betrieb fort. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Controller neu starten** aus, und wählen Sie dann **Neustart in StorageGRID** aus.

NetApp® StorageGRID® Appliance Installer

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Reboot Controller
Request a controller reboot.

RAID Mode
Upgrade Firmware
Reboot Controller

Reboot into StorageGRID Reboot into Maintenance Mode

Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

MTU-Einstellung ändern

Sie können die MTU-Einstellung ändern, die Sie beim Konfigurieren von IP-Adressen für den Appliance-Node zugewiesen haben.

Über diese Aufgabe



Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.



Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein.

Um die MTU-Einstellung zu ändern, ohne den Appliance-Node neu zu booten, [Verwenden Sie das Werkzeug IP ändern](#).

Wenn das Client- oder Admin-Netzwerk während der ersten Installation nicht im Installationsprogramm der StorageGRID-Appliance konfiguriert wurde, [Ändern Sie die MTU-Einstellung im Wartungsmodus](#).

Ändern Sie die MTU-Einstellung mit dem Tool IP ändern

Bevor Sie beginnen

Sie haben die `passwords.txt` Datei zum Verwenden des Tools zum Ändern der IP-Adresse.

Schritte

Greifen Sie auf das Change IP-Tool zu und aktualisieren Sie die MTU-Einstellungen, wie in beschrieben ["Ändern der Node-Netzwerkkonfiguration"](#).

Ändern Sie die MTU-Einstellung im Wartungsmodus

Ändern Sie die MTU-Einstellung unter Verwendung des Wartungsmodus, wenn Sie mit dem Tool IP ändern nicht auf diese Einstellungen zugreifen können.

Bevor Sie beginnen

Das Gerät war "[In den Wartungsmodus versetzt](#)".

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren > IP-Konfiguration** aus.
2. Nehmen Sie die gewünschten Änderungen an den MTU-Einstellungen für Grid Network, Admin Network und Client Network vor.
3. Wenn Sie mit den Einstellungen zufrieden sind, wählen Sie **Speichern**.
4. Wenn diese Prozedur erfolgreich abgeschlossen ist und Sie weitere durchzuführenden Verfahren haben, während sich der Node im Wartungsmodus befindet, führen Sie sie jetzt aus. Wenn Sie fertig sind oder Fehler auftreten und von vorne beginnen möchten, wählen Sie **Erweitert > Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:
 - Wählen Sie **Neustart in StorageGRID** aus
 - Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. Wählen Sie diese Option aus, wenn während des Verfahrens Fehler auftreten und neu starten möchten. Nachdem der Node das Neubooten in den Wartungsmodus abgeschlossen hat, starten Sie den entsprechenden Schritt während des ausgefallenen Verfahrens neu.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Überprüfen Sie die DNS-Server-Konfiguration

Sie können die DNS-Server, die derzeit von diesem Appliance-Knoten verwendet werden, überprüfen und vorübergehend ändern.

Bevor Sie beginnen

Das Gerät war ["In den Wartungsmodus versetzt"](#).

Über diese Aufgabe

Möglicherweise müssen Sie die DNS-Servereinstellungen ändern, wenn eine verschlüsselte Appliance keine Verbindung zum Schlüsselverwaltungsserver (KMS) oder KMS-Cluster herstellen kann, da der Hostname für das KMS als Domänenname anstelle einer IP-Adresse angegeben wurde. Alle Änderungen, die Sie an den DNS-Einstellungen für die Appliance vornehmen, sind temporär und gehen verloren, wenn Sie den Wartungsmodus verlassen. Um diese Änderungen dauerhaft vorzunehmen, geben Sie die DNS-Server im Grid Manager an (**MAINTENANCE > Network > DNS-Server**).

- Temporäre Änderungen an der DNS-Konfiguration sind nur für Node-verschlüsselte Appliances erforderlich, bei denen der KMS-Server mithilfe eines vollständig qualifizierten Domännennamens anstelle einer IP-Adresse für den Hostnamen definiert wird.
- Wenn eine Node-verschlüsselte Appliance über einen Domännennamen eine Verbindung zu einem KMS herstellt, muss sie eine Verbindung zu einem der für das Grid definierten DNS-Server herstellen. Einer dieser DNS-Server übersetzt dann den Domain-Namen in eine IP-Adresse.
- Wenn der Knoten keinen DNS-Server für das Grid erreichen kann oder wenn Sie die DNS-Einstellungen für das Grid geändert haben, wenn ein Node-verschlüsselter Appliance-Knoten offline war, kann der Node keine Verbindung zum KMS herstellen. Verschlüsselte Daten auf der Appliance können erst entschlüsselt werden, nachdem das DNS-Problem behoben wurde.

Um ein DNS-Problem zu beheben, das die KMS-Verbindung verhindert, geben Sie die IP-Adresse eines oder mehrerer DNS-Server im Installationsprogramm der StorageGRID Appliance an. Diese temporären DNS-Einstellungen ermöglichen es der Appliance, eine Verbindung zum KMS herzustellen und Daten auf dem Knoten zu entschlüsseln.

Wenn sich beispielsweise der DNS-Server für das Grid ändert, während ein verschlüsselter Knoten offline war, kann der Node das KMS nicht erreichen, wenn es wieder online ist, da er weiterhin die vorherigen DNS-Werte verwendet. Durch Eingabe der neuen IP-Adresse des DNS-Servers im StorageGRID-Appliance-Installationsprogramm kann eine temporäre KMS-Verbindung die Knotendaten entschlüsseln.

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren > DNS-Konfiguration** aus.
2. Vergewissern Sie sich, dass die angegebenen DNS-Server richtig sind.

DNS Servers

 Configuration changes made on this page will not be passed to the StorageGRID software after appliance installation.

Servers

Server 1	<input type="text" value="10.224.223.135"/>	
Server 2	<input type="text" value="10.224.223.136"/>	
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>

3. Ändern Sie bei Bedarf die DNS-Server.



Änderungen an den DNS-Einstellungen erfolgen temporär und gehen verloren, wenn Sie den Wartungsmodus beenden.

4. Wenn Sie mit den temporären DNS-Einstellungen zufrieden sind, wählen Sie **Speichern**.

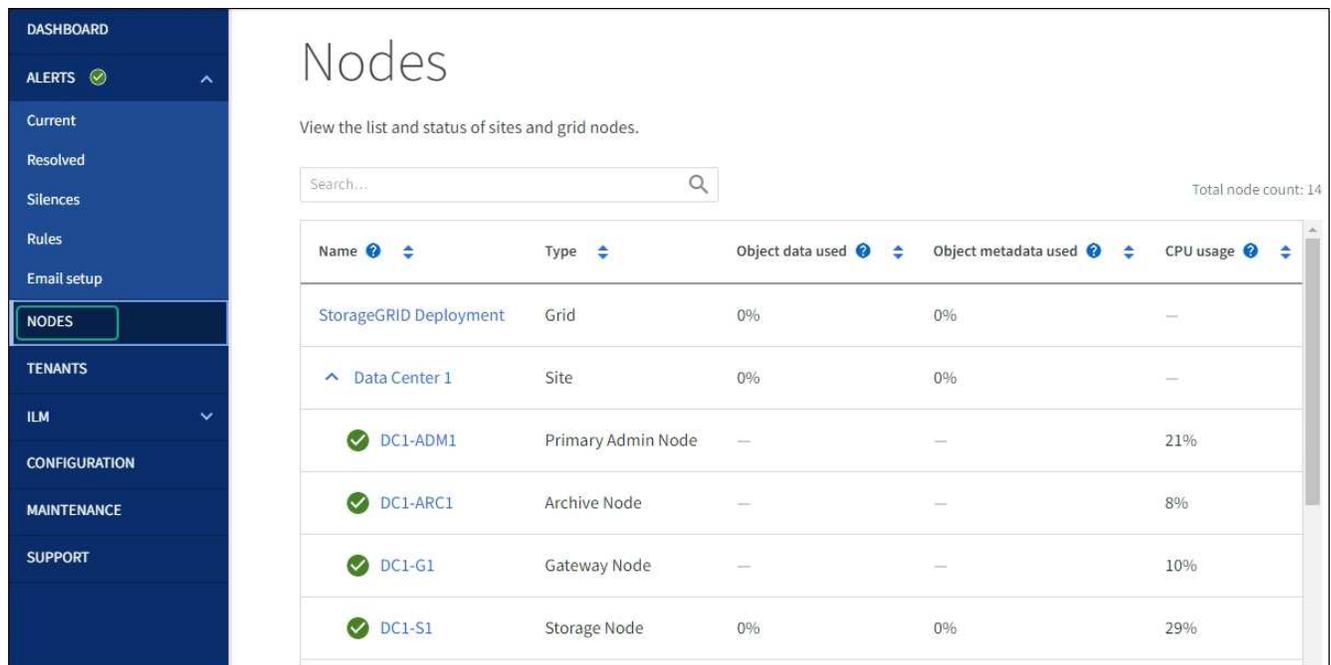
Der Knoten verwendet die auf dieser Seite angegebenen DNS-Servereinstellungen, um eine Verbindung mit dem KMS herzustellen, sodass die Daten auf dem Knoten entschlüsselt werden können.

5. Nachdem die Node-Daten entschlüsselt wurden, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:
 - Wählen Sie **Neustart in StorageGRID** aus, um den Controller neu zu starten, wobei der Knoten wieder in das Raster integriert wird. Wählen Sie diese Option, wenn Sie im Wartungsmodus ausgeführt werden und den Node in den normalen Betrieb zurückkehren möchten.
 - Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. (Diese Option ist nur verfügbar, wenn sich der Controller im Wartungsmodus befindet.) Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Wenn der Node neu gebootet und neu in das Grid wechselt, werden die im Grid Manager aufgeführten systemweiten DNS-Server verwendet. Nach dem erneuten Beitritt zum Grid verwendet die Appliance nicht mehr die im StorageGRID Appliance Installer angegebenen temporären DNS-Server, während sich die Appliance im Wartungsmodus befindet.

Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden (✓ Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.



Aktualisieren Sie die MAC-Adressenverweise

In einigen Fällen müssen Sie möglicherweise die MAC-Adressenreferenzen nach dem Austausch einer Appliance aktualisieren.

Über diese Aufgabe

Wenn eine der Netzwerkschnittstellen auf einer Appliance, die Sie ersetzen, für DHCP konfiguriert ist, müssen Sie möglicherweise die permanenten DHCP-Lease-Zuweisungen auf den DHCP-Servern aktualisieren, um auf die MAC-Adressen der Ersatz-Appliance zu verweisen. Das Update stellt sicher, dass dem Ersatzgerät die erwarteten IP-Adressen zugewiesen werden.

Schritte

1. Suchen Sie das Etikett auf der Vorderseite des Geräts. Das Etikett enthält die MAC-Adresse für den BMC-Verwaltungsport der Appliance.
2. Um die MAC-Adresse für den Admin-Netzwerkanschluss zu ermitteln, müssen Sie der Hexadezimalzahl auf dem Etikett **2** hinzufügen.

Wenn die MAC-Adresse auf dem Etikett beispielsweise mit **09** endet, endet die MAC-Adresse für den Admin-Port in **0B**. Wenn die MAC-Adresse auf dem Etikett mit **(y)FF** endet, endet die MAC-Adresse für den Admin-Port in **(y+1)01**.

Sie können diese Berechnung einfach durchführen, indem Sie den Rechner unter Windows öffnen, ihn auf den Programmiermodus setzen, Hex auswählen, die MAC-Adresse eingeben und dann **+ 2 =** eingeben.

3. Bitten Sie Ihren Netzwerkadministrator, die DNS/Netzwerk- und IP-Adresse für das Gerät, das Sie entfernt haben, mit der MAC-Adresse für das Ersatzgerät zu verknüpfen.



Sie müssen sicherstellen, dass alle IP-Adressen für das Originalgerät aktualisiert wurden, bevor Sie das Ersatzgerät mit Strom versorgen. Andernfalls erhält die Appliance beim Booten von neuen DHCP IP-Adressen und kann die Verbindung zu StorageGRID möglicherweise nicht wiederherstellen. Dieser Schritt gilt für alle StorageGRID-Netzwerke, die mit der Appliance verbunden sind.



Wenn die ursprüngliche Appliance statische IP-Adresse verwendet, übernimmt die neue Appliance automatisch die IP-Adressen der entfernten Appliance.

Überwachung der Node-Verschlüsselung im Wartungsmodus

Wenn Sie während der Installation die Node-Verschlüsselung für die Appliance aktiviert haben, können Sie den Verschlüsselungsstatus aller Appliance-Nodes überwachen, einschließlich Details zur Node-Verschlüsselung und zum Key Management Server (KMS).

Siehe "[Konfigurieren von Verschlüsselungsmanagement-Servern](#)" Für Informationen zur Implementierung von KMS für StorageGRID-Appliances.

Bevor Sie beginnen

- Während der Installation aktivieren Sie die Node-Verschlüsselung für die Appliance. Sie können die Node-Verschlüsselung nicht aktivieren, nachdem die Appliance installiert wurde.
- Das ist schon "[Das Gerät in den Wartungsmodus versetzt](#)".

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Hardware konfigurieren > Node-Verschlüsselung**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

 You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfe01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate 

Client certificate 

Clear KMS Key

 Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

Die Seite Node Encryption enthält drei Abschnitte:

- Der Verschlüsselungsstatus gibt an, ob die Node-Verschlüsselung für die Appliance aktiviert oder deaktiviert ist.
- Details des Schlüsselmanagementservers zeigen Informationen über den KMS an, der zur Verschlüsselung der Appliance verwendet wird. Sie können die Abschnitte Server- und Clientzertifikat erweitern, um Zertifikatdetails und -Status anzuzeigen.
 - Um Probleme mit den Zertifikaten selbst zu lösen, wie z. B. die Verlängerung abgelaufener Zertifikate, siehe ["Anweisungen zur Konfiguration von KMS"](#).
 - Wenn bei der Verbindung zu KMS-Hosts unerwartete Probleme auftreten, überprüfen Sie, ob der ["DNS-Server sind korrekt"](#) und das ["Appliance-Netzwerk wurde ordnungsgemäß konfiguriert"](#).
 - Wenden Sie sich an den technischen Support, wenn Sie Ihre Zertifikatsprobleme nicht lösen können.
- Der klare KMS-Schlüssel deaktiviert die Node-Verschlüsselung für die Appliance, entfernt die Zuordnung zwischen der Appliance und dem für den StorageGRID-Standort konfigurierten

Schlüsselmanagementserver und löscht alle Daten von der Appliance. Unbedingt [Löschen Sie den KMS-Schlüssel](#) Bevor Sie die Appliance in ein anderes StorageGRID-System installieren können.



Durch das Löschen der KMS-Konfiguration werden Daten von der Appliance gelöscht, sodass dauerhaft kein Zugriff darauf besteht. Diese Daten können nicht wiederhergestellt werden.

2. Wenn Sie den Status der Node-Verschlüsselung überprüfen, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:
 - Wählen Sie **Neustart in StorageGRID** aus, um den Controller neu zu starten, wobei der Knoten wieder in das Raster integriert wird. Wählen Sie diese Option, wenn Sie im Wartungsmodus ausgeführt werden und den Node in den normalen Betrieb zurückkehren möchten.
 - Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. (Diese Option ist nur verfügbar, wenn sich der Controller im Wartungsmodus befindet.) Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

Die Konfiguration des Verschlüsselungsmanagement-Servers löschen

Durch Löschen der KMS-Konfiguration (Key Management Server) wird die Node-Verschlüsselung auf der Appliance deaktiviert. Nach dem Löschen der KMS-Konfiguration werden die Daten auf der Appliance dauerhaft gelöscht und sind nicht mehr zugänglich. Diese Daten können nicht wiederhergestellt werden.

Bevor Sie beginnen

Wenn Daten auf der Appliance aufbewahrt werden müssen, müssen Sie einen Node außer Betrieb nehmen oder den Node klonen, bevor Sie die KMS-Konfiguration löschen.



Wenn KMS gelöscht wird, werden die Daten auf der Appliance dauerhaft gelöscht und sind nicht mehr zugänglich. Diese Daten können nicht wiederhergestellt werden.

"Bauen Sie den Node aus" Um beliebige Daten zu anderen Nodes in StorageGRID zu verschieben.

Über diese Aufgabe

Beim Löschen der Appliance-KMS-Konfiguration wird die Node-Verschlüsselung deaktiviert, wodurch die Zuordnung zwischen dem Appliance-Node und der KMS-Konfiguration für den StorageGRID-Standort entfernt wird. Die Daten auf dem Gerät werden gelöscht und das Gerät wird im Installationszustand zurückgelassen. Dieser Prozess kann nicht rückgängig gemacht werden.

Sie müssen die KMS-Konfiguration löschen:

- Bevor Sie die Appliance in einem anderen StorageGRID-System installieren können, wird kein KMS verwendet oder ein anderer KMS verwendet.



Löschen Sie die KMS-Konfiguration nicht, wenn Sie einen Appliance-Node in einem StorageGRID-System, das denselben KMS-Schlüssel verwendet, neu installieren möchten.

- Bevor Sie einen Node wiederherstellen und neu installieren können, bei dem die KMS-Konfiguration verloren ging und der KMS-Schlüssel nicht wiederhergestellt werden kann.
- Bevor Sie ein Gerät zurückgeben, das zuvor an Ihrem Standort verwendet wurde.

- Nach der Stilllegung einer Appliance, für die die Node-Verschlüsselung aktiviert war.



Die Appliance muss vor dem Löschen von KMS deaktiviert werden, um ihre Daten auf andere Nodes im StorageGRID System zu verschieben. Das Löschen von KMS vor der Deaktivierung der Appliance führt zu Datenverlusten und kann dazu führen, dass die Appliance funktionsunfähig bleibt.

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.

`https://Controller_IP:8443`

Controller_IP Die IP-Adresse des Compute-Controllers (nicht des Storage-Controllers) in einem der drei StorageGRID-Netzwerke.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Hardware Konfigurieren > Node Encryption**.



Wenn die KMS-Konfiguration gelöscht wird, werden die Daten auf der Appliance dauerhaft gelöscht. Diese Daten können nicht wiederhergestellt werden.

3. Wählen Sie unten im Fenster **KMS-Schlüssel löschen und Daten löschen**.
4. Wenn Sie sicher sind, dass Sie die KMS-Konfiguration löschen möchten, geben Sie ein **clear** Wählen Sie im Warndialogfeld **KMS-Schlüssel löschen und Daten löschen**.

Der KMS-Schlüssel und alle Daten werden vom Node gelöscht und die Appliance wird neu gebootet. Dies kann bis zu 20 Minuten dauern.

5. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.

`https://Controller_IP:8443`

Controller_IP Die IP-Adresse des Compute-Controllers (nicht des Storage-Controllers) in einem der drei StorageGRID-Netzwerke.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

6. Wählen Sie **Hardware Konfigurieren > Node Encryption**.
7. Vergewissern Sie sich, dass die Knotenverschlüsselung deaktiviert ist und dass die Schlüssel- und Zertifikatinformationen in **Key Management Server Details** und die Kontrolle **KMS-Schlüssel löschen und Daten löschen** aus dem Fenster entfernt werden.

Die Node-Verschlüsselung kann auf der Appliance erst wieder aktiviert werden, wenn sie in einem Grid neu installiert wird.

Nachdem Sie fertig sind

Nachdem die Appliance neu gebootet wurde und Sie überprüft haben, dass der KMS gelöscht wurde und sich die Appliance im Installationszustand befindet, können Sie die Appliance physisch aus dem StorageGRID System entfernen. Siehe "[Anweisungen zur Vorbereitung des Geräts für die Neuinstallation](#)".

Klonen von Appliance-Nodes

Klonen von Appliance-Nodes: Übersicht

Sie können einen Appliance-Node in StorageGRID klonen, um eine Appliance mit neuerem Design oder höheren Funktionen zu verwenden. Durch das Klonen werden alle Informationen über den vorhandenen Node an die neue Appliance übertragen, ein einfach zu durchsetzender Hardware-Upgrade-Prozess bietet eine Alternative zur Ausmusterung und Erweiterung beim Austausch von Appliances.

Mit dem Appliance-Node-Klonen können Sie einen vorhandenen Appliance-Node (Quelle) im Grid ganz einfach durch eine kompatible Appliance (Ziel) ersetzen, die Teil desselben logischen StorageGRID-Standorts ist. Dabei werden alle Daten auf die neue Appliance übertragen, die Appliance wird in Betrieb versetzt, um den alten Appliance-Node zu ersetzen und die alte Appliance im Installationszustand zu lassen.

Warum einen Appliance-Node klonen?

Sie können einen Appliance-Node klonen, wenn Sie Folgendes benötigen:

- Ersetzen Sie Appliances, die sich dem Ende ihrer Lebensdauer nähert.
- Aktualisieren Sie vorhandene Nodes, um von der verbesserten Appliance-Technologie zu profitieren.
- Erhöhen Sie die Grid-Storage-Kapazität, ohne die Anzahl der Storage-Nodes in Ihrem StorageGRID System zu ändern.
- Verbessern Sie die Storage-Effizienz, z. B. durch Ändern des RAID-Modus von DDP-8 auf DDP-16 oder auf RAID-6.
- Node-Verschlüsselung wird effizient implementiert, sodass die externen Verschlüsselungsmanagement-Server (KMS) verwendet werden können.

Welches StorageGRID Netzwerk wird verwendet?

Durch das Klonen werden Daten vom Quell-Node über ein beliebiges StorageGRID-Netzwerk direkt an die Ziel-Appliance übertragen. Das Grid-Netzwerk wird normalerweise verwendet, Sie können aber auch das Admin-Netzwerk oder das Client-Netzwerk verwenden, wenn die Quell-Appliance mit diesen Netzwerken verbunden ist. Wählen Sie das Netzwerk für den Klon-Traffic aus, das die beste Performance bei der Datenübertragung bietet, ohne die Leistung des StorageGRID-Netzwerks oder die Datenverfügbarkeit zu beeinträchtigen.

Bei der Installation der Ersatzanwendung müssen Sie temporäre IP-Adressen für StorageGRID-Verbindung und Datentransfer angeben. Da die Ersatz-Appliance Teil derselben Netzwerke ist wie der Appliance-Node, den sie ersetzt, müssen Sie für jedes dieser Netzwerke auf der Ersatz-Appliance temporäre IP-Adressen angeben.

Kompatibilität der Ziel-Appliance

Ersatz-Appliances müssen vom gleichen Typ sein wie der Quell-Node, den sie ersetzen, und beide müssen Teil desselben logischen StorageGRID-Standorts sein.

- Eine Ersatz-Services-Appliance kann sich von dem Admin-Node oder dem Gateway-Node unterscheiden, den er ersetzt.
 - Sie können eine SG100-Quell-Node-Appliance zu einer SG1000-Services-Ziel-Appliance klonen, um dem Admin-Node oder Gateway-Node eine höhere Funktion zuzuweisen.

- Sie können eine SG1000-Quell-Node-Appliance in einer SG100-Services-Ziel-Appliance klonen, um die SG1000 für eine anspruchsvollere Applikation neu zu implementieren.

Beispiel: Wenn eine SG1000-Quell-Node-Appliance als Admin-Node verwendet wird und Sie sie als dedizierten Load-Balancing-Node verwenden möchten.

- Durch den Austausch einer SG1000-Quell-Node-Appliance durch eine SG100-Services-Ziel-Appliance wird die maximale Geschwindigkeit der Netzwerkports von 100 GbE auf 25 GbE verringert.
- Die SG100- und SG1000-Appliances verfügen über unterschiedliche Netzwerkverbindungen. Wenn Sie den Gerätetyp ändern, müssen möglicherweise die Kabel oder SFP-Module ersetzt werden.
- Eine Ersatzspeichergerät muss über eine größere Kapazität verfügen als der zu ersetzende Speicher-Node.
 - Wenn die Ziel-Storage-Appliance über dieselbe Anzahl von Laufwerken wie der Quell-Node verfügt, müssen die Laufwerke in der Ziel-Appliance über eine größere Kapazität (in TB) verfügen.
 - Wenn Sie planen, auf dem Zielknoten denselben RAID-Modus wie auf dem Quellknoten zu verwenden, Oder in einem weniger Storage-effizienten RAID-Modus (z. B. Wechsel von RAID 6 zu DDP) müssen die Laufwerke in der Ziel-Appliance größer (in TB) sein als die Laufwerke in der Quell-Appliance.
 - Wenn die Anzahl der in einer Ziel-Storage-Appliance installierten Standardlaufwerke aufgrund der Installation von Solid-State-Laufwerken (SSDs) geringer ist als die Anzahl der Laufwerke im Quell-Node, ist die allgemeine Storage-Kapazität der Standardlaufwerke in der Ziel-Appliance (in TB) Muss die gesamte funktionale Laufwerkskapazität aller Laufwerke im Quell-Storage-Node überschreiten.

Wenn Sie beispielsweise eine SG5760 Quell-Storage-Node-Appliance mit 60 Laufwerken auf eine SG6060 Ziel-Appliance mit 58 Standardlaufwerken klonen, sollten Sie vor dem Klonen in der SG6060 Ziel-Appliance größere Laufwerke installieren, um die Storage-Kapazität aufrechtzuerhalten. (Die zwei Laufwerksschächte, die SSDs in der Ziel-Appliance enthalten, sind nicht in der gesamten Appliance-Storage-Kapazität enthalten.)

Wenn jedoch eine SG5760 Quell-Node-Appliance mit 60 Laufwerken mit SANtricity Dynamic Disk Pools DDP-8 konfiguriert ist, kann die SG6060 Appliance mit 58 Laufwerken und derselben Größe mit DDP-16 aufgrund der verbesserten Storage-Effizienz ein gültiges Klonziel für die SG6060 Appliance werden.

Auf der Seite **NODES** im Grid Manager können Sie Informationen zum aktuellen RAID-Modus des Quell-Appliance-Knotens anzeigen. Wählen Sie die Registerkarte * Storage* für das Gerät aus.

- Die Anzahl der Volumes in einer Ziel-Storage-Appliance muss größer oder gleich der Anzahl der Volumes im Quell-Node sein. Sie können einen Quell-Node mit 16 Objektspeicher-Volumes (rangedb) nicht auf einer Ziel-Storage-Appliance mit 12 Objektspeicher-Volumes klonen, selbst wenn die Ziel-Appliance über eine größere Kapazität als der Quell-Node verfügt. Die meisten Storage Appliances verfügen über 16 Objektspeicher-Volumes, außer der SGF6112 Storage Appliance mit nur 12 Objektspeicher-Volumes.

Welche Informationen sind nicht geklont?

Die folgenden Appliance-Konfigurationen werden beim Klonen nicht auf die Ersatz-Appliance übertragen. Sie müssen sie während der Ersteinrichtung des Ersatzgeräts konfigurieren.

- BMC Schnittstelle
- Netzwerkverbindungen
- Verschlüsselungsstatus der Nodes
- SANtricity System Manager (für Storage-Nodes)

- RAID-Modus (für Storage-Nodes)

Welche Probleme verhindern das Klonen?

Wenn beim Klonen eines der folgenden Probleme auftreten, stoppt der Klonprozess und eine Fehlermeldung wird erzeugt:

- Falsche Netzwerkkonfiguration
- Fehlende Konnektivität zwischen Quell- und Ziel-Appliances
- Nicht kompatibel mit Quell- und Ziel-Appliance
- Bei Storage-Nodes eine Ersatz-Appliance mit unzureichender Kapazität

Sie müssen jedes Problem lösen, damit das Klonen fortgesetzt werden kann.

Überlegungen und Anforderungen zum Klonen von Appliance-Nodes

Vor dem Klonen eines Appliance-Nodes müssen Sie die Überlegungen und Anforderungen verstehen.

Hardwareanforderungen für die Ersatz-Appliance

Stellen Sie sicher, dass das Ersatzgerät die folgenden Kriterien erfüllt:

- Der Quell-Node (eine Appliance, die ersetzt wird) und das Ziel-Appliance müssen denselben Appliance-Typ sein:
 - Sie können eine Admin-Node-Appliance oder eine Gateway-Node-Appliance nur auf einer neuen Services-Appliance klonen.
 - Sie können eine Storage-Node-Appliance nur auf einer neuen Storage Appliance klonen.
- Bei Admin-Node- oder Gateway-Node-Appliances müssen die Quell-Node-Appliance und die Ziel-Appliance nicht den gleichen Gerätetyp aufweisen. Bei einer Änderung des Gerätetyps müssen jedoch möglicherweise die Kabel oder SFP-Module ausgetauscht werden.

Sie können beispielsweise eine SG1000-Node-Appliance durch ein SG100 ersetzen oder eine SG100-Appliance durch eine SG1000-Appliance ersetzen.

- Bei Storage-Node-Appliances müssen die Quell-Node-Appliance und die Ziel-Appliance nicht den gleichen Appliance-Typ aufweisen. Folgendes gilt jedoch:
 - Die Ziel-Appliance muss über eine größere Speicherkapazität verfügen als die Quell-Appliance.
Beispielsweise kann eine SG5700 Node Appliance durch eine SG6000 Appliance ersetzt werden.
 - Die Ziel-Appliance muss eine gleiche oder größere Anzahl von Objekt-Storage-Volumes aufweisen als die Quell-Appliance.

Beispielsweise können Sie eine SG6000 Node-Appliance (16 Objektspeicher-Volumes) nicht durch eine SGF6112-Appliance (12 Objektspeicher-Volumes) ersetzen.

Wenden Sie sich an Ihren StorageGRID Vertriebsmitarbeiter, wenn Sie Unterstützung bei der Auswahl kompatibler Ersatzgeräte benötigen, um bestimmte Appliance-Nodes in Ihrer StorageGRID Installation zu klonen.

Das Klonen eines Appliance-Nodes wird vorbereitet

Vor dem Klonen eines Appliance-Node müssen Sie folgende Informationen haben:

- Beziehen Sie eine temporäre IP-Adresse für das Grid-Netzwerk von Ihrem Netzwerkadministrator zur Verwendung mit der Ziel-Appliance während der ersten Installation. Wenn der Quellknoten zu einem Admin-Netzwerk oder Client-Netzwerk gehört, erhalten Sie temporäre IP-Adressen für diese Netzwerke.

Temporäre IP-Adressen befinden sich normalerweise im selben Subnetz wie die zu klonende Quell-Node-Appliance und sind nach Abschluss des Klonens nicht erforderlich. Die Quell- und Ziel-Appliances müssen eine Verbindung zu dem primären Admin-Node Ihrer StorageGRID herstellen, um eine Klonverbindung herzustellen.

- Bestimmung des Netzwerks zum Klonen von Datenübertragungsdaten, das die beste Performance bei der Datenübertragung bietet, ohne die Leistung des StorageGRID-Netzwerks oder die Datenverfügbarkeit zu beeinträchtigen



Die Verwendung des 1-GbE-Admin-Netzwerks für die Übertragung von Klondaten führt zu langsamerem Klonen.

- Ermitteln, ob die Node-Verschlüsselung mithilfe eines Verschlüsselungsmanagement-Servers (KMS) auf der Ziel-Appliance verwendet wird, damit die Node-Verschlüsselung während der Erstinstallation der Ziel-Appliance vor dem Klonen aktiviert werden kann. Sie können prüfen, ob die Knotenverschlüsselung auf dem Quell-Appliance-Node aktiviert ist, wie in beschrieben "[Aktivieren der Node-Verschlüsselung](#)".

Der Quell- und die Ziel-Appliance können unterschiedliche Node-Verschlüsselungseinstellungen aufweisen. Die Entschlüsselung und Verschlüsselung der Daten erfolgt automatisch während des Datentransfers und beim Neustart des Ziel-Nodes und Beitritt zum Grid.

- Ermitteln Sie, ob der RAID-Modus auf der Ziel-Appliance von der Standardeinstellung geändert werden soll, damit Sie diese Informationen bei der Erstinstallation der Ziel-Appliance vor dem Klonen angeben können. Auf der Seite **NODES** im Grid Manager können Sie Informationen zum aktuellen RAID-Modus des Quell-Appliance-Knotens anzeigen. Wählen Sie die Registerkarte * Storage* für das Gerät aus.

Der Quell- und die Ziel-Appliance können unterschiedliche RAID-Einstellungen aufweisen.

- Planen Sie ausreichend Zeit, um den Node-Klonprozess abzuschließen. Für den Datentransfer von einem betrieblichen Storage Node zu einer Ziel-Appliance sind möglicherweise mehrere Tage erforderlich. Planen Sie das Klonen zu einer Zeit, die die Auswirkungen auf Ihr Geschäft minimiert.
- Sie sollten jeweils nur einen Appliance-Node klonen. Durch Klonen wird verhindert, dass Sie weitere StorageGRID-Wartungsarbeiten gleichzeitig ausführen.
- Nachdem Sie einen Appliance-Node geklont haben, können Sie die Quell-Appliance verwenden, die zu einem Installationszustand zurückgeschickt wurde, als Ziel, eine weitere kompatible Node-Appliance zu klonen.

Klon-Appliance-Node

Der Klonprozess kann mehrere Tage dauern, bis die Daten zwischen dem Quell-Node (Appliance, die ersetzt wird) und der Ziel-Appliance übertragen werden.

Bevor Sie beginnen

- Sie haben das kompatible Zielgerät in einem Schrank oder Rack installiert, alle Kabel angeschlossen und mit Strom versorgt.

- Sie haben überprüft, ob die Installationsversion für die StorageGRID Appliance auf der Ersatzanwendung mit der Softwareversion des StorageGRID-Systems übereinstimmt. Dabei müssen Sie ggf. die StorageGRID Appliance Installer-Firmware aktualisieren.
- Sie haben die Ziel-Appliance konfiguriert, einschließlich der Konfiguration von StorageGRID-Verbindungen, SANtricity System Manager (nur Storage Appliances) und der BMC-Schnittstelle.
 - Verwenden Sie beim Konfigurieren von StorageGRID-Verbindungen die temporären IP-Adressen.
 - Verwenden Sie bei der Konfiguration von Netzwerkverbindungen die abschließende Link-Konfiguration.



Lassen Sie das Installationsprogramm der StorageGRID Appliance nach Abschluss der Erstkonfiguration der Ziel-Appliance offen. Nach dem Start des Node-Klonprozesses kehren Sie zur Installationsseite der Zielanwendung zurück.

- Optional ist die Node-Verschlüsselung für die Ziel-Appliance aktiviert.
- Sie haben optional den RAID-Modus für die Ziel-Appliance eingestellt (nur Storage Appliances).
- Sie haben die geprüft "[Überlegungen und Anforderungen zum Klonen von Appliance-Nodes](#)".

Sie sollten jeweils nur einen Appliance-Node klonen, um die Netzwerk-Performance und Datenverfügbarkeit von StorageGRID zu erhalten.

Schritte

1. "[Platzieren Sie den Quellknoten, den Sie klonen, in den Wartungsmodus](#)".
2. Wählen Sie im StorageGRID-Appliance-Installationsprogramm auf dem Quellknoten im Abschnitt Installation der Startseite die Option **Klonen aktivieren** aus.

Der Abschnitt primäre Admin-Node-Verbindung wird durch den Abschnitt „Verbindung zum Ziel-Node klonen“ ersetzt.

Home

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

This Node

Node type: Storage ▾

Node name: hrmny2-1-254-sn

Cancel

Save

Clone target node connection

Clone target node IP: 0.0.0.0

Connection state: No connection information available.

Cancel

Save

Installation

Current state: Waiting for configuration and validation of clone target.

Start Cloning

Disable Cloning

- Geben Sie für **Zielknoten-IP** die temporäre IP-Adresse ein, die dem Zielknoten zugewiesen ist, das Netzwerk für den Datenverkehr der Klondatenübertragung verwenden soll, und wählen Sie dann **Speichern** aus.

Normalerweise geben Sie die IP-Adresse für das Grid-Netzwerk ein. Wenn Sie jedoch ein anderes Netzwerk für den Datenverkehr von Klondaten verwenden müssen, geben Sie die IP-Adresse des Zielknoten in diesem Netzwerk ein.



Die Verwendung des 1-GbE-Admin-Netzwerks für die Übertragung von Klondaten führt zu langsamerem Klonen.

Nachdem die Zielanwendung konfiguriert und validiert wurde, ist im Abschnitt Installation **Klonen starten** auf dem Quellknoten aktiviert.

Wenn Probleme bestehen, die das Klonen verhindern, ist **Klonen starten** nicht aktiviert und Probleme, die Sie lösen müssen, werden als **Verbindungsstatus** aufgeführt. Diese Probleme sind auf der Startseite des StorageGRID-Appliance-Installationsprogramms sowohl des Quell-Knotens als auch der Ziel-Appliance aufgeführt. Es wird immer nur ein Problem angezeigt, und der Status wird automatisch aktualisiert, wenn sich die Bedingungen ändern. Lösen Sie alle Klonprobleme, um **Klonen starten** zu aktivieren.

Wenn **Klonen starten** aktiviert ist, zeigt der **Aktueller Status** das zum Klonen des Datenverkehrs ausgewählte StorageGRID-Netzwerk sowie Informationen über die Verwendung dieser Netzwerkverbindung an. Siehe ["Überlegungen und Anforderungen zum Klonen von Appliance-Nodes"](#).

4. Wählen Sie **Klonen starten** auf dem Quellknoten aus.
5. Überwachen Sie den Klonfortschritt mit dem Installationsprogramm von StorageGRID Appliance auf dem Quell- oder Zielknoten.

Das Installationsprogramm der StorageGRID Appliance auf den Quell- und den Ziel-Nodes weist denselben Status auf.

NetApp® StorageGRID® Appliance Installer Help

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Monitor Cloning

1. Establish clone peering relationship		Complete
2. Clone another node from this node		Running
Step	Progress	Status
Send data to clone target node	<div style="width: 0%;"></div>	Sending data, 0% complete. 8.99 GB transferred
3. Activate cloned node and leave this one offline		Pending

Die Seite Klonen überwachen bietet detaillierte Fortschritte für jede Phase des Klonprozesses:

- **Aufbau einer Klon-Peering-Beziehung** zeigt den Fortschritt der Klonerstellung und -Konfiguration.
 - **Ein weiterer Knoten von diesem Knoten klonen** zeigt den Fortschritt der Datenübertragung an. (Dieser Teil des Klonprozesses kann mehrere Tage dauern.)
 - **Geklonter Knoten aktivieren und diesen offline lassen** zeigt den Fortschritt der Übertragung der Steuerung auf den Zielknoten und der Platzierung des Quellknoten in einen Pre-install Zustand, nachdem die Datenübertragung abgeschlossen ist.
6. Wenn Sie den Klonprozess beenden und den Quellknoten vor dem Abschluss des Klonens in den Dienst zurücksenden müssen, wechseln Sie auf dem Quellknoten zur Startseite des StorageGRID Appliance Installer und wählen Sie **Erweitert > Controller neu starten** aus, und wählen Sie dann **Neustart in StorageGRID** aus.

Wenn der Klonprozess beendet wird:

- Der Quell-Node beendet den Wartungsmodus und verbindet sich neu zu StorageGRID.
- Der Ziel-Node bleibt im Installationszustand. Um das Klonen des Quellknoten neu zu starten, starten Sie den Klonprozess erneut von Schritt 1.

Wenn das Klonen erfolgreich abgeschlossen wurde:

- Die Quell- und Ziel-Knoten tauschen IP-Adressen aus:
 - Der Zielknoten verwendet nun die IP-Adressen, die ursprünglich dem Quellknoten für Grid-, Admin- und Client-Netzwerke zugewiesen wurden.
 - Der Quellknoten verwendet jetzt die temporäre IP-Adresse, die dem Zielknoten ursprünglich zugewiesen wurde.
- Der Ziel-Node beendet den Wartungsmodus und tritt dem StorageGRID bei und ersetzt den Quell-Node.
- Die Quell-Appliance befindet sich in einem vorinstallierten Zustand, so als ob Sie es hätten **"Es für die**



Wenn das Gerät nicht wieder in das Raster integriert wird, wechseln Sie zur Startseite des StorageGRID-Appliance-Installationsprogramms für den Quellknoten, wählen Sie **Erweitert > Controller neu starten** und wählen Sie dann **Neustart im Wartungsmodus** aus. Nachdem der Quell-Node im Wartungsmodus neu gebootet wurde, wiederholen Sie den Vorgang des Node-Klonens.

- Benutzerdaten auf der Quell-Appliance bleiben als Wiederherstellungsoption, wenn bei dem Ziel-Node ein unerwartetes Problem auftritt. Nachdem der Ziel-Node der StorageGRID erneut beigetreten ist, sind die Benutzerdaten auf der Quell-Appliance veraltet und werden nicht mehr benötigt.

Veraltete Benutzerdaten werden überschrieben, wenn Sie die Quell-Appliance als neuen Node in einem anderen Grid installieren oder erweitern.

Sie können auch die Controller-Konfiguration auf der Quell-Appliance zurücksetzen, damit auf diese Daten nicht zugegriffen werden kann:

- a. Öffnen Sie das "[StorageGRID-Appliance-Installationsprogramm](#)" Für die Quell-Appliance, die die temporäre IP-Adresse verwendet, die ursprünglich dem Zielknoten zugewiesen wurde.
- b. Wählen Sie **Hilfe > Support und Debugging-Tools**.
- c. Wählen Sie **Speicher-Controller-Konfiguration Zurücksetzen**.



Wenden Sie sich bei Bedarf an den technischen Support, um Hilfe beim Zurücksetzen der Storage-Controller-Konfiguration zu erhalten.



Das Überschreiben der Daten oder das Zurücksetzen der Controller-Konfiguration erschwert oder unmöglich das Abrufen der veralteten Daten. Allerdings werden die Daten von keiner der beiden Methoden sicher aus der Quell-Appliance entfernt. Wenn eine sichere Löschung erforderlich ist, verwenden Sie ein Datenlösch-Werkzeug oder einen Dienst, um die Daten dauerhaft und sicher aus der Quell-Appliance zu entfernen.

Ihre Vorteile:

- Verwenden Sie die Quell-Appliance als Ziel für weitere Klonvorgänge: Es ist keine zusätzliche Konfiguration erforderlich. Dieser Appliance wurde bereits die temporäre IP-Adresse zugewiesen, die ursprünglich für das erste Klonziel angegeben wurde.
- Installieren und richten Sie die Quell-Appliance als neuen Appliance-Node ein.
- Entsorgen Sie die Quell-Appliance, wenn sie nicht mehr mit StorageGRID verwendet wird.

Instandhaltung der SGF6112 Hardware

SGF6112-Appliance warten

Möglicherweise müssen Sie Wartungsmaßnahmen an Ihrem Gerät durchführen. In diesem Abschnitt finden Sie spezifische Verfahren zur Wartung Ihrer SGF6112-Appliance.

Bei den in diesem Abschnitt beschriebenen Verfahren wird davon ausgegangen, dass die Appliance bereits als

Storage-Node in einem StorageGRID-System bereitgestellt wurde.

Konfigurationswartungsverfahren werden über den Appliance Installer, Grid Manager oder die BMC-Schnittstelle durchgeführt. Hierzu gehören folgende Verfahren:

- Schalten Sie die Appliance Identify-LED ein und aus
- Suchen Sie die Appliance im Datacenter
- Schalten Sie das Gerät aus
- Ändern Sie die Link-Konfiguration der Appliance

Hardware-Wartungsverfahren erfordern die physische Manipulation bestimmter SGF6112-Komponenten.

Upgrade der Laufwerk-Firmware

Die Firmware auf den Laufwerken im SGF6112 wird bei jedem Neustart des Geräts automatisch überprüft. Bei Bedarf wird die Firmware automatisch auf die Version aktualisiert, die von der aktuellen StorageGRID-Version erwartet wird. Firmware-Upgrades erfolgen in der Regel während Upgrades der StorageGRID Software. Alle notwendigen Upgrades der Laufwerk-Firmware für bestehende StorageGRID-Versionen werden in Hotfixes integriert. Befolgen Sie die Anweisungen, die jedem Hotfix beiliegen, um sicherzustellen, dass das Upgrade auf alle Laufwerke angewendet wird, die davon profitieren könnten.



SANtricity System Manager ist nicht für die Wartung der SGF6112 Appliance erforderlich.

Allgemeine Wartungsverfahren

Siehe "[Allgemeine Wartungsverfahren](#)" Für Verfahren, die für alle Appliances gleich sind, wie z. B. das Anwenden eines Hotfix, das Wiederherstellen eines Knotens oder Standorts und das Durchführen von Netzwerkwartungen.

Siehe "[Appliance-Hardware einrichten](#)" Für Gerätewartungsverfahren, die auch während der Erstinstallation und -Konfiguration der Appliance durchgeführt werden.

Konfigurationswartungsverfahren

Schalten Sie die Appliance Identify-LED ein und aus

Die blaue Identifizieren-LED auf der Vorder- und Rückseite des Geräts kann eingeschaltet werden, um das Gerät in einem Rechenzentrum zu lokalisieren.

Bevor Sie beginnen

Sie haben die BMC-IP-Adresse der Appliance, die Sie identifizieren möchten.

Schritte

1. Rufen Sie die BMC-Schnittstelle des Geräts auf.
2. Wählen Sie **Server Identify** Aus.

Der aktuelle Status der Identifizieren-LED ist ausgewählt.

3. Wählen Sie **EIN** oder **AUS**, und wählen Sie dann **Aktion ausführen**.

Wenn Sie **EIN** auswählen, leuchten die blauen Identifizieren-LEDs auf der Vorderseite (abgebildet) und der

Rückseite des Geräts.



Wenn eine Blende auf dem Controller installiert ist, kann es schwierig sein, die vordere Identify-LED zu erkennen.

4. Schalten Sie die LED nach Bedarf ein und aus.

Verwandte Informationen

["Suchen Sie die Appliance im Datacenter"](#)

["Greifen Sie auf die BMC-Schnittstelle zu"](#)

Suchen Sie die Appliance im Datacenter

Suchen Sie die Appliance, sodass Sie Hardware-Wartungsarbeiten oder -Upgrades durchführen können.

Bevor Sie beginnen

- Sie haben festgelegt, welches Gerät gewartet werden muss.
- Um die Appliance in Ihrem Rechenzentrum zu finden, ["Schalten Sie die blaue Identify-LED ein"](#).

Schritte

1. Finden Sie die Appliance im Rechenzentrum.

- Achten Sie darauf, dass die blaue Identifizieren-LED auf der Vorderseite oder Rückseite des Geräts leuchtet.

Die ID-LED auf der Vorderseite befindet sich hinter der Frontblende und ist möglicherweise schwer zu erkennen, ob die Blende installiert ist.



- Überprüfen Sie anhand der an der Vorderseite des Geräts angebrachten Etiketten, ob Sie das richtige Gerät gefunden haben.
- 2. Entfernen Sie gegebenenfalls die Frontverkleidung, um Zugang zu den Bedienelementen und Anzeigen auf der Vorderseite zu erhalten.
- 3. Schalten Sie die blaue Identifizieren-LED aus, wenn Sie sie zur Lokalisierung des Geräts verwendet haben.
 - Drücken Sie den Identifizieren-LED-Schalter an der Vorderseite des Geräts.
 - Verwenden Sie die BMC-Schnittstelle des Geräts.

Fahren Sie die SGF6112-Appliance herunter

Fahren Sie die Appliance herunter, um eine Hardwarewartung durchzuführen.

Bevor Sie beginnen

- Das ist schon "[Das Gerät befindet sich physisch](#)".

Über diese Aufgabe

Um Serviceunterbrechungen zu vermeiden, fahren Sie die Appliance während eines geplanten Wartungsfensters herunter, wenn normalerweise mit Serviceunterbrechungen zu rechnen ist.

Schritte

1. Fahren Sie das Gerät herunter:



Sie müssen ein kontrolliertes Herunterfahren des Geräts durchführen, indem Sie die unten angegebenen Befehle eingeben. Es ist eine Best Practice, nach Möglichkeit eine kontrollierte Abschaltung durchzuführen, um unnötige Warnmeldungen zu vermeiden, sicherzustellen, dass vollständige Protokolle verfügbar sind und Serviceunterbrechungen zu vermeiden.

- a. Wenn Sie sich noch nicht beim Grid-Knoten angemeldet haben, melden Sie sich mit PuTTY oder einem anderen ssh-Client an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

b. Schalten Sie das Gerät aus:

shutdown -h now

Dieser Befehl kann bis zu 10 Minuten in Anspruch nehmen.

2. Überprüfen Sie anhand einer der folgenden Methoden, ob das Gerät ausgeschaltet ist:

- Sehen Sie sich die LED-Betriebsanzeige an der Vorderseite des Geräts an, und vergewissern Sie sich, dass sie ausgeschaltet ist.
- Überprüfen Sie auf der Seite Power Control der BMC-Schnittstelle, ob das Gerät ausgeschaltet ist.

Schalten Sie SGF6112 ein, und überprüfen Sie den Betrieb

Schalten Sie den Controller nach dem Abschluss der Wartung ein.

Bevor Sie beginnen

- Der Controller wurde in einem Rack oder Rack installiert und die Daten- und Stromkabel angeschlossen.

["Setzen Sie den SGF6112-Controller wieder in den Schrank oder das Rack ein"](#)

- Der Controller befindet sich physisch im Datacenter.

["SGF6112 Appliance im Datacenter lokalisieren"](#)

Schritte

1. Schalten Sie das Gerät ein.

Möglicherweise müssen Sie die Blende entfernen, um auf den Netzschalter zugreifen zu können. Wenn dies der Fall ist, müssen Sie sie anschließend wieder einbauen.

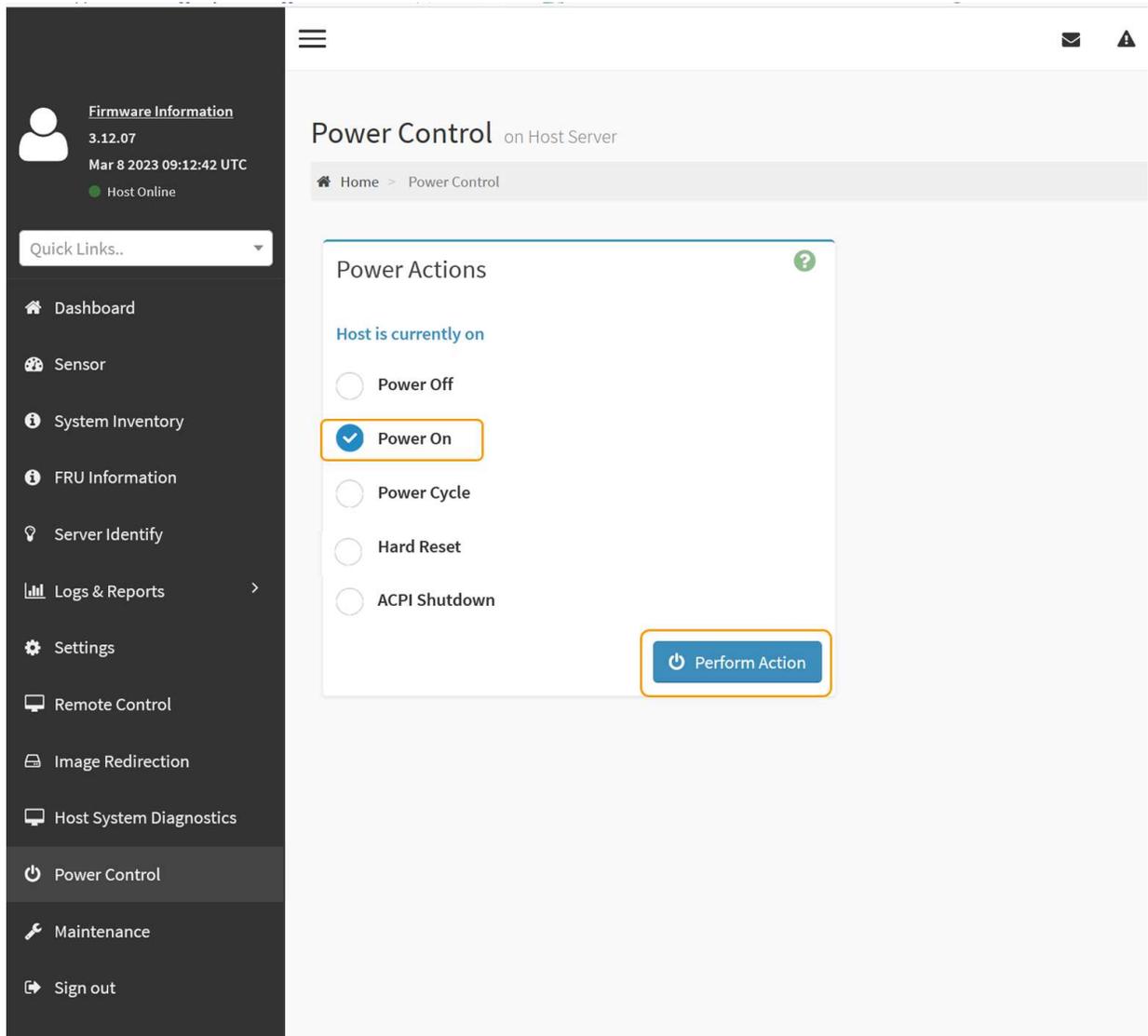
2. Überwachen Sie die Controller-LEDs und die Startcodes mit einer der folgenden Methoden:

- Drücken Sie den Netzschalter an der Vorderseite des Controllers.
- Verwenden Sie die BMC-Schnittstelle des Controllers:
 - i. Greifen Sie auf die BMC-Schnittstelle des Controllers zu.

["Greifen Sie auf die BMC-Schnittstelle zu"](#)

ii. Wählen Sie **Power Control**.

iii. Wählen Sie **Einschalten** und dann **Aktion ausführen**.



Verwenden Sie die BMC-Schnittstelle, um den Startstatus zu überwachen.

3. Vergewissern Sie sich, dass der Appliance-Controller im Grid Manager und ohne Warnungen angezeigt wird.

Es kann bis zu 20 Minuten dauern, bis der Controller im Grid Manager angezeigt wird.



Nehmen Sie einen anderen Appliance-Node nur offline, wenn diese Appliance über ein grünes Symbol verfügt.

4. Vergewissern Sie sich, dass die neue Appliance vollständig betriebsbereit ist, indem Sie sich beim Grid-Node über PuTTY oder einen anderen ssh-Client anmelden:
 - a. Geben Sie den folgenden Befehl ein: `ssh Appliance_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

Verwandte Informationen

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

Ändern der Link-Konfiguration der SGF6112-Appliance

Sie können die Ethernet-Link-Konfiguration der Appliance ändern, einschließlich des Port Bond-Modus, des Netzwerk-Bond-Modus und der Verbindungsgeschwindigkeit.

Bevor Sie beginnen

- Das ist schon ["Das Gerät in den Wartungsmodus versetzt"](#).



In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den Wartungsmodus versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren > Link-Konfiguration** aus.

2. Nehmen Sie die gewünschten Änderungen an der Verbindungskonfiguration vor.

Weitere Informationen zu den Optionen finden Sie unter ["Netzwerkverbindungen konfigurieren"](#).

3. Wenn Sie mit Ihrer Auswahl zufrieden sind, klicken Sie auf **Speichern**.



Wenn Sie Änderungen am Netzwerk oder an der Verbindung vorgenommen haben, über die Sie verbunden sind, können Sie die Verbindung verlieren. Wenn die Verbindung nicht innerhalb von 1 Minute wiederhergestellt wird, geben Sie die URL für den StorageGRID-Appliance-Installer erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind: **https://appliance_IP:8443**

4. Nehmen Sie alle erforderlichen Änderungen an den IP-Adressen der Appliance vor.

Wenn Sie Änderungen an den VLAN-Einstellungen vorgenommen haben, hat sich das Subnetz für die Appliance möglicherweise geändert. Informationen zum Ändern der IP-Adressen für die Appliance finden Sie unter ["Konfigurieren Sie StorageGRID-IP-Adressen"](#).

5. Wählen Sie im Menü die Option **Netzwerk konfigurieren > Ping-Test** aus.

6. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in Netzwerken zu prüfen, die möglicherweise von den Änderungen der Verbindungskonfiguration betroffen sind, die Sie bei der Konfiguration der Appliance vorgenommen haben.

Zusätzlich zu allen anderen Tests, die Sie durchführen möchten, bestätigen Sie, dass Sie die Grid Network IP-Adresse des primären Admin-Knotens und die Grid-Netzwerk-IP-Adresse von mindestens einem anderen Knoten pinggen können. Gehen Sie gegebenenfalls zu den Anweisungen für die Konfiguration von Netzwerkverbindungen zurück, und beheben Sie etwaige Probleme.

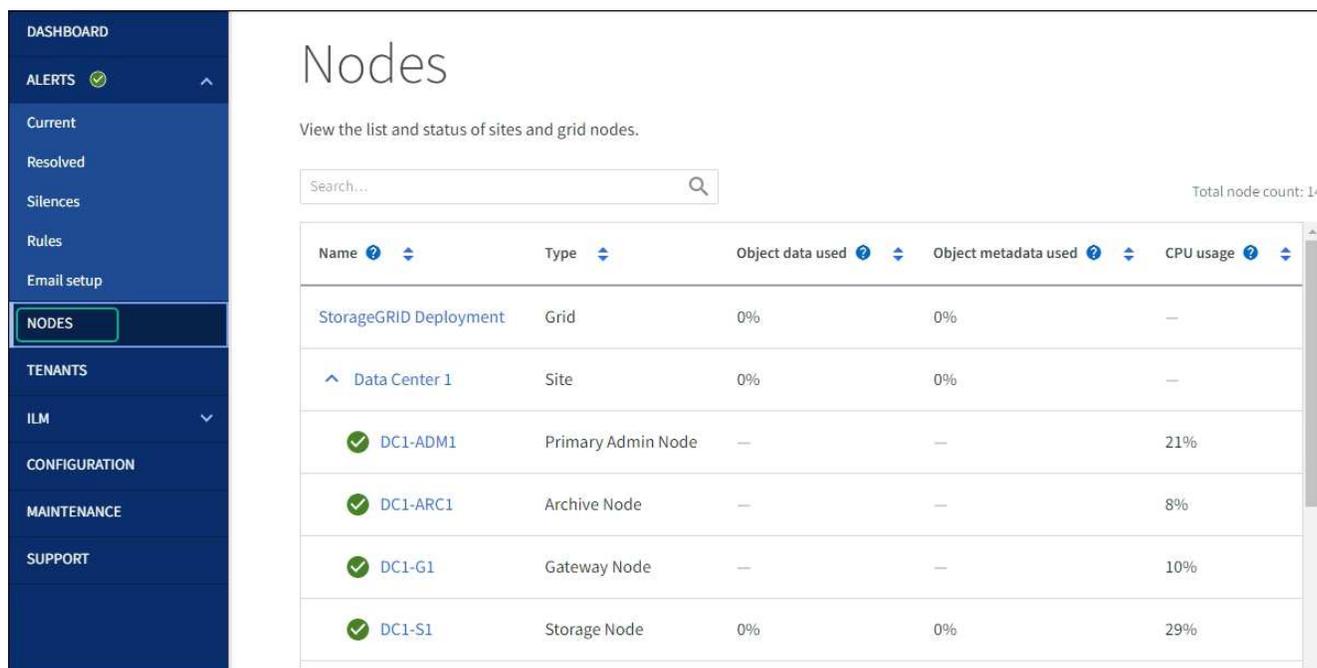
7. Sobald Sie zufrieden sind, dass die Änderungen an der Link-Konfiguration funktionieren, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

- Wählen Sie **Neustart in StorageGRID** aus, um den Compute-Controller neu zu starten, wenn der Knoten wieder dem Grid hinzugefügt wird. Wählen Sie diese Option, wenn Sie im Wartungsmodus ausgeführt werden und den Node in den normalen Betrieb zurückkehren möchten.

- Wählen Sie **Neustart im Wartungsmodus**, um den Compute-Controller neu zu starten, wobei der Knoten im Wartungsmodus verbleibt. (Diese Option ist nur verfügbar, wenn sich der Controller im Wartungsmodus befindet.) Wählen Sie diese Option aus, wenn zusätzliche Wartungsmaßnahmen auf dem Node ausgeführt werden müssen, bevor er dem Grid erneut beitreten kann.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden (✓ Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.



Hardware-Wartungsverfahren

Prüfen Sie, ob die Komponente im SGF6112 ausgetauscht werden soll

Wenn Sie sich nicht sicher sind, welche Hardwarekomponente in Ihrem Gerät ausgetauscht werden soll, gehen Sie wie folgt vor, um die Komponente und den Standort

des Geräts im Rechenzentrum zu identifizieren.

Bevor Sie beginnen

- Sie haben die Seriennummer der Speicher-Appliance, bei der die Komponente ausgetauscht werden muss.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

Gehen Sie wie folgt vor, um das Gerät mit fehlerhafter Hardware zu identifizieren und zu ermitteln, welche der folgenden austauschbaren Hardwarekomponenten nicht ordnungsgemäß funktioniert:

- Netzteile
- Lüfter
- Solid State-Laufwerke (SSDs)
- Netzwerkschnittstellenkarten (NICs)
- CMOS-Batterie

Schritte

1. Identifizieren Sie die fehlerhafte Komponente und den Namen der Appliance, in der sie installiert ist.
 - a. Wählen Sie im Grid-Manager **ALERTS** > **Current** aus.

Die Seite „Meldungen“ wird angezeigt.

- b. Wählen Sie die Warnmeldung aus, um die Warnungsdetails anzuzeigen.



Wählen Sie die Meldung und nicht die Überschrift einer Gruppe von Warnungen aus.

- c. Notieren Sie den Node-Namen und die eindeutige Identifizierungsbezeichnung der ausgefallenen Komponente.

Appliance NIC fault detected

A problem with a network interface card (NIC) in the appliance was detected.

Recommended actions

1. Reseat the NIC. Refer to the instructions for your appliance.
2. If necessary, replace the NIC. See the maintenance instructions for your appliance.

Time triggered

2023-02-17 13:36:31 EST (2023-02-17 18:36:31 UTC)

Status

Active (silence this alert )

Site / Node

Data Center 1 **SGF6112-032-X6606A**

Severity

 Critical

Description

ConnectX-6 Lx EN adapter card,
25GbE, Dual-port SFP28, PCIe 4.0 x8,
No Crypto

Firmware Version

26.33.1048 (MT_0000000531)

Device

hic3

Part number

X1153A

2. Identifizieren Sie das Gehäuse mit der zu ersetzenden Komponente.

- a. Wählen Sie im Grid Manager die Option **NODES** aus.
- b. Wählen Sie in der Tabelle auf der Seite Nodes den Namen des Appliance-Storage-Node mit der fehlerhaften Komponente aus.
- c. Wählen Sie die Registerkarte **Hardware** aus.

Überprüfen Sie die Seriennummer * des Compute-Controllers im Abschnitt StorageGRID-Gerät. Überprüfen Sie, ob die Seriennummer mit der Seriennummer des Speichergeräts übereinstimmt, in dem Sie die Komponente austauschen. Wenn die Seriennummer übereinstimmt, haben Sie das richtige Gerät gefunden.

StorageGRID Appliance

Appliance model: ?	SGF6112	
Storage controller failed drive count: ?	2	
Storage data drive type: ?	SSD	
Storage data drive size: ?	1.92 TB	
Storage RAID mode: ?	MRAIDA [failed SSD in slot 7 (lower), 8 (upper)]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Degraded	
Compute controller BMC IP: ?	10.227.102.100	
Compute controller serial number: ?	703C RNL M1020M.	
Compute hardware: ?	Needs Attention	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Failed	
Compute controller power supply B: ?	Nominal	

- Wenn der Abschnitt StorageGRID-Appliance in Grid-Manager nicht angezeigt wird, ist der ausgewählte Knoten keine StorageGRID-Appliance. Wählen Sie einen anderen Knoten in der Strukturansicht aus.
- Wenn die Seriennummern nicht übereinstimmen, wählen Sie einen anderen Knoten aus der Strukturansicht aus.

3. Nachdem Sie den Knoten gefunden haben, an dem die Komponente ersetzt werden muss, notieren Sie sich die BMC-IP-Adresse der Appliance, die im Abschnitt StorageGRID-Appliance aufgeführt ist.

Um die Appliance im Rechenzentrum zu lokalisieren, können Sie die BMC-IP-Adresse verwenden, um die LED für die Geräteidentifizierung einzuschalten.

"Schalten Sie die LED für die Geräteidentifizierung ein und aus"

Ersetzen Sie ein oder beide Netzteile im SGF6112-Gerät

Die SGF6112 Appliance verfügt über zwei Netzteile für Redundanz. Wenn eines der Netzteile ausfällt, müssen Sie es so schnell wie möglich austauschen, um sicherzustellen, dass das Gerät über eine redundante Stromversorgung verfügt. Beide Netzteile, die im Gerät betrieben werden, müssen das gleiche Modell und die gleiche Nennleistung aufweisen.

Bevor Sie beginnen

- Das ist schon "[Das Gerät befindet sich physisch](#)" Bei zu ersetzenden Netzteilen.
- Das ist schon "[Standort des zu ersetzenden Netzteils ermittelt](#)".
- Wenn Sie nur ein Netzteil ersetzen:

- Sie haben das Ersatznetzteil entpackt und sichergestellt, dass es das gleiche Modell und die gleiche Stromleistung wie das Netzteil ist, das Sie ersetzen.
- Sie haben bestätigt, dass das andere Netzteil installiert ist und in Betrieb ist.
- Wenn Sie beide Netzteile gleichzeitig ersetzen:
 - Sie haben die Ersatz-Netzteile entpackt und sichergestellt, dass sie das gleiche Modell und die gleiche Wattzahl haben.

Über diese Aufgabe

Die Abbildung zeigt die beiden Netzteile für den SGF6112. Die Netzteile sind von der Rückseite des Geräts zugänglich.



Schritte

1. Wenn Sie nur ein Netzteil ersetzen, müssen Sie das Gerät nicht herunterfahren. Wechseln Sie zum [Ziehen Sie das Netzkabel ab](#) Schritt: Wenn Sie beide Netzteile gleichzeitig ersetzen, gehen Sie folgendermaßen vor, bevor Sie die Netzkabel abziehen:
 - a. ["Schalten Sie das Gerät aus"](#).

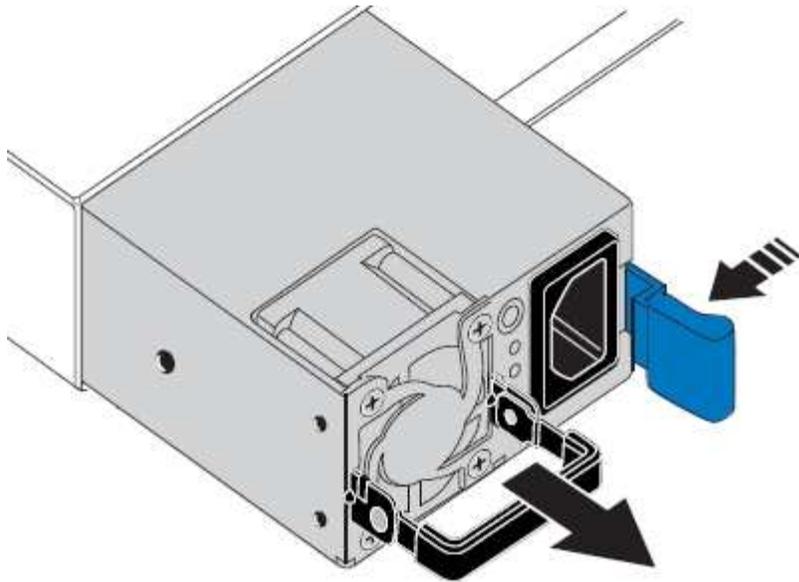


Wenn Sie jemals eine ILM-Regel verwendet haben, die nur eine Kopie eines Objekts erstellt und beide Netzteile gleichzeitig austauschen, müssen Sie die Netzteile während eines geplanten Wartungsfensters austauschen. Andernfalls verlieren Sie während dieses Verfahrens vorübergehend den Zugriff auf diese Objekte. Siehe Informationen zu ["Warum sollten Sie die Single-Copy-Replizierung nicht verwenden"](#).

2. `[[Trenne den Netzstecker_Power_cordel, Start=2]]` Trennen Sie das Netzkabel von jedem zu ersetzenden Netzteil.

Von der Rückseite des Geräts aus gesehen befindet sich das Netzteil A (PSU0) auf der rechten Seite und das Netzteil B (PSU1) auf der linken Seite.

3. Heben Sie den Griff am ersten zu ersetzenden Netzteil an.
4. Drücken Sie auf den blauen Riegel, und ziehen Sie das Netzteil heraus.



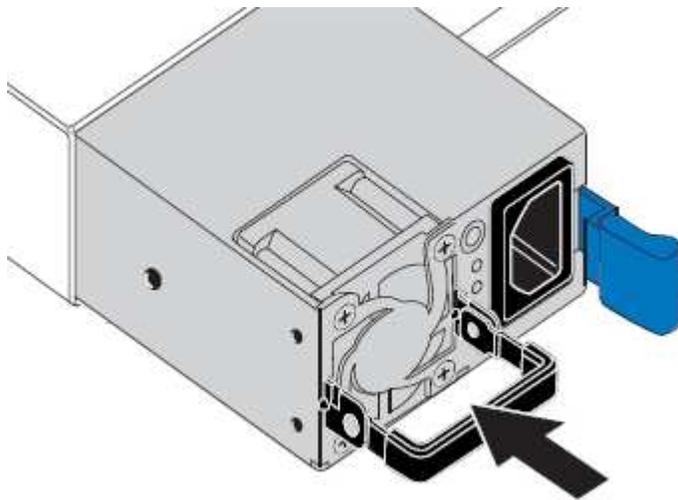
5. Schieben Sie das Ersatznetzteil mit der blauen Verriegelung nach rechts in das Gehäuse.



Beide Netzteile müssen das gleiche Modell und die gleiche Wattzahl haben.

Stellen Sie sicher, dass sich die blaue Verriegelung auf der rechten Seite befindet, wenn Sie die Ersatzeinheit einschieben.

Sie werden ein Klicken spüren, wenn das Netzteil einrastet.



6. Drücken Sie den Griff wieder gegen das Gehäuse des Netzteils.

7. Wenn Sie beide Netzteile austauschen, wiederholen Sie die Schritte 2 bis 6, um das zweite Netzteil auszutauschen.

8. **"Schließen Sie die Stromkabel an die ersetzten Geräte an, und wenden Sie Strom an".**

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Ersetzen Sie den Lüfter in einem SGF6112-Gerät

Das SGF6112-Gerät verfügt über acht Lüfter. Wenn einer der Lüfter ausfällt, müssen Sie

ihn so schnell wie möglich austauschen, um sicherzustellen, dass das Gerät ordnungsgemäß gekühlt wird.

Bevor Sie beginnen

- Sie haben den richtigen Ersatzlüfter.
- Sie haben die Position des zu ersetzenden Lüfters festgelegt.

"Überprüfen Sie die zu ersetzenKomponenten"

- Sie haben die SGF6112-Appliance physisch angeordnet, bei der der Lüfter im Datacenter ausgetauscht wird.

"Suchen Sie die Appliance im Datacenter"



A ["Kontrolliertes Herunterfahren des Geräts"](#) Ist erforderlich, bevor Sie das Gerät aus dem Rack entfernen.

- Sie haben alle Kabel getrennt und die Geräteabdeckung entfernt.

"Entfernen Sie die Abdeckung des SGF6112"

- Sie haben bestätigt, dass die anderen Lüfter installiert sind und ausgeführt werden.

Über diese Aufgabe

Um Serviceunterbrechungen zu vermeiden, vergewissern Sie sich, dass alle anderen Storage-Nodes mit dem Grid verbunden sind, bevor Sie den Lüfteraustausch starten oder den Lüfter während eines geplanten Wartungsfensters austauschen, wenn normalerweise Serviceunterbrechungen zu erwarten sind. Weitere Informationen finden Sie unter ["Monitoring der Verbindungsstatus der Nodes"](#).



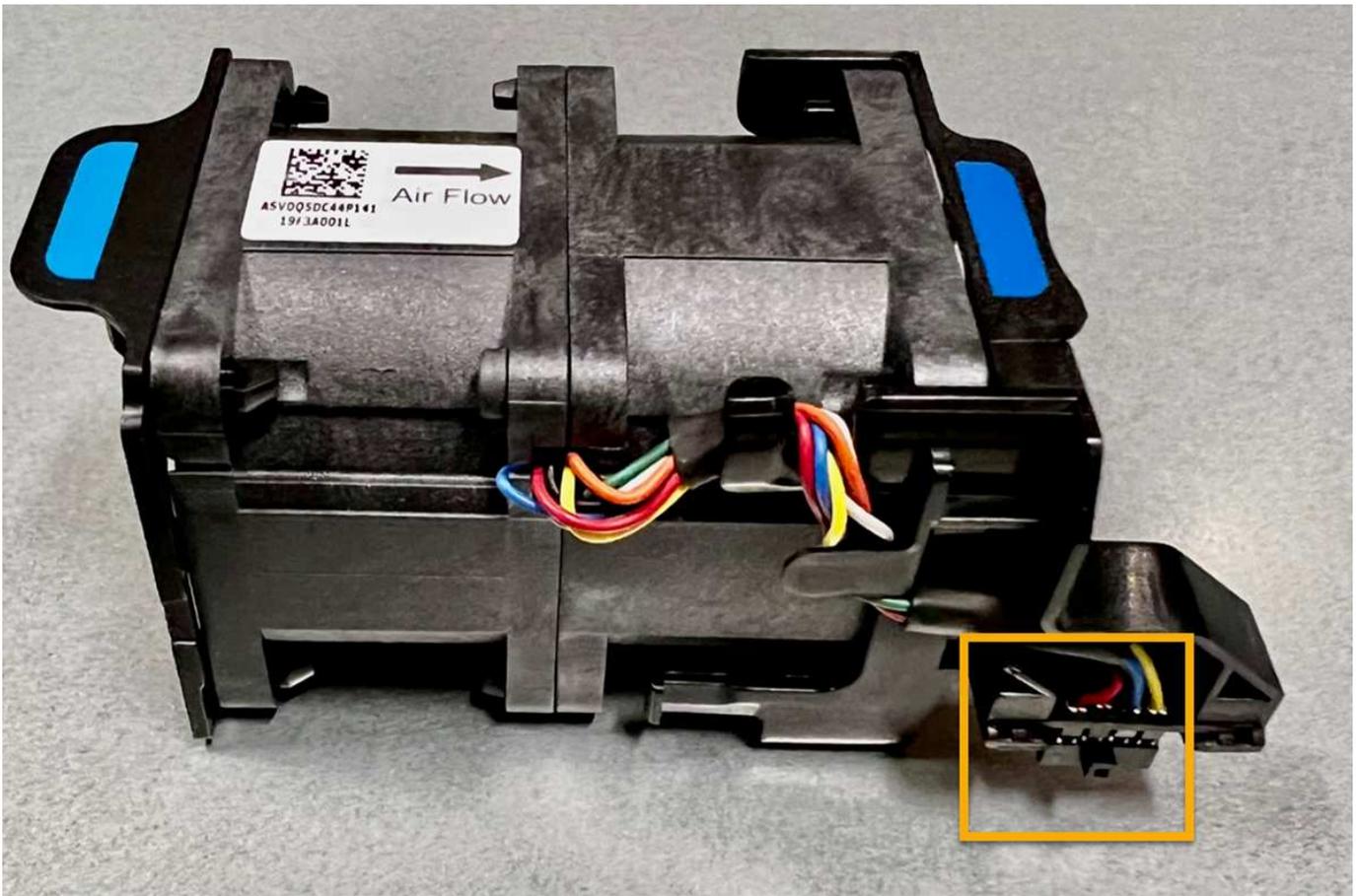
Wenn Sie jemals eine ILM-Regel verwendet haben, die nur eine Kopie eines Objekts erstellt, müssen Sie den Lüfter während eines geplanten Wartungsfensters ersetzen. Andernfalls verlieren Sie während dieses Verfahrens vorübergehend den Zugriff auf diese Objekte. Siehe Informationen zu ["Warum sollten Sie die Single-Copy-Replizierung nicht verwenden"](#).

Auf den Geräteknoten kann nicht zugegriffen werden, wenn Sie den Lüfter austauschen.

Das Foto zeigt einen Ventilator für das Gerät. Der elektrische Anschluss ist markiert. Die Kühllüfter sind zugänglich, nachdem Sie die obere Abdeckung aus dem Gerät nehmen.



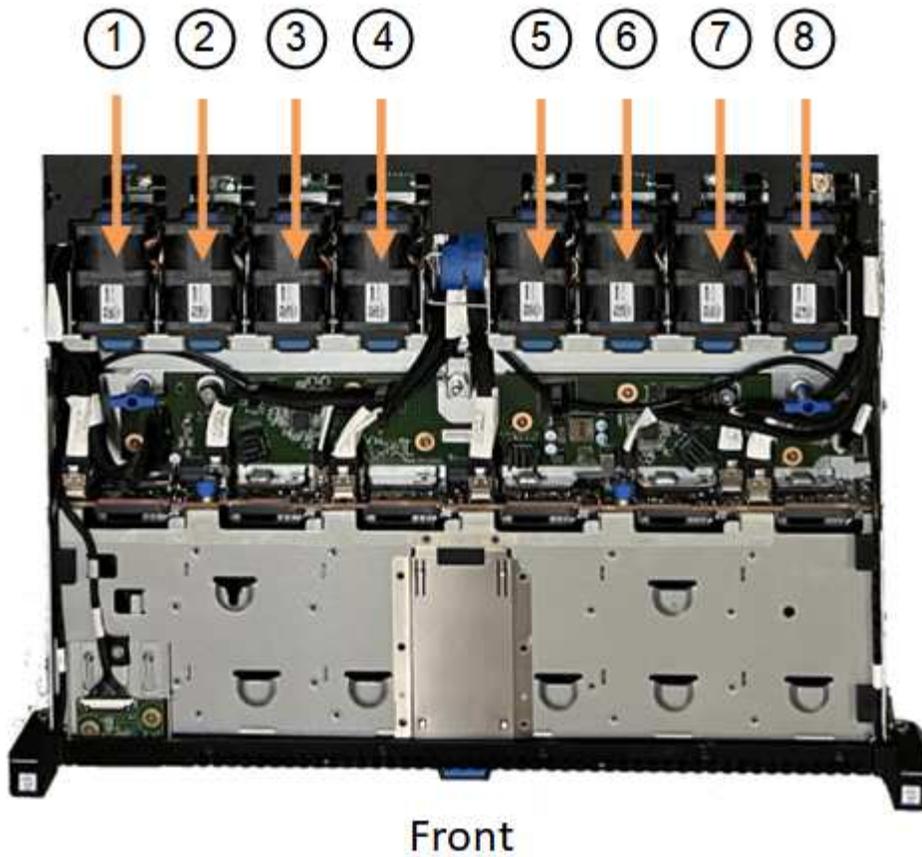
Jede der beiden Netzteile enthält zudem einen Lüfter. Die Netzteil Lüfter sind in diesem Verfahren nicht enthalten.



Schritte

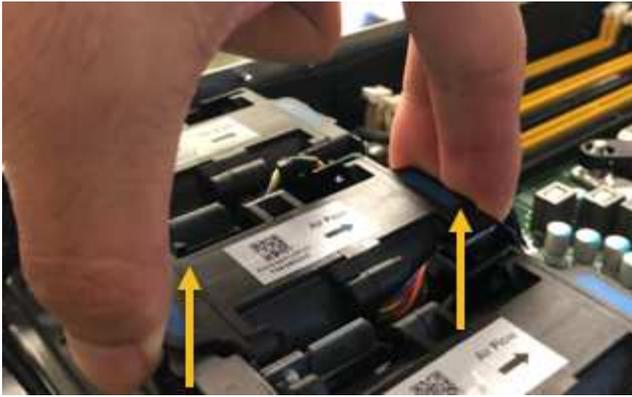
1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Suchen Sie den Lüfter, den Sie ersetzen müssen.

Die acht Lüfter befinden sich in den folgenden Positionen im Gehäuse (vordere Hälfte des SGF6112 mit entfernter oberer Abdeckung):



	Lüftereinheit
1	Fan_SYS0
2	Fan_SYS1
3	Fan_SYS2
4	Fan_SYS3
5	Fan_SYS4
6	Fan_SYS5
7	Fan_SYS6
8	Fan_SYS7

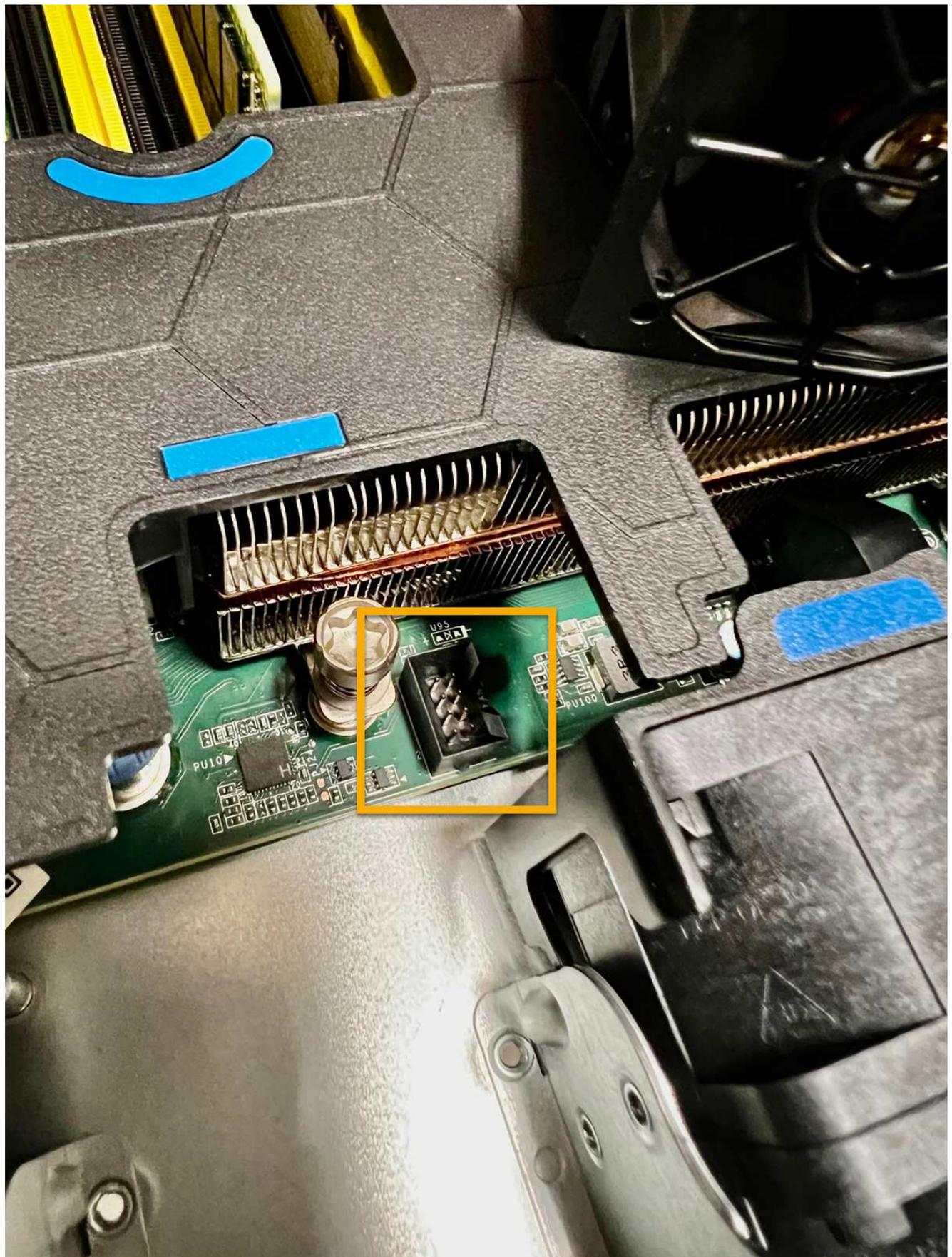
1. Heben Sie den defekten Lüfter mithilfe der blauen Laschen am Lüfter aus dem Gehäuse.



2. Schieben Sie den Ersatzlüfter in den offenen Steckplatz des Gehäuses.

Stellen Sie sicher, dass der Anschluss am Lüfter an der Buchse in der Platine ausgerichtet ist.

3. Drücken Sie den Lüfteranschluss fest in die Platine (Buchse hervorgehoben).



4. Setzen Sie die obere Abdeckung wieder auf das Gerät, und drücken Sie die Verriegelung nach unten, um die Abdeckung zu sichern.

5. Schalten Sie das Gerät ein, und überwachen Sie die Geräte-LEDs und die Startcodes.

Verwenden Sie die BMC-Schnittstelle, um den Boot-up-Status zu überwachen.

6. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Ersetzen Sie die Laufwerke in der SGF6112-Appliance

Die SGF6112 Storage Appliance enthält 12 SSD-Laufwerke. Die Daten auf den Laufwerken werden durch ein RAID-Schema geschützt, mit dem die Appliance nach dem Ausfall eines einzelnen Laufwerks wiederherstellen kann, ohne dass die Daten von einem anderen Node kopiert werden müssen.

Wenn ein zweites Laufwerk ausfällt, bevor ein erster Laufwerksausfall behoben wurde, müssen möglicherweise Daten von anderen Nodes kopiert werden, um die Redundanz wiederherzustellen. Diese Wiederherstellung von Redundanz kann länger dauern – was möglicherweise nicht möglich ist, wenn ILM-Regeln mit einer einzigen Kopie verwendet werden oder in der Vergangenheit verwendet wurden oder wenn die Datenredundanz durch Ausfälle auf anderen Nodes beeinträchtigt wurde. Wenn daher eines der SGF6112-Laufwerke ausfällt, müssen Sie es so schnell wie möglich austauschen, um Redundanz zu gewährleisten.

Bevor Sie beginnen

- Das ist schon "[Das Gerät befindet sich physisch](#)".
- Sie haben überprüft, welches Laufwerk ausgefallen ist, indem Sie feststellen, dass die linke LED des Laufwerks gelb leuchtet oder den Grid Manager für verwenden "[Zeigen Sie die Warnung an, die durch das ausgefallene Laufwerk verursacht wurde](#)".



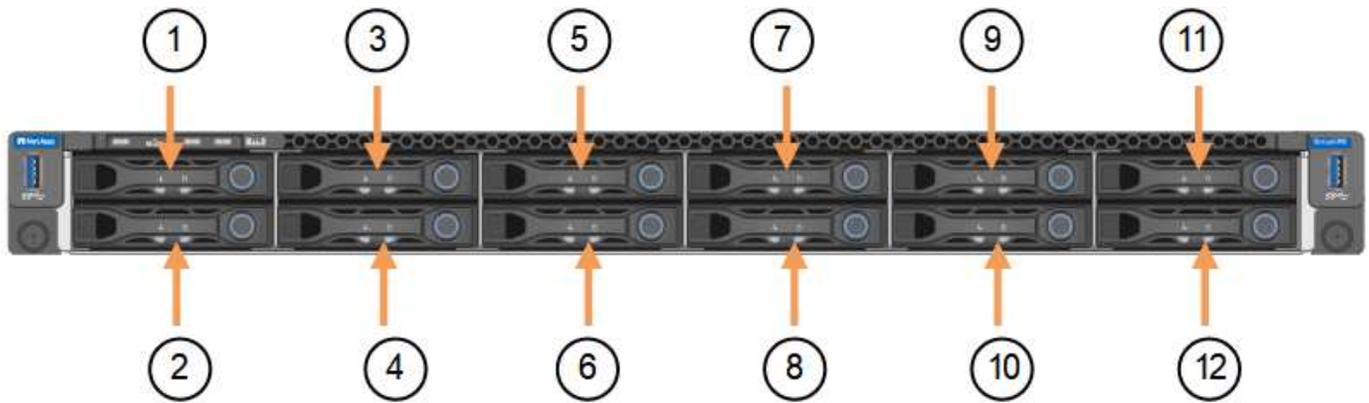
Informationen zur Anzeige von Statusanzeigen zur Überprüfung des Fehlers finden Sie unter.

- Sie haben das Ersatzlaufwerk erhalten.
- Sie haben einen angemessenen ESD-Schutz erhalten.

Schritte

1. Stellen Sie sicher, dass die linke Fehler-LED des Laufwerks gelb leuchtet, oder verwenden Sie die Laufwerksteckplatz-ID aus der Warnmeldung, um das Laufwerk zu finden.

Die zwölf Laufwerke befinden sich in den folgenden Positionen im Gehäuse (Vorderseite des Gehäuses mit entfernter Blende):



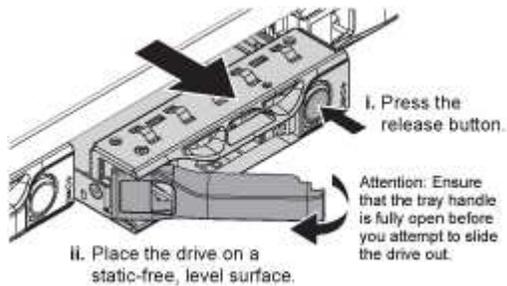
Position	Laufwerk
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

Sie können den Grid Manager auch verwenden, um den Status der SSD-Laufwerke zu überwachen. Wählen Sie **KNOTEN**. Wählen Sie anschließend aus **Storage Node > Hardware**. Wenn ein Laufwerk ausgefallen ist, enthält das Feld Speicher-RAID-Modus eine Meldung darüber, welches Laufwerk ausgefallen ist.

1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Packen Sie das Ersatzlaufwerk aus und legen Sie es in der Nähe des Geräts auf eine statische, Ebene Fläche.

Alle Verpackungsmaterialien speichern.

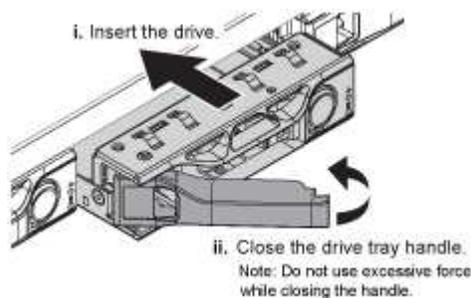
3. Drücken Sie die Entriegelungstaste am ausgefallenen Laufwerk.



Der Griff an den Antriebsfedern öffnet sich teilweise, und das Laufwerk löst sich aus dem Schlitz.

4. Öffnen Sie den Griff, schieben Sie das Laufwerk heraus und legen Sie es auf eine statisch freie, Ebene Oberfläche.
5. Drücken Sie die Entriegelungstaste am Ersatzlaufwerk, bevor Sie es in den Laufwerkschacht einsetzen.

Die Verriegelungsfedern öffnen sich.



6. Setzen Sie das Ersatzlaufwerk in den Steckplatz ein, und schließen Sie dann den Laufwerkgriff.



Beim Schließen des Griffs keine übermäßige Kraft anwenden.

Wenn das Laufwerk vollständig eingesetzt ist, hören Sie einen Klick.

Das ersetzte Laufwerk wird automatisch mit gespiegelten Daten von den Arbeitslaufwerken neu aufgebaut. Die Laufwerk-LED blinkt zunächst, hört aber auf zu blinken, sobald das System feststellt, dass das Laufwerk über genügend Kapazität verfügt und funktionsfähig ist.

Sie können den Status der Neuerstellung mithilfe des Grid Manager überprüfen.

7. Wenn mehr als ein Laufwerk ausgefallen und ersetzt wurde, haben Sie möglicherweise Warnmeldungen, die darauf hinweisen, dass einige Volumes Daten wiederherstellen müssen. Wenn Sie eine Warnmeldung erhalten, wählen Sie vor dem Versuch, eine Volume-Wiederherstellung durchzuführen, **NODES > appliance Storage Node > Hardware**. Überprüfen Sie im Abschnitt StorageGRID-Appliance auf der Seite, ob der Speicher-RAID-Modus ordnungsgemäß ist oder neu erstellt wird. Wenn im Status ein oder mehrere ausgefallene Laufwerke aufgeführt sind, korrigieren Sie diese Bedingung, bevor Sie eine Wiederherstellung des Volumes durchführen.
8. Gehen Sie im Grid Manager zu **NODES > appliance Storage Node > Hardware**. Überprüfen Sie im Abschnitt StorageGRID-Gerät auf der Seite, ob der Speicher-RAID-Modus ordnungsgemäß funktioniert.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Ersetzen Sie die NIC im SGF6112

Möglicherweise müssen Sie eine Netzwerkschnittstellenkarte (NIC) in der SGF6112 austauschen, wenn sie nicht optimal funktioniert oder ausgefallen ist.

Mit diesen Verfahren können Sie:

- Entfernen Sie die NIC
- Installieren Sie die NIC neu

Entfernen Sie die NIC

Bevor Sie beginnen

- Sie haben die richtige Ersatz-NIC.
- Sie haben den Speicherort der zu ersetzenden NIC festgelegt.

["Überprüfen Sie die Position der zu ersetzenden Komponente"](#)

- Sie haben die SGF6112 Appliance physisch angeordnet, bei der die NIC im Datacenter ersetzt wird.

["Suchen Sie die Appliance im Datacenter"](#)



A ["Kontrolliertes Herunterfahren des Geräts"](#) Ist erforderlich, bevor Sie das Gerät aus dem Rack entfernen.

- Sie haben alle Kabel getrennt und die Geräteabdeckung entfernt.

["Entfernen Sie die Abdeckung des SGF6112"](#)

Über diese Aufgabe

Um Serviceunterbrechungen zu vermeiden, vergewissern Sie sich, dass alle anderen Speicher-Nodes mit dem Grid verbunden sind, bevor Sie den Austausch der Netzwerkschnittstellenkarte (NIC) starten oder die NIC während eines geplanten Wartungsfensters austauschen, wenn normalerweise mit Serviceunterbrechungen zu rechnen ist. Weitere Informationen finden Sie unter ["Monitoring der Verbindungsstatus der Nodes"](#).

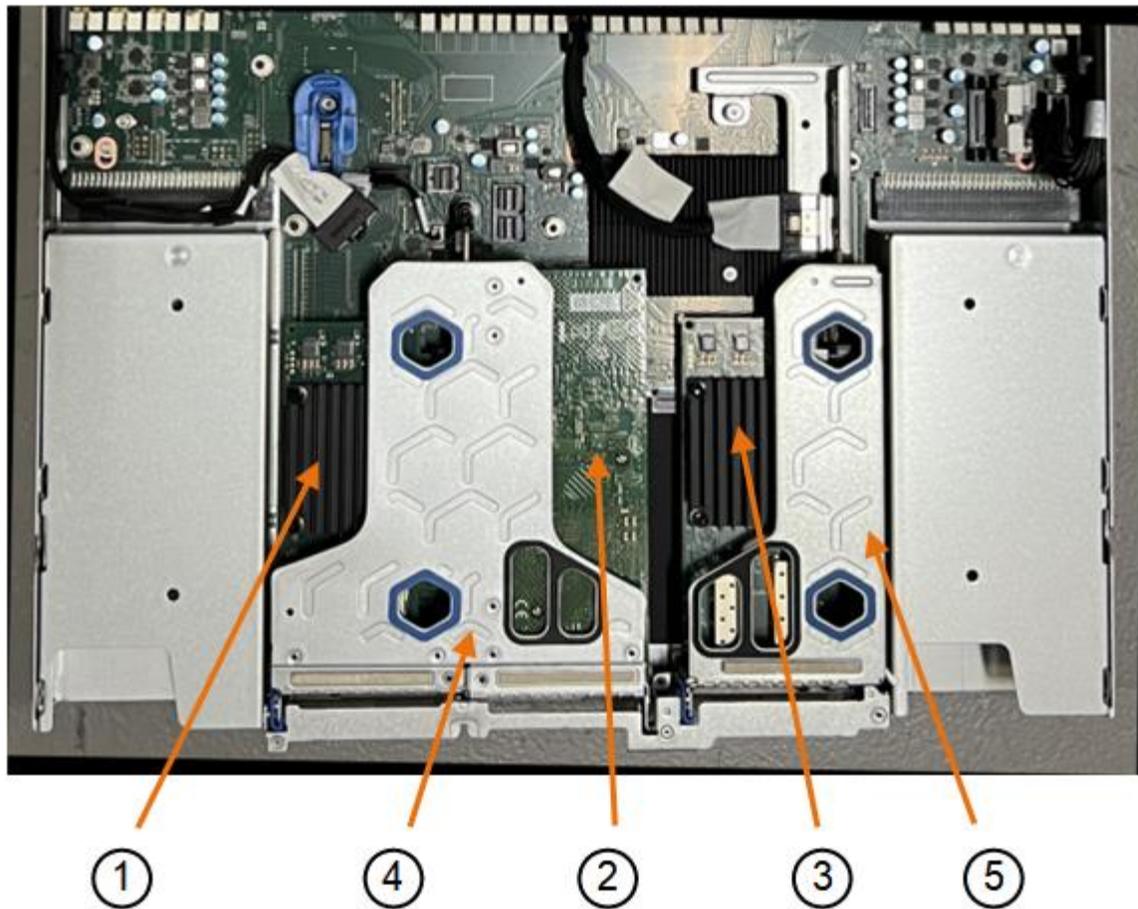


Wenn Sie jemals eine ILM-Regel verwendet haben, die nur eine Kopie eines Objekts erstellt, müssen Sie die NIC während eines geplanten Wartungsfensters ersetzen. Andernfalls verlieren Sie während dieses Verfahrens vorübergehend den Zugriff auf diese Objekte. Siehe Informationen zu ["Warum sollten Sie die Single-Copy-Replizierung nicht verwenden"](#).

Schritte

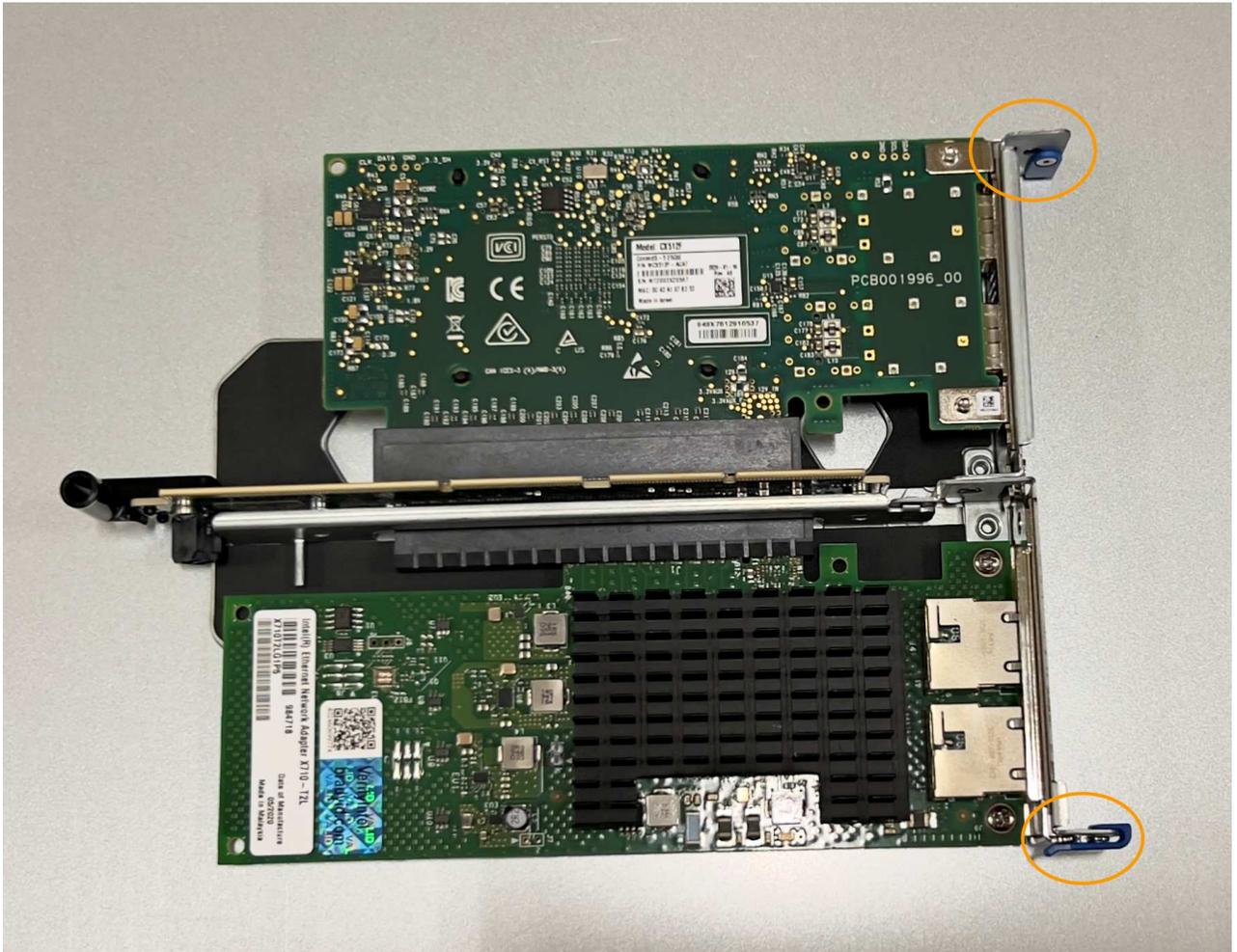
1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Suchen Sie die Riserbaugruppe, in der sich die NIC auf der Rückseite des Geräts befindet.

Die drei NICs des SGF6112 befinden sich in zwei Riser-Baugruppen in den auf dem Foto gezeigten Positionen im Gehäuse (Rückseite des SGF6112 mit entfernter oberer Abdeckung):

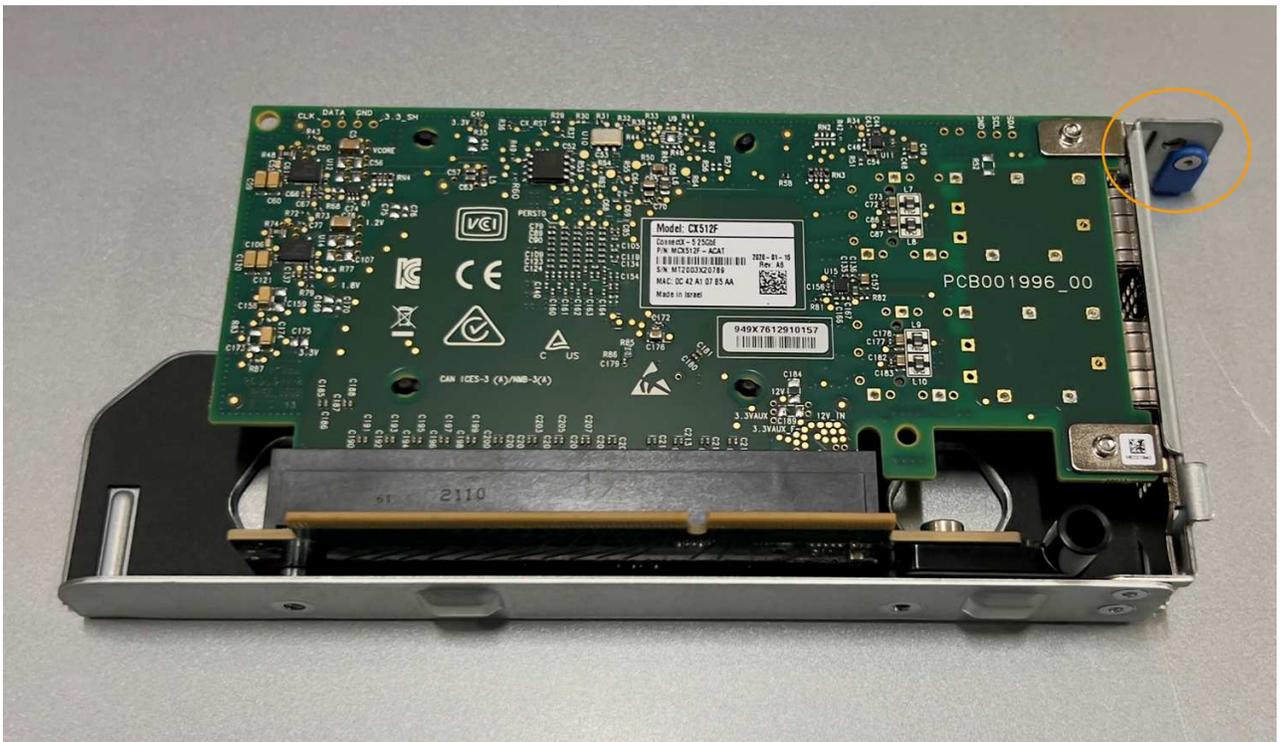


	Geräte- oder Teilename	Beschreibung
1	Schluck1/Schluck2	10/25-GbE-Ethernet-Netzwerkports in der zwei-Port-Riser-Baugruppe
2	Mtc1/mtc2	1/10GBase-T-Management-Ports in der zwei-Port-Riser-Baugruppe
3	Hik3/hik4	10/25-GbE-Ethernet-Netzwerkports in der ein-Port-Riser-Baugruppe
4	Steckplatzbaugruppe mit zwei Steckplätzen	Unterstützung für eine der 10/25-GbE-NICs und die 1/10GBase-T-NIC
5	Steckplatzbaugruppe	Unterstützung für eine der 10/25-GbE-NICs

1. Fassen Sie die Riser-Baugruppe mit der fehlerhaften NIC durch die blau markierten Löcher, und heben Sie sie vorsichtig nach oben. Bewegen Sie die Riser-Baugruppe beim Anheben in Richtung Gehäusevorderseite, damit die externen Anschlüsse in den installierten NICs das Gehäuse entfernen können.
2. Platzieren Sie den Riser auf einer flachen antistatischen Oberfläche mit der Metallrahmen-Seite nach unten, um Zugang zu den NICs zu erhalten.
 - **Zwei-Steckplatz-Riser-Baugruppe mit zwei NICs**



◦ Einsteckmontage mit einem NIC



3. Öffnen Sie die blaue Verriegelung (eingekreist) auf der zu ersetzenden NIC, und entfernen Sie die NIC vorsichtig aus der Riserbaugruppe. Führen Sie die NIC leicht durch, um die NIC aus ihrem Anschluss zu entfernen. Verwenden Sie keine übermäßige Kraft.
4. Stellen Sie die NIC auf eine flache antistatische Oberfläche.

Installieren Sie die NIC neu

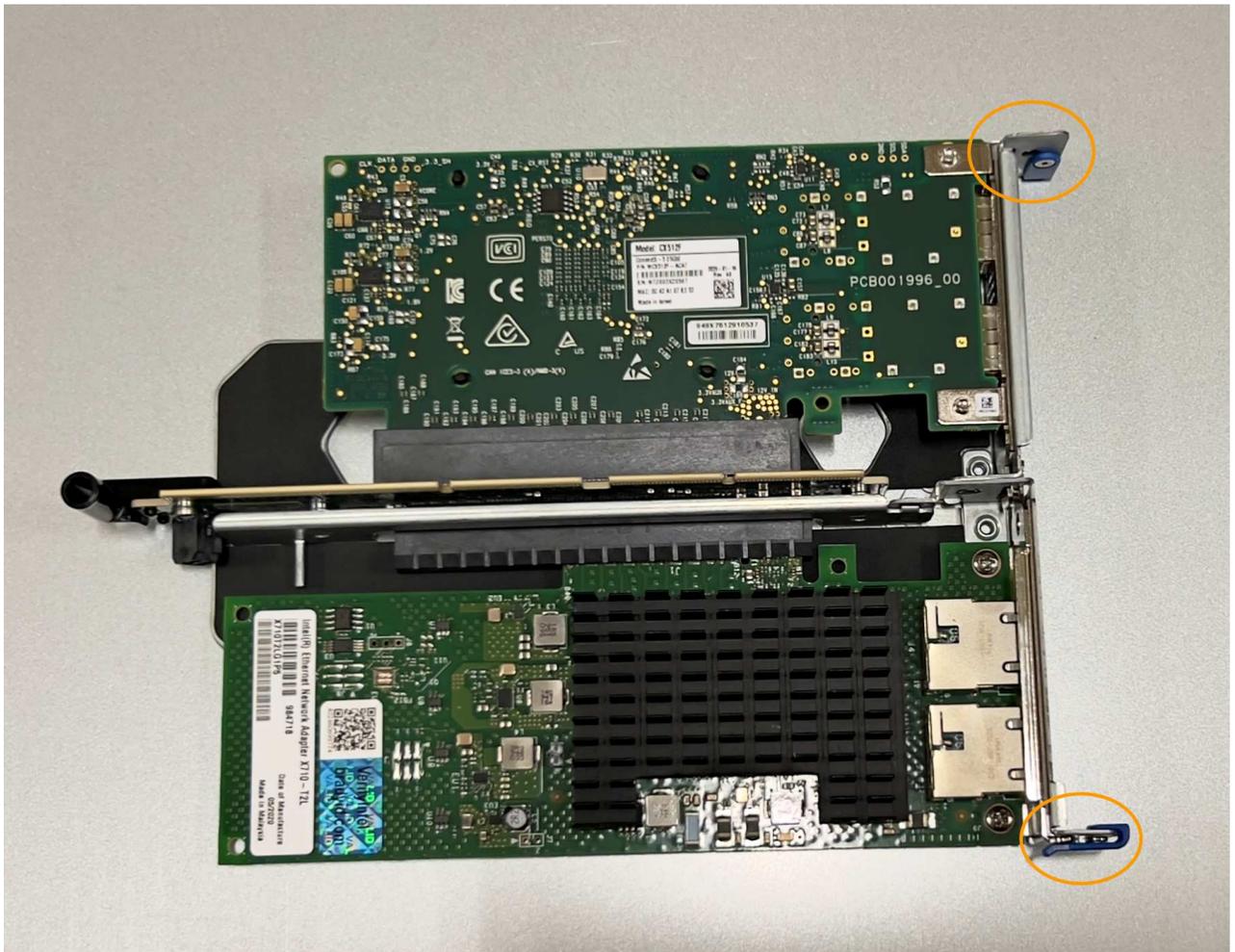
Installieren Sie die Ersatz-NIC an derselben Stelle wie die entfernte.

Bevor Sie beginnen

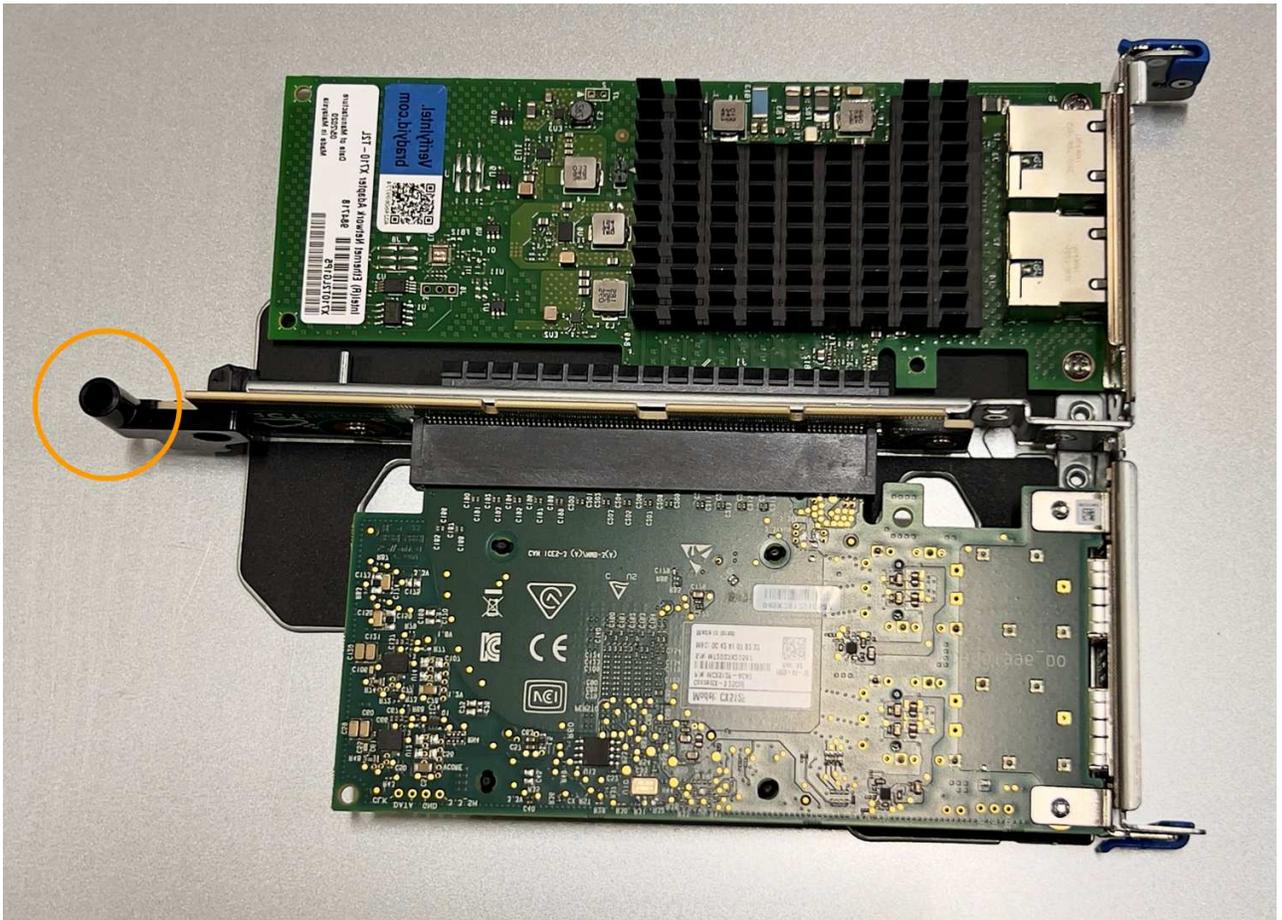
- Sie haben die richtige Ersatz-NIC.
- Sie haben die vorhandene fehlerhafte NIC entfernt.

Schritte

1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Nehmen Sie die Ersatz-NIC aus der Verpackung.
3. Wenn Sie eine der NICs in der Riserbaugruppe mit zwei Steckplätzen austauschen, gehen Sie wie folgt vor:
 - a. Stellen Sie sicher, dass sich die blaue Verriegelung in der geöffneten Position befindet.
 - b. Richten Sie die NIC an ihrem Anschluss an der Riserbaugruppe aus. Drücken Sie die NIC vorsichtig in den Anschluss, bis sie wie auf dem Foto gezeigt vollständig eingesetzt ist, und schließen Sie die blaue Verriegelung.



- c. Suchen Sie die Ausrichtungsbohrung auf der Riserbaugruppe mit zwei Steckplätzen (eingekreist), die mit einem Führungsstift auf der Systemplatine ausgerichtet ist, um sicherzustellen, dass die Riserbaugruppe richtig positioniert ist.



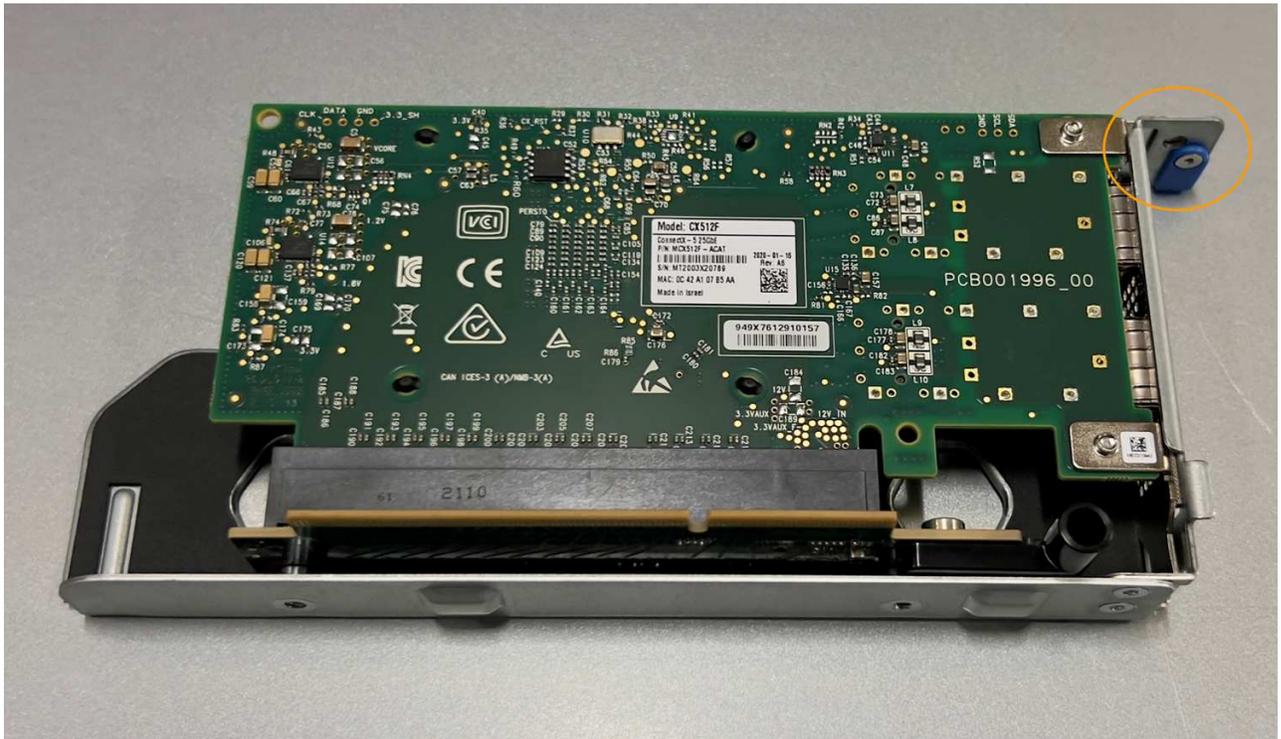
d. Suchen Sie den Führungsstift auf der Systemplatine



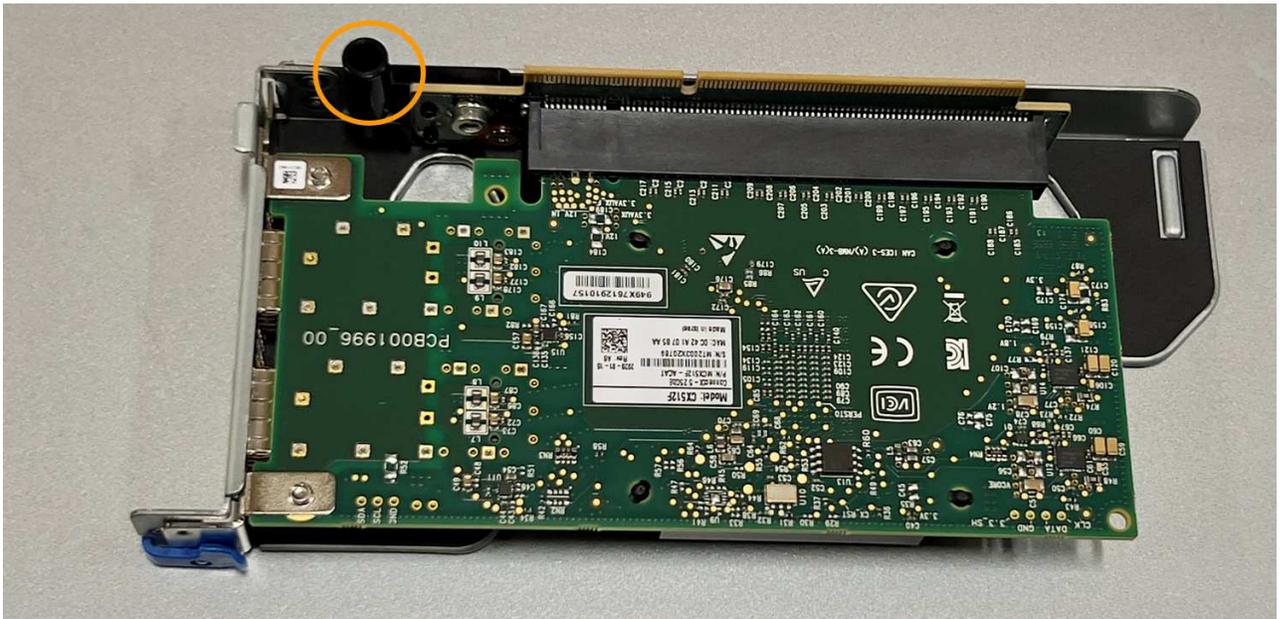
e. Positionieren Sie die Riser-Baugruppe im Gehäuse, und achten Sie darauf, dass sie mit dem

Anschluss auf der Systemplatine und dem Führungsstift ausgerichtet ist.

- f. Drücken Sie die Steckerbaugruppe mit zwei Steckplätzen vorsichtig entlang der Mittellinie neben den blau markierten Löchern, bis sie vollständig eingesetzt ist.
4. Wenn Sie die NIC in der Einsteckkarte austauschen, gehen Sie wie folgt vor:
- a. Stellen Sie sicher, dass sich die blaue Verriegelung in der geöffneten Position befindet.
 - b. Richten Sie die NIC an ihrem Anschluss an der Riserbaugruppe aus. Drücken Sie die NIC vorsichtig in den Anschluss, bis sie wie auf dem Foto gezeigt vollständig eingesetzt ist, und schließen Sie die blaue Verriegelung.



- c. Suchen Sie die Ausrichtungsbohrung auf der Einsteckkarte (eingekreist), die mit einem Führungsstift auf der Systemplatine ausgerichtet ist, um sicherzustellen, dass die Riserbaugruppe richtig positioniert ist.



d. Suchen Sie den Führungsstift auf der Systemplatine



e. Positionieren Sie die Steckplatzbaugruppe im Gehäuse, und achten Sie darauf, dass sie mit dem Anschluss auf der Systemplatine und dem Führungsstift ausgerichtet ist.

f. Drücken Sie die Steckerbaugruppe mit einem Steckplatz vorsichtig entlang der Mittellinie neben den blau markierten Löchern, bis sie vollständig eingesetzt ist.

5. Entfernen Sie die Schutzkappen von den NIC-Ports, an denen Sie die Kabel neu installieren.

Nachdem Sie fertig sind

Wenn Sie keine weiteren Wartungsmaßnahmen im Gerät durchführen müssen, setzen Sie die Geräteabdeckung wieder ein, bringen Sie das Gerät wieder in das Rack ein, schließen Sie die Kabel an und schalten Sie das Gerät mit Strom aus.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Ersetzen Sie die CMOS-Batterie des SGF6112

Gehen Sie wie folgt vor, um die CMOS-Knopfzellenbatterie auf der Systemplatine auszutauschen.

Mit diesen Verfahren können Sie:

- Entfernen Sie die CMOS-Batterie
- Setzen Sie die CMOS-Batterie wieder ein

Entfernen Sie die CMOS-Batterie

Bevor Sie beginnen

- Sie haben überprüft, ob die CMOS-Batterie des SGF6112 ausgetauscht werden muss.

["Überprüfen Sie die zu ersetzenKomponenten"](#)

- Sie haben das SGF6112-Gerät physisch positioniert, in dem Sie die CMOS-Batterie im Rechenzentrum austauschen.

["Suchen Sie die Appliance im Datacenter"](#)



A ["Kontrolliertes Herunterfahren des Geräts"](#) Ist erforderlich, bevor Sie das Gerät aus dem Rack entfernen.

- Sie haben alle Kabel getrennt und die Geräteabdeckung entfernt.

["Entfernen Sie die Abdeckung des SGF6112"](#)

Über diese Aufgabe

Um Serviceunterbrechungen zu vermeiden, vergewissern Sie sich, dass alle anderen Speicher-Nodes mit dem Stromnetz verbunden sind, bevor Sie den Austausch der CMOS-Batterie starten, oder tauschen Sie die Batterie während eines geplanten Wartungsfensters aus, wenn normalerweise mit Serviceunterbrechungen zu rechnen ist. Weitere Informationen finden Sie unter ["Monitoring der Verbindungsstatus der Nodes"](#).



Wenn Sie jemals eine ILM-Regel verwendet haben, die nur eine Kopie eines Objekts erstellt, müssen Sie die Batterie während eines geplanten Wartungsfensters austauschen. Andernfalls verlieren Sie während dieses Verfahrens vorübergehend den Zugriff auf diese Objekte. Siehe Informationen zu ["Warum sollten Sie die Single-Copy-Replizierung nicht verwenden"](#).

Schritte

1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Suchen Sie die Steckerbaugruppe mit zwei Steckplätzen an der Rückseite des Geräts.



3. Fassen Sie die Riserbaugruppe durch die blau markierten Löcher und heben Sie sie vorsichtig nach oben. Bewegen Sie die Riser-Baugruppe beim Anheben in Richtung Gehäusevorderseite, damit die externen Anschlüsse in den installierten NICs das Gehäuse entfernen können.
4. Platzieren Sie die Riserkarte auf einer flachen antistatischen Oberfläche mit der Metallrahmen-Seite nach unten.
5. Suchen Sie den CMOS-Akku auf der Systemplatine in der Position unter der entfernten Riserbaugruppe.



6. Drücken Sie den Halteclip (hervorgehoben) mit dem Finger oder einem Hebelwerkzeug aus Kunststoff von der Batterie weg, um ihn aus der Steckdose zu ziehen.



7. Entfernen Sie die Batterie, und entsorgen Sie sie ordnungsgemäß.

Setzen Sie die CMOS-Batterie wieder ein

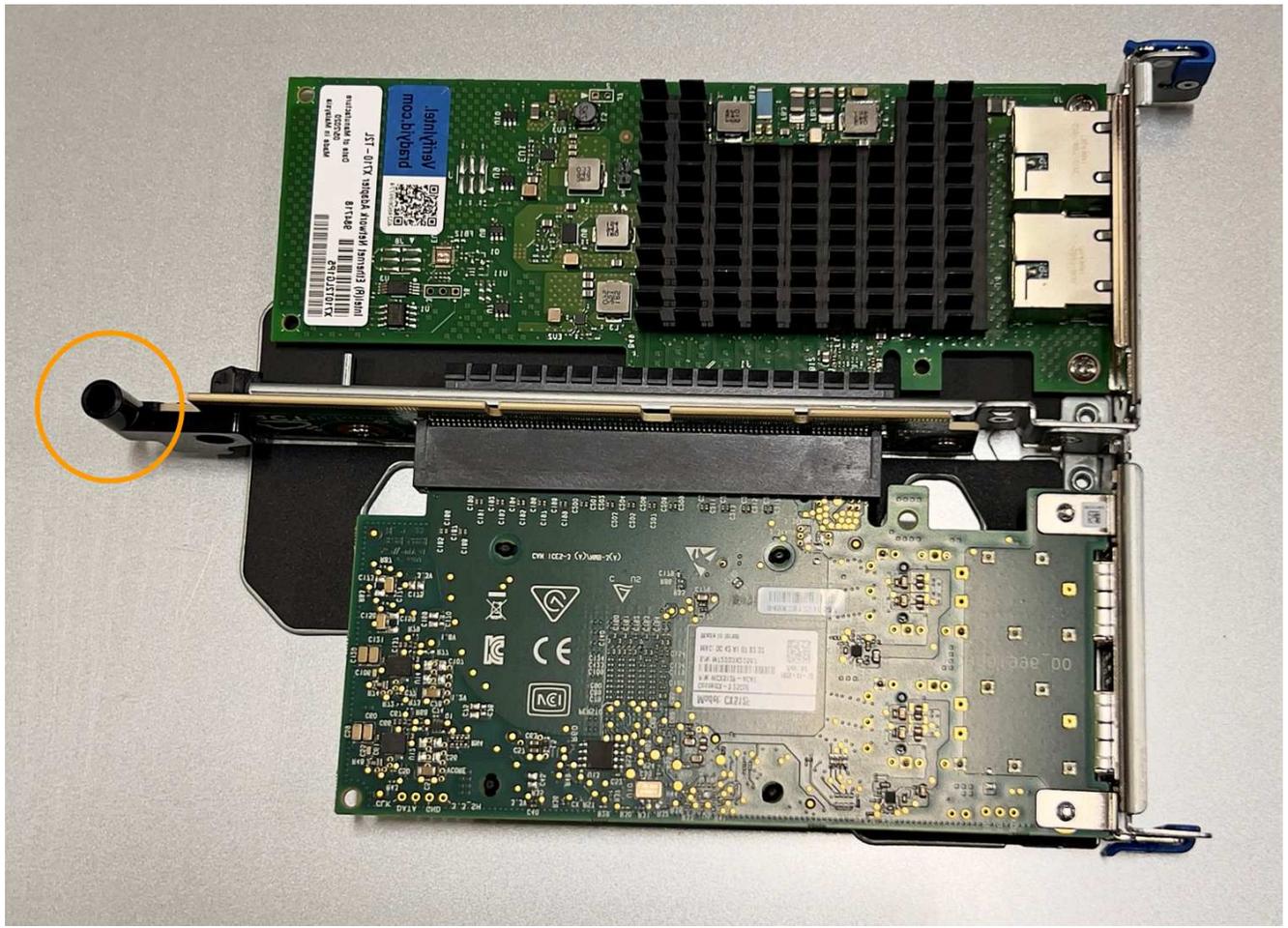
Setzen Sie den Ersatz-CMOS-Akku in den Sockel auf der Systemplatine ein.

Bevor Sie beginnen

- Sie haben die richtige Ersatz-CMOS-Batterie (CR2032).
- Sie haben die fehlerhafte CMOS-Batterie entfernt.

Schritte

1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Entfernen Sie den CMOS-Akku aus der Verpackung.
3. Drücken Sie den Ersatzakku mit der positiven (+) Seite nach oben in den leeren Sockel auf der Systemplatine, bis der Akku einrastet.
4. Suchen Sie die Ausrichtungsbohrung auf der Riserbaugruppe mit zwei Steckplätzen (eingekreist), die mit dem Führungsstift auf der Systemplatine ausgerichtet ist, um sicherzustellen, dass die Riserbaugruppe richtig positioniert ist.



5. Suchen Sie den Führungsstift auf der Systemplatine



6. Positionieren Sie die Riser-Baugruppe im Gehäuse, und achten Sie darauf, dass sie mit dem Anschluss auf der Systemplatine und dem Führungsstift ausgerichtet ist.
7. Drücken Sie die Steckerbaugruppe mit zwei Steckplätzen vorsichtig entlang der Mittellinie neben den blau markierten Löchern, bis sie vollständig eingesetzt ist.
8. Wenn Sie keine weiteren Wartungsmaßnahmen im Gerät durchführen müssen, setzen Sie die Geräteabdeckung wieder ein, bringen Sie das Gerät wieder in das Rack ein, schließen Sie die Kabel an und schalten Sie das Gerät mit Strom aus.
9. Wenn die Appliance, bei der Sie die Appliance ausgetauscht haben, zur Verschlüsselung von Daten einen Schlüsselverwaltungsserver (KMS) verwendet hat, ist möglicherweise eine zusätzliche Konfiguration erforderlich, bevor der Node dem Grid beitreten kann. Wenn der Node nicht automatisch in das Raster integriert wird, stellen Sie sicher, dass diese Konfigurationseinstellungen auf die neue Appliance übertragen wurden, und konfigurieren Sie manuell alle Einstellungen, die nicht über die erwartete Konfiguration verfügen:
 - ["Konfigurieren Sie StorageGRID-Verbindungen"](#)
 - ["Konfigurieren Sie die Node-Verschlüsselung für die Appliance"](#)
10. Melden Sie sich bei der Appliance an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:
11. Stellen Sie die BMC-Netzwerkverbindung für die Appliance wieder her. Es gibt zwei Möglichkeiten:
 - Verwenden Sie statische IP, Netzmaske und Gateway
 - Verwenden Sie DHCP, um eine IP, eine Netzmaske und ein Gateway zu erhalten
 - i. Geben Sie zum Wiederherstellen der BMC-Konfiguration für die Verwendung einer statischen IP, Netzmaske und eines Gateways die folgenden Befehle ein:


```
run-host-command ipmitool lan set 1 ipsrc static
```

```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP
```

```
run-host-command ipmitool lan set 1 netmask Netmask_IP
```

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```
 - i. Geben Sie den folgenden Befehl ein, um die BMC-Konfiguration so wiederherzustellen, dass DHCP zum Abrufen einer IP, einer Netmask und eines Gateways verwendet wird:


```
run-host-command ipmitool lan set 1 ipsrc dhcp
```
12. Stellen Sie nach dem Wiederherstellen der BMC-Netzwerkverbindung eine Verbindung zur BMC-Schnittstelle her, um die zusätzlich angewendete benutzerdefinierte BMC-Konfiguration zu prüfen und wiederherzustellen. Sie sollten beispielsweise die Einstellungen für SNMP-Trap-Ziele und E-Mail-Benachrichtigungen bestätigen. Siehe ["Konfigurieren Sie die BMC-Schnittstelle"](#).
13. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

SGF6112-Gerät austauschen

Möglicherweise müssen Sie das Gerät austauschen, wenn es nicht optimal funktioniert oder es ausgefallen ist.

Bevor Sie beginnen

- Sie haben ein Ersatzgerät mit der gleichen Teilenummer wie das Gerät, das Sie austauschen.
- Sie verfügen über Etiketten, um jedes Kabel zu identifizieren, das mit dem Gerät verbunden ist.
- Das ist schon "[Das Gerät befindet sich physisch](#)".

Über diese Aufgabe

Auf den StorageGRID-Node kann nicht zugegriffen werden, wenn Sie die Appliance ersetzen. Wenn das Gerät ausreichend funktioniert, können Sie zu Beginn dieses Verfahrens eine kontrollierte Abschaltung durchführen.



Wenn Sie die Appliance vor der Installation der StorageGRID-Software ersetzen, können Sie nach Abschluss dieses Verfahrens möglicherweise nicht sofort auf den StorageGRID Appliance Installer zugreifen. Sie können zwar von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm der StorageGRID-Appliance zugreifen, können jedoch nicht von Hosts in anderen Subnetzen darauf zugreifen. Diese Bedingung sollte sich innerhalb von 15 Minuten lösen (wenn ein ARP-Cache-Eintrag für die ursprüngliche Appliance-Zeit vorliegt), oder Sie können den Zustand sofort löschen, indem Sie alle alten ARP-Cache-Einträge manuell vom lokalen Router oder Gateway löschen.

Schritte

1. Zeigt die aktuellen Konfigurationen des Geräts an und zeichnet sie auf.

a. Melden Sie sich bei der zu ersetzenden Appliance an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

b. Geben Sie Ein: **run-host-command ipmitool lan print** Zeigt die aktuellen BMC-Konfigurationen für die Appliance an.

2. Fahren Sie das Gerät herunter:

["Fahren Sie SGF6112 herunter"](#)

3. Wenn eine der Netzwerkschnittstellen auf dieser StorageGRID-Appliance für DHCP konfiguriert ist, müssen Sie möglicherweise die permanenten DHCP-Lease-Zuordnungen auf den DHCP-Servern aktualisieren, um auf die MAC-Adressen der Ersatz-Appliance zu verweisen, um sicherzustellen, dass der Appliance die erwarteten IP-Adressen zugewiesen werden. Siehe "[Aktualisieren Sie die MAC-Adressenverweise](#)".

4. Entfernen und ersetzen Sie das Gerät:

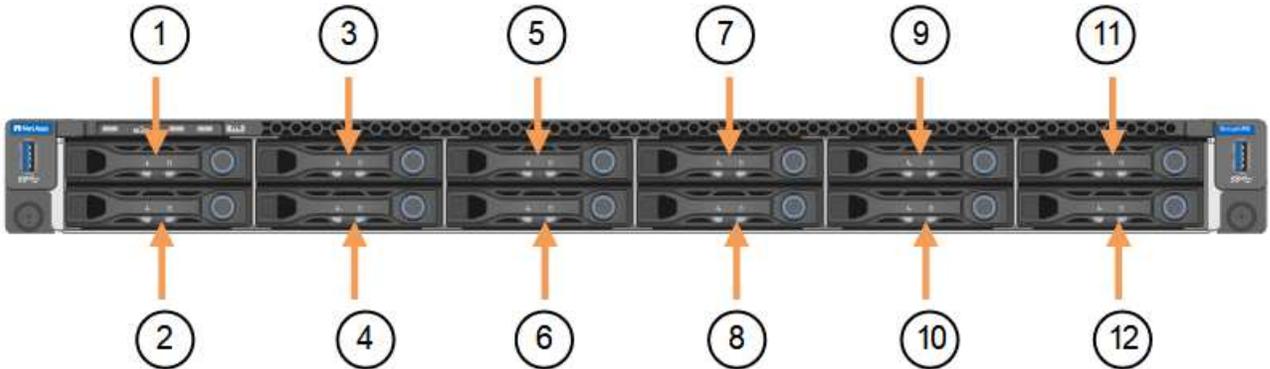
a. Beschriften Sie die Kabel und trennen Sie dann die Kabel und alle Netzwerk-Transceiver.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

- b. Entfernen Sie das ausgefallene Gerät aus dem Schrank oder Rack.
- c. Notieren Sie sich die Position der austauschbaren Komponenten (zwei Netzteile, acht Lüfter, drei NICs und zwölf SSDs) im ausgefallenen Gerät.

Die zwölf Laufwerke befinden sich in den folgenden Positionen im Gehäuse (Vorderseite des Gehäuses mit entfernter Blende):



	Laufwerk
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

d. Übertragen Sie die austauschbaren Komponenten auf das Ersatzgerät.

Befolgen Sie die Wartungsanweisungen, um die austauschbaren Komponenten wieder einzusetzen.



Wenn Sie die Daten auf den Laufwerken aufbewahren möchten, müssen Sie die SSD-Laufwerke in die gleichen Laufwerkschächte einsetzen, die sie in der ausgefallenen Appliance belegt haben. Andernfalls zeigt der Appliance Installer eine Warnmeldung an, und Sie müssen die Laufwerke in die richtigen Steckplätze stecken und die Appliance neu starten, bevor die Appliance wieder in das Raster eingesetzt werden kann.

a. Setzen Sie das Ersatzgerät in den Schrank oder Rack ein.

b. Ersetzen Sie die Kabel und optische Transceiver.

c. Schalten Sie das Gerät ein, und warten Sie, bis es wieder in das Stromnetz eingesetzt wird. Wenn die Appliance nicht erneut dem Raster angeschlossen wird, befolgen Sie die Anweisungen auf der Startseite des StorageGRID-Geräteinstallationsprogramms, um Probleme zu beheben.



Um Datenverluste zu vermeiden, wenn das Appliance Installer anzeigt, dass physische Hardwareänderungen erforderlich sind, z. B. das Verschieben von Festplattenlaufwerken in verschiedene Steckplätze, schalten Sie die Appliance vor Hardwareänderungen aus.

5. Wenn die Appliance, bei der Sie die Appliance ausgetauscht haben, zur Verschlüsselung von Daten einen Schlüsselverwaltungsserver (KMS) verwendet hat, ist möglicherweise eine zusätzliche Konfiguration erforderlich, bevor der Node dem Grid beitreten kann. Wenn der Node nicht automatisch in das Raster integriert wird, stellen Sie sicher, dass diese Konfigurationseinstellungen auf die neue Appliance übertragen wurden, und konfigurieren Sie manuell alle Einstellungen, die nicht über die erwartete Konfiguration verfügen:

- ["Konfigurieren Sie StorageGRID-Verbindungen"](#)
- ["Konfigurieren Sie die Node-Verschlüsselung für die Appliance"](#)

6. Melden Sie sich bei der ersetzten Appliance an:

a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

b. Geben Sie das im aufgeführten Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

7. Stellen Sie die BMC-Netzwerkverbindung für die ersetzte Appliance wieder her. Es gibt zwei Möglichkeiten:

- Verwenden Sie statische IP, Netzmaske und Gateway
- Verwenden Sie DHCP, um eine IP, eine Netzmaske und ein Gateway zu erhalten
- i. Geben Sie zum Wiederherstellen der BMC-Konfiguration für die Verwendung einer statischen IP, Netzmaske und eines Gateways die folgenden Befehle ein:

```
run-host-command ipmitool lan set 1 ipsrc static
```

```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP
```

```
run-host-command ipmitool lan set 1 netmask Netmask_IP
```

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

- i. Geben Sie den folgenden Befehl ein, um die BMC-Konfiguration so wiederherzustellen, dass DHCP zum Abrufen einer IP, einer Netmask und eines Gateways verwendet wird:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

8. Stellen Sie nach dem Wiederherstellen der BMC-Netzwerkverbindung eine Verbindung zur BMC-Schnittstelle her, um die zusätzlich angewendete benutzerdefinierte BMC-Konfiguration zu prüfen und wiederherzustellen. Sie sollten beispielsweise die Einstellungen für SNMP-Trap-Ziele und E-Mail-Benachrichtigungen bestätigen. Siehe "[Konfigurieren Sie die BMC-Schnittstelle](#)".
9. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

Verwandte Informationen

["Appliance in einem Schrank oder Rack installieren \(SGF6112\)"](#)

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

["Anzeigen von Startcodes für die Appliance"](#)

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Verlegung des SGF6112 in Schrank oder Rack

Entfernen Sie das SGF6112 aus einem Schrank oder Rack, um auf die obere Abdeckung zuzugreifen oder das Gerät an einen anderen Ort zu bringen. Setzen Sie das Gerät dann nach Abschluss der Hardwarewartung in einen Schrank oder ein Rack ein.

SGF6112 aus Schrank oder Rack entfernen

Bevor Sie beginnen

- Jedes Kabel, das mit dem SGF6112 verbunden ist, ist mit Etiketten versehen.
- Sie haben den Standort des SGF6112, an dem Sie Wartungsarbeiten im Datacenter durchführen.

["SGF6112 im Datacenter lokalisieren"](#)

- Sie haben die SGF6112 heruntergefahren.

["Fahren Sie SGF6112 herunter"](#)



Schalten Sie das Gerät nicht über den Netzschalter aus.

Schritte

1. Beschriften Sie die Netzkabel des Geräts, und ziehen Sie sie ab.
2. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
3. Beschriften Sie die Gerätedatenkabel und alle SFP+- oder SFP28-Transceiver, und trennen Sie sie anschließend.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

4. Lösen Sie die beiden unverlierbaren Schrauben an der Gerätevorderseite.



5. Schieben Sie das SGF6112 aus dem Rack nach vorn, bis die Montageschienen vollständig ausgefahren sind und die Verriegelungen auf beiden Seiten hörbar einrasten.

Die obere Abdeckung des Geräts ist zugänglich.

6. Optional: Wenn Sie das Gerät vollständig aus dem Schrank oder Rack entfernen, befolgen Sie die Anweisungen für den Schienensatz, um das Gerät von den Schienen zu entfernen.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Setzen Sie SGF6112 wieder in den Schrank oder das Rack ein

Bevor Sie beginnen

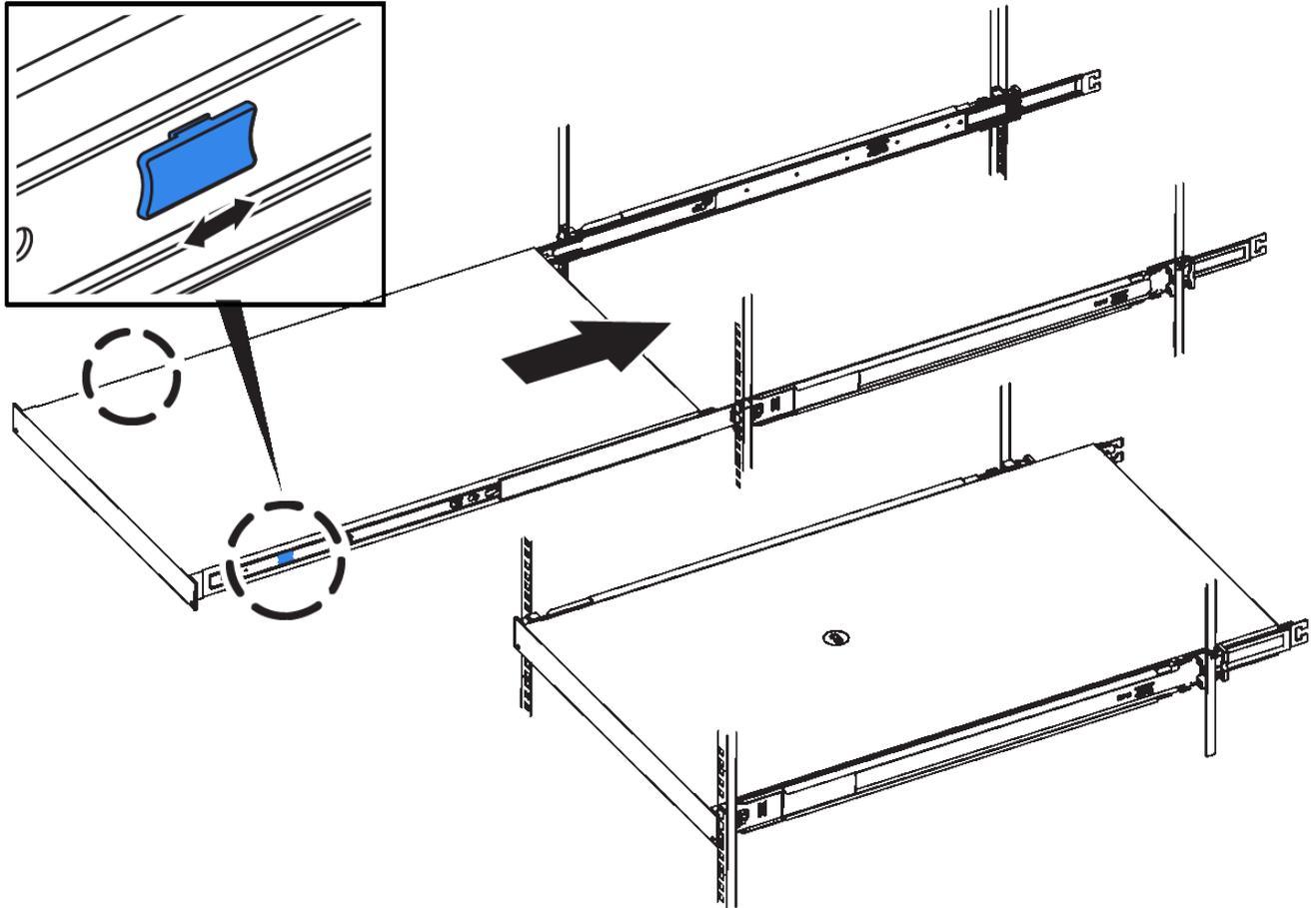
Sie haben die Geräteabdeckung wieder angebracht.

["Setzen Sie die SGF6112-Abdeckung wieder ein"](#)

Schritte

1. Drücken Sie die blaue Schiene, um beide Rackschienen gleichzeitig zu entbinden, und schieben Sie die SGF6112 in das Rack, bis sie vollständig eingesetzt ist.

Wenn Sie den Controller nicht weiter bewegen können, ziehen Sie die blauen Laschen auf beiden Seiten des Chassis, um den Controller vollständig einzuschieben.



Bringen Sie die Frontverkleidung erst an, nachdem Sie den Controller eingeschaltet haben.

- Ziehen Sie die unverlierbaren Schrauben an der Vorderseite des Controllers fest, um den Controller im Rack zu befestigen.



- Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
- Schließen Sie die Controller-Datenkabel und alle SFP+- oder SFP28-Transceiver wieder an.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

"Kabelgerät (SGF6112)"

- Schließen Sie die Controller-Stromkabel wieder an.

"Stromkabel anschließen und Strom anschließen (SGF6112)"

Nachdem Sie fertig sind

Das Gerät kann neu gestartet werden.

"Schalten Sie SGF6112 ein, und überprüfen Sie den Betrieb"

SGF6112-Abdeckung austauschen

Entfernen Sie die Geräteabdeckung, um zu Wartungszwecken Zugang zu den internen Komponenten zu erhalten, und bringen Sie die Abdeckung wieder an, wenn Sie fertig sind.

Entfernen Sie die Abdeckung

Bevor Sie beginnen

Nehmen Sie das Gerät aus dem Schrank oder Rack, um auf die obere Abdeckung zuzugreifen.

"SGF6112 aus Schrank oder Rack entfernen"

Schritte

1. Stellen Sie sicher, dass die Verriegelung der SGF6112-Abdeckung nicht verriegelt ist. Falls erforderlich, drehen Sie die blaue Kunststoffverriegelung um eine Vierteldrehung in die Entsperrungsrichtung, wie auf der Verriegelung gezeigt.
2. Drehen Sie den Riegel nach oben und zurück in Richtung der Rückseite des SGF6112-Gehäuses, bis er anhält. Heben Sie dann die Abdeckung vorsichtig vom Gehäuse ab, und legen Sie sie beiseite.



Wickeln Sie das Gurtende eines ESD-Armbands um Ihr Handgelenk und sichern Sie das Clip-Ende an einem Metallboden, um eine statische Entladung bei Arbeiten im Inneren des SGF6112 zu verhindern.

Setzen Sie die Abdeckung wieder ein

Bevor Sie beginnen

Sie haben alle Wartungsarbeiten im Gerät durchgeführt.

Schritte

1. Halten Sie bei geöffneter Abdeckungsverriegelung die Abdeckung über dem Gehäuse und richten Sie die Öffnung in der oberen Abdeckung an dem Stift im Gehäuse aus. Wenn die Abdeckung ausgerichtet ist, senken Sie sie auf das Gehäuse ab.



2. Drehen Sie die Verriegelung nach vorne und unten, bis sie anhält und die Abdeckung vollständig im Gehäuse sitzt. Stellen Sie sicher, dass an der Vorderkante der Abdeckung keine Lücken vorhanden sind.

Wenn die Abdeckung nicht vollständig eingesetzt ist, können Sie die SGF6112 möglicherweise nicht in das Rack schieben.

3. Optional: Drehen Sie die blaue Kunststoffverriegelung um eine Vierteldrehung in die Schlossrichtung, wie auf der Verriegelung gezeigt, um sie zu verriegeln.

Nachdem Sie fertig sind

Setzen Sie das Gerät wieder in den Schrank oder das Rack ein.

["Setzen Sie SGF6112 wieder in den Schrank oder das Rack ein"](#)

Wartung der SG6000 Hardware

Warten Sie die SG6000-Appliance

Möglicherweise müssen Sie auf der SG6000-Appliance Wartungsarbeiten durchführen.

In diesem Abschnitt wird davon ausgegangen, dass die Appliance bereits als Speicher-Node in einem StorageGRID-System bereitgestellt wurde.

Siehe ["Allgemeine Verfahren"](#) Für Wartungsverfahren, die von allen Geräten verwendet werden.

Siehe ["Richten Sie die Hardware ein"](#) Für Wartungsverfahren, die auch während der Erstinstallation und -Konfiguration der Appliance durchgeführt werden.

Um Serviceunterbrechungen zu vermeiden, vergewissern Sie sich, dass alle anderen Speicherknoten mit dem Raster verbunden sind, bevor Sie das Gerät herunterfahren oder das Gerät während eines geplanten Wartungsfensters herunterfahren, wenn die Serviceunterbrechungen akzeptabel sind. Weitere Informationen finden Sie unter ["Monitoring der Verbindungsstatus der Nodes"](#).



Wenn Sie jemals eine ILM-Regel verwendet haben, die nur eine Kopie eines Objekts erstellt, müssen Sie die Appliance während eines geplanten Wartungsfensters herunterfahren. Andernfalls verlieren Sie während des Wartungsvorgangs, die einen Storage-Node außer Betrieb nimmt, möglicherweise vorübergehend den Zugriff auf diese Objekte. Weitere Informationen finden Sie unter "[Verwalten von Objekten mit Information Lifecycle Management](#)".

Verfahren zur Wartungskonfiguration

Upgrades des SANtricity OS auf Storage Controllern

Um die optimale Funktion des Storage Controllers sicherzustellen, müssen Sie auf die neueste Wartungsversion des SANtricity-Betriebssystems aktualisieren, das für Ihre StorageGRID Appliance geeignet ist.

Konsultieren Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um zu bestimmen, welche Version Sie verwenden sollen.

Laden Sie die neue Datei für die SANtricity OS Software von herunter "[NetApp Downloads mit StorageGRID Appliance](#)".

Verwenden Sie eines der folgenden Verfahren, das auf der derzeit installierten Version von SANtricity OS basiert:

- Wenn der Storage-Controller SANtricity OS 08.42.20.00 (11.42) oder eine neuere Version verwendet, führen Sie das Upgrade mit dem Grid Manager durch.

["Aktualisieren Sie SANtricity OS auf Storage-Controllern mit Grid Manager"](#)

- Wenn der Storage-Controller eine SANtricity OS-Version verwendet, die älter als 08.42.20.00 ist (11.42), führen Sie das Upgrade im Wartungsmodus durch.

["Aktualisieren Sie das SANtricity OS auf Storage Controllern mit dem Wartungsmodus"](#)



Wenn Sie ein Upgrade des SANtricity-Betriebssystems für Ihre Storage Appliance durchführen, müssen Sie die Anweisungen in der StorageGRID-Dokumentation befolgen. Wenn Sie andere Anweisungen verwenden, kann das Gerät nicht mehr funktionieren.

Aktualisieren Sie SANtricity OS auf Storage-Controllern mit Grid Manager

Bei Storage-Controllern, die derzeit SANtricity OS 08.42.20.00 (11.42) oder eine neuere Version verwenden, müssen Sie zum Anwenden eines Upgrades den Grid-Manager verwenden.

Bevor Sie beginnen

- Sie haben den konsultiert "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um sicherzustellen, dass die für das Upgrade verwendete SANtricity OS-Version mit Ihrer Appliance kompatibel ist.
- Sie haben die "[Berechtigung für Wartung oder Root-Zugriff](#)".
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Provisionierungs-Passphrase.

- Sie haben Zugriff auf ["NetApp Downloads mit StorageGRID Appliance"](#).

Über diese Aufgabe

Andere Software-Updates (StorageGRID Software-Upgrade oder Hotfix) können erst nach Abschluss des SANtricity OS Upgrades durchgeführt werden. Wenn Sie versuchen, vor Abschluss des SANtricity OS-Upgrades einen Hotfix oder ein StorageGRID-Software-Upgrade zu starten, werden Sie zur Upgrade-Seite von SANtricity OS umgeleitet.

Das Verfahren ist erst abgeschlossen, wenn das SANtricity OS Upgrade erfolgreich auf alle zutreffenden Nodes angewendet wurde, die für das Upgrade ausgewählt wurden. Das SANtricity Betriebssystem kann länger als 30 Minuten dauern, bis das Betriebssystem auf jedem Node (sequenziell) und bis zu 90 Minuten zum Neustart jeder StorageGRID Storage Appliance benötigt wird. Alle Nodes in Ihrem Grid, die SANtricity OS nicht verwenden, sind von diesem Verfahren nicht betroffen.



Die folgenden Schritte sind nur anwendbar, wenn Sie den Grid Manager zur Durchführung des Upgrades verwenden. Die Storage Controller in der Appliance können nicht mit dem Grid-Manager aktualisiert werden, wenn die Controller SANtricity OS verwenden, die älter als 08.42.20.00 (11.42) sind.



Mit diesem Verfahren wird der NVSRAM automatisch auf die neueste Version aktualisiert, die mit dem Upgrade des SANtricity-Betriebssystems verknüpft ist. Sie müssen keine separate NVSRAM-Aktualisierungsdatei anwenden.



Stellen Sie sicher, dass Sie den aktuellen StorageGRID-Hotfix installieren, bevor Sie mit diesem Vorgang beginnen. Siehe ["StorageGRID Hotfix Verfahren"](#) Entsprechende Details.

Schritte

1. Laden Sie die neue SANtricity OS Softwaredatei von herunter ["NetApp Downloads mit StorageGRID Appliance"](#).

Achten Sie darauf, die SANtricity Betriebssystemversion für Ihre Storage Controller auszuwählen.

2. Wählen Sie **WARTUNG > System > Software-Update**.

Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade Upgrade to the next StorageGRID version and apply the latest hotfix for that version. Upgrade →	StorageGRID hotfix Apply a hotfix to your current StorageGRID software version. Apply hotfix →	SANtricity OS update Update the SANtricity OS software on your StorageGRID storage appliances. Update →
--	---	--

3. Wählen Sie im Abschnitt SANtricity OS Update die Option **Update** aus.

Die Seite SANtricity OS Upgrade wird angezeigt und enthält die Details zu den einzelnen Appliance-Nodes, einschließlich:

- Node-Name
- Standort
- Appliance-Modell
- Version des SANtricity Betriebssystems
- Status
- Status des letzten Upgrades

4. Lesen Sie die Informationen in der Tabelle für alle Upgrade-fähigen Geräte. Vergewissern Sie sich, dass alle Speicher-Controller den Status **nominal** haben. Wenn der Status eines Controllers **Unbekannt** lautet, gehen Sie zu **Nodes > Appliance Node > Hardware**, um das Problem zu untersuchen und zu beheben.

5. Wählen Sie die Upgrade-Datei für das SANtricity Betriebssystem aus, die Sie von der NetApp Support-Website heruntergeladen haben.

- a. Wählen Sie **Durchsuchen**.
- b. Suchen und wählen Sie die Datei aus.
- c. Wählen Sie **Offen**.

Die Datei wird hochgeladen und validiert. Wenn der Validierungsprozess abgeschlossen ist, wird der Dateiname mit einem grünen Häkchen neben der Schaltfläche **Browse** angezeigt. Ändern Sie den Dateinamen nicht, da er Teil des Überprüfungsprozesses ist.

6. Geben Sie die Provisionierungs-Passphrase ein und wählen Sie **Weiter**.

Ein Warnfeld zeigt an, dass die Verbindung Ihres Browsers vorübergehend unterbrochen wird, da Dienste auf Knoten, die aktualisiert werden, neu gestartet werden.

7. Wählen Sie **Ja**, um die SANtricity OS-Upgrade-Datei auf den primären Admin-Knoten zu übertragen.

Wenn das SANtricity OS Upgrade startet:

- a. Die Integritätsprüfung wird ausgeführt. Dieser Prozess überprüft, dass für keine Nodes der Status „Aufmerksamkeit erforderlich“ angezeigt wird.



Wenn Fehler gemeldet werden, beheben Sie sie, und wählen Sie erneut **Start**.

- b. Die Fortschrittstabelle für das SANtricity OS-Upgrade wird angezeigt. In dieser Tabelle werden alle Storage-Nodes in Ihrem Raster und die aktuelle Phase des Upgrades für jeden Node angezeigt.



In der Tabelle sind alle Appliance Storage-Nodes aufgeführt. Softwarebasierte Storage-Nodes werden nicht angezeigt. Wählen Sie für alle Nodes, die das Upgrade erfordern * genehmigen.

SANtricity OS

Upload files — **2** Upgrade

Approved nodes are added to a queue and upgraded sequentially. Each node can take up to 30 minutes, which includes updating NVSRAM. When the upgrade is complete, the node is rebooted.

Select **Approve all** or approve nodes one at a time. To remove nodes from the queue, select **Remove all** or remove nodes one at a time. If the uploaded file doesn't apply to an approved node, the upgrade process skips that node and moves to the next node in the queue.

Optionally, select **Skip nodes and finish** to end the upgrade and skip any unapproved nodes.

SANtricity OS upgrade file: RCB_11.70.3_280x_6283a64d.dlp

0 out of 3 completed

Node name	Current version	Progress	Stage	Details	Status	Actions
10-224-2-24-S1	08.40.60.01	<div style="width: 100%; height: 10px; background-color: #add8e6;"></div>	Waiting for you to approve		Nominal	Approve
lab-37-sgws- quanta-10	08.73.00.00	<div style="width: 100%; height: 10px; background-color: #add8e6;"></div>	Waiting for you to approve		Nominal	Approve
storage-7	98.72.09.00	<div style="width: 100%; height: 10px; background-color: #add8e6;"></div>	Waiting for you to approve		Nominal	Approve

8. Sortieren Sie die Liste der Knoten wahlweise in aufsteigender oder absteigender Reihenfolge nach:

- Node-Name
- Aktuelle Version
- Fortschritt
- Stufe
- Status

Sie können auch einen Begriff in das Suchfeld eingeben, um nach bestimmten Knoten zu suchen.

9. Genehmigen Sie die Grid-Knoten, die Sie zur Upgrade-Warteschlange hinzufügen möchten. Genehmigte Nodes werden nacheinander aktualisiert.



Genehmigen Sie das SANtricity OS Upgrade für einen Appliance-Speicher-Node nur, wenn Sie sicher sind, dass der Node bereit ist, angehalten und neu gestartet zu werden. Wenn das Upgrade von SANtricity OS auf einem Node genehmigt wird, werden die Services auf diesem Node angehalten und der Upgrade-Prozess beginnt. Wenn die Aktualisierung des Node abgeschlossen ist, wird der Appliance-Node später neu gebootet. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren.

- Klicken Sie auf die Schaltfläche **Alle genehmigen**, um alle Speicher-Nodes der SANtricity OS Upgrade-Warteschlange hinzuzufügen.



Wenn die Reihenfolge, in der die Knoten aktualisiert werden, wichtig ist, genehmigen Sie nacheinander Knoten oder Gruppen von Knoten, und warten Sie, bis das Upgrade für jeden Knoten abgeschlossen ist, bevor Sie den nächsten Knoten genehmigen.

- Wählen Sie eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere Knoten zur SANtricity OS-Upgrade-Warteschlange hinzuzufügen. Die Schaltfläche **approve** ist deaktiviert, wenn der Status nicht nominal ist.

Nachdem Sie **Genehmigen** ausgewählt haben, bestimmt der Upgrade-Prozess, ob der Knoten aktualisiert werden kann. Wenn ein Knoten aktualisiert werden kann, wird er der Upgrade-Warteschlange hinzugefügt.

Bei einigen Nodes wird die ausgewählte Upgrade-Datei absichtlich nicht angewendet. Sie können das Upgrade abschließen, ohne dass Sie ein Upgrade dieser spezifischen Nodes durchführen müssen. Nodes, die absichtlich kein Upgrade durchgeführt wurden, zeigen eine Phase komplett (Upgrade versucht) und geben den Grund an, warum der Node nicht in der Spalte Details aktualisiert wurde.

10. Wenn Sie einen Knoten oder alle Knoten aus der SANtricity OS Upgrade-Warteschlange entfernen möchten, wählen Sie **Entfernen** oder **Alle entfernen**.

Wenn die Phase über Queued hinaus fortschreitet, wird die Schaltfläche **Entfernen** ausgeblendet und Sie können den Knoten nicht mehr aus dem SANtricity OS-Upgrade-Prozess entfernen.

11. Warten Sie, während das SANtricity OS Upgrade auf jeden genehmigten Grid-Node angewendet wird.

- Wenn bei einem Node während der Anwendung des SANtricity OS Upgrades eine Fehlerstufe angezeigt wird, ist das Upgrade für den Node fehlgeschlagen. Mithilfe des technischen Supports müssen Sie das Gerät möglicherweise in den Wartungsmodus versetzen, um es wiederherzustellen.
- Wenn die Firmware auf dem Node zu alt ist, um mit dem Grid-Manager aktualisiert zu werden, wird auf dem Node die Fehlerstufe angezeigt. Darin enthalten sind die Details, die Sie zum Upgrade von SANtricity OS auf dem Node mit dem Wartungsmodus verwenden müssen. Gehen Sie wie folgt vor, um den Fehler zu beheben:
 - i. Verwenden Sie den Wartungsmodus, um ein Upgrade von SANtricity OS auf dem Node durchzuführen, auf dem eine Fehlerstufe angezeigt wird.
 - ii. Verwenden Sie den Grid-Manager, um das SANtricity OS-Upgrade neu zu starten und abzuschließen.

Wenn das SANtricity OS Upgrade auf allen genehmigten Nodes abgeschlossen ist, wird die Fortschrittstabelle für SANtricity OS Upgrades geschlossen, und ein grünes Banner zeigt die Anzahl der aktualisierten Nodes sowie Datum und Uhrzeit des Upgrades an.

12. Wenn ein Knoten nicht aktualisiert werden kann, notieren Sie sich den Grund, der in der Spalte Details angezeigt wird, und führen Sie die entsprechende Aktion durch.



Das SANtricity OS-Upgrade ist erst abgeschlossen, wenn Sie das SANtricity OS-Upgrade auf allen aufgeführten Storage-Nodes genehmigen.

Grund	Empfohlene Maßnahmen
Storage-Node wurde bereits aktualisiert.	Keine weiteren Maßnahmen erforderlich.

Grund	Empfohlene Maßnahmen
Das SANtricity OS Upgrade ist für diesen Node nicht verfügbar.	Der Node verfügt nicht über einen Storage Controller, der vom StorageGRID System gemanagt werden kann. Schließen Sie das Upgrade ab, ohne den Node mit dieser Meldung zu aktualisieren.
Die SANtricity OS-Datei ist mit diesem Node nicht kompatibel.	Der Node erfordert eine andere SANtricity OS-Datei als die ausgewählte. Laden Sie nach Abschluss des aktuellen Upgrades die korrekte SANtricity OS-Datei für den Node herunter, und wiederholen Sie den Upgrade-Vorgang.

13. Wenn Sie die Genehmigung von Nodes beenden und zur Seite SANtricity OS zurückkehren möchten, um einen Upload einer neuen SANtricity OS-Datei zu ermöglichen, gehen Sie wie folgt vor:

a. Wählen Sie **Knoten überspringen und beenden**.

Es wird eine Warnung angezeigt, in der Sie gefragt werden, ob Sie den Aktualisierungsvorgang wirklich beenden möchten, ohne alle zutreffenden Knoten zu aktualisieren.

b. Wählen Sie * OK* aus, um zur Seite **SANtricity OS** zurückzukehren.

c. Wenn Sie bereit sind, mit der Genehmigung von Knoten fortzufahren, [Laden Sie das SANtricity OS herunter](#) Um den Upgrade-Vorgang neu zu starten.



Nodes, die bereits genehmigt und ohne Fehler aktualisiert wurden, werden weiterhin aktualisiert.

14. Wiederholen Sie dieses Upgrade-Verfahren für alle Nodes in einer vollständigen Phase, für die eine andere SANtricity OS Upgrade-Datei erforderlich ist.



Verwenden Sie für alle Nodes, für die der Status als Warnung angezeigt wird, den Wartungsmodus, um das Upgrade durchzuführen.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

["Aktualisieren Sie das SANtricity OS auf Storage Controllern mit dem Wartungsmodus"](#)

Aktualisieren Sie das SANtricity OS auf Storage Controllern mit dem Wartungsmodus

Für Storage-Controller, die derzeit SANtricity OS verwenden, die älter als 08.42.20.00 (11.42) sind, müssen Sie das Verfahren des Wartungsmodus verwenden, um ein Upgrade durchzuführen.

Bevor Sie beginnen

- Sie haben den konsultiert ["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#) Um sicherzustellen, dass die für das Upgrade verwendete SANtricity OS-Version mit Ihrer Appliance kompatibel ist.
- Wenn die StorageGRID-Appliance in einem StorageGRID-System ausgeführt wird, haben Sie den SG6000-CN-Controller in eingesetzt ["Wartungsmodus"](#).



Im Wartungsmodus wird die Verbindung zum Storage Controller unterbrochen.

Über diese Aufgabe

Führen Sie keine Upgrades des SANtricity OS bzw. NVSRAM im E-Series Controller auf mehr als einer StorageGRID Appliance gleichzeitig durch.



Wenn Sie mehrere StorageGRID Appliances gleichzeitig aktualisieren, kann dies in Abhängigkeit von Ihrem Implementierungsmodell und den ILM-Richtlinien zu Datenunverfügbarkeit führen.

Schritte

1. Vergewissern Sie sich, dass das Gerät in ist "**Wartungsmodus**".
2. Greifen Sie über ein Service-Laptop auf den SANtricity System Manager zu und melden Sie sich an.
3. Laden Sie die neue SANtricity OS Software-Datei und die NVSRAM-Datei auf den Management-Client herunter.



Das NVSRAM bezieht sich auf die StorageGRID Appliance. Verwenden Sie den Standard-NVSRAM-Download nicht.

4. Folgen Sie den Anweisungen im Handbuch „*Upgrade SANtricity OS*“ oder der Online-Hilfe von SANtricity System Manager, um die Firmware und NVSRAM zu aktualisieren.



Aktivieren Sie die Upgrade-Dateien sofort. Die Aktivierung darf nicht verzögert werden.

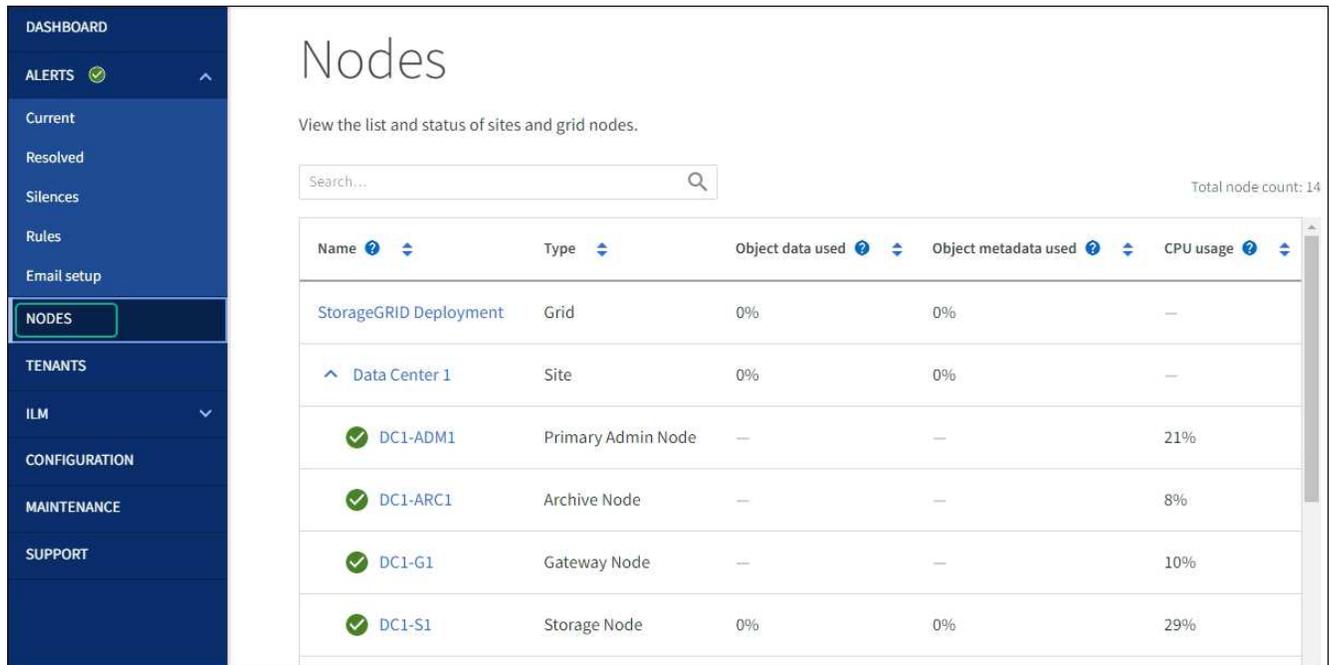
5. Wenn diese Prozedur erfolgreich abgeschlossen ist und Sie weitere durchzuführenden Verfahren haben, während sich der Node im Wartungsmodus befindet, führen Sie sie jetzt aus. Wenn Sie fertig sind oder Fehler auftreten und von vorne beginnen möchten, wählen Sie **Erweitert > Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

- Wählen Sie **Neustart in StorageGRID** aus
- Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. Wählen Sie diese Option aus, wenn während des Verfahrens Fehler auftreten und neu starten möchten. Nachdem der Node das Neubooten in den Wartungsmodus abgeschlossen hat, starten Sie den entsprechenden Schritt während des ausgefallenen Verfahrens neu.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid

beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite Knoten sollte ein normaler Status angezeigt werden (grünes Häkchen-Symbol  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.



Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	21%
 DC1-ARC1	Archive Node	—	—	8%
 DC1-G1	Gateway Node	—	—	10%
 DC1-S1	Storage Node	0%	0%	29%

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

["Aktualisieren Sie SANtricity OS auf Storage-Controllern mit Grid Manager"](#)

Aktualisieren Sie die Laufwerk-Firmware mit SANtricity System Manager

Aktualisieren Sie die Firmware des SG6000 Laufwerks mithilfe von SANtricity System Manager über die Online-Methode

Aktualisieren Sie mit der Online-Methode des SANtricity System Managers die Firmware auf den Laufwerken in Ihrer Appliance, um sicherzustellen, dass Sie über die neuesten Funktionen und Fehlerbehebungen verfügen.

Bevor Sie beginnen

- Die Storage Appliance hat einen optimalen Status.
- Alle Laufwerke haben einen optimalen Status.



Aktualisieren Sie nicht gleichzeitig die Laufwerk-Firmware auf mehr als einer StorageGRID Appliance. Dies kann je nach Bereitstellungsmodell und ILM-Richtlinie zu einer Nichtverfügbarkeit von Daten führen.

Über diese Aufgabe

Die Laufwerke werden nacheinander aktualisiert, während die Appliance I/O-Vorgänge durchführt. Bei dieser Methode müssen Sie das Gerät nicht in den Wartungsmodus versetzen. Allerdings kann die System-Performance beeinträchtigt sein und das Upgrade kann mehrere Stunden länger dauern als die Offline-Methode.



Laufwerke, die zu Volumes ohne Redundanz gehören, müssen mithilfe des aktualisiert werden "[Offline-Methode](#)". Die Offline-Methode sollte für alle Laufwerke verwendet werden, die mit dem Flash Read-Cache verbunden sind (z. B. SSD-Laufwerke im SG6060), sowie für alle Pools oder Volume-Gruppen, deren Betrieb derzeit beeinträchtigt ist.

Es gibt zwei Laufwerkstypen: SSD und HDD. Sie müssen den verwenden "[Offline-Methode](#)" Um die Firmware auf den SSDs zu aktualisieren (z. B. SSD-Laufwerke im SG6060). Sie können entweder die Online- oder die Offline-Methode verwenden, um die Firmware auf HDDs zu aktualisieren.

Schritte

1. Greifen Sie mit einer der folgenden Methoden auf SANtricity System Manager zu:
 - Verwenden Sie das StorageGRID-Appliance-Installationsprogramm, und wählen Sie **Erweitert > SANtricity-Systemmanager**
 - Verwenden Sie den Grid-Manager, und wählen Sie **NODES > Storage Node > SANtricity System Manager** aus
 - Verwenden Sie SANtricity System Manager, indem Sie zur Storage Controller-IP navigieren:

`https://Storage_Controller_IP`
2. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des SANtricity System Manager-Administrators ein.
3. Überprüfen Sie die Version der Laufwerk-Firmware, die derzeit in der Speicher-Appliance installiert ist:
 - a. Wählen Sie im SANtricity System Manager **SUPPORT > Upgrade-Center** aus.
 - b. Wählen Sie unter Laufwerk-Firmware-Upgrade die Option **Upgrade starten** aus.

Auf der Seite Laufwerksfirmware aktualisieren werden die aktuell installierten Laufwerksfirmware-Dateien angezeigt.

- c. Beachten Sie die aktuellen Versionen der Laufwerk-Firmware und die Laufwerkskennungen in der Spalte Aktueller Laufwerk-Firmware.

Upgrade Drive Firmware

1 Select Upgrade Files

Review your current drive firmware and select upgrade files below...

[What do I need to know before upgrading drive firmware?](#)

Current Drive Firmware

MS02, KPM51VUG800G

Total rows: 1 |

In diesem Beispiel:

- Die Version der Laufwerk-Firmware lautet **MS02**.
 - Die Laufwerk-ID lautet **KPM51VUG800G**.
- d. Wählen Sie in der Spalte „verbundene Laufwerke“ die Option **Laufwerke anzeigen** aus, um anzuzeigen, wo diese Laufwerke in Ihrem Speichergerät installiert sind.
- e. Schließen Sie das Fenster Upgrade Drive Firmware.
4. Laden Sie das verfügbare Laufwerk-Firmware-Upgrade herunter, und bereiten Sie es vor:
- a. Wählen Sie unter Laufwerk-Firmware-Upgrade **NetApp Support** aus.
- b. Wählen Sie auf der NetApp Support-Website die Registerkarte **Downloads** aus und wählen Sie dann **E-Series Festplatten-Firmware** aus.

Die Seite E-Series Festplatten-Firmware wird angezeigt.

- c. Suchen Sie nach jedem in Ihrer Speicheranwendung installierten **Drive Identifier**, und stellen Sie sicher, dass jeder Laufwerkennung die neueste Firmware-Version hat.
- Wenn die Firmware-Version kein Link ist, hat diese Laufwerkennung die neueste Firmware-Version.
 - Wenn eine oder mehrere Laufwerk-Teilenummern für eine Laufwerksidentifikation aufgeführt sind, ist für diese Laufwerke ein Firmware-Upgrade verfügbar. Sie können einen beliebigen Link auswählen, um die Firmware-Datei herunterzuladen.

Drive Part Number	Descriptions	Drive Identifier	Firmware Rev. (Download)	Notes and Config Info	Release Date
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	MS03	MS02 Fixes Bug 1194908 MS03 Fixes Bug 1334862	04-Sep-2020

- d. Wenn eine spätere Firmware-Version aufgeführt wird, wählen Sie den Link im Firmware-Rev. Aus (Download) Spalte zum Herunterladen einer .zip Archiv mit der Firmware-Datei.
- e. Extrahieren Sie die von der Support-Website heruntergeladenen Archivdateien der Laufwerk-Firmware (entpacken).
5. Installieren Sie das Laufwerk-Firmware-Upgrade:
- a. Wählen Sie im SANtricity System Manager unter Upgrade der Laufwerk-Firmware die Option **Upgrade starten** aus.
- b. Wählen Sie **Durchsuchen** aus, und wählen Sie die neuen Laufwerk-Firmware-Dateien aus, die Sie von der Support-Website heruntergeladen haben.

Die Firmware-Dateien des Laufwerks haben einen ähnlichen Dateinamen wie
D_HUC101212CSS600_30602291_MS01_2800_0002.dlp.

Sie können bis zu vier Laufwerk-Firmware-Dateien auswählen, jeweils eine. Wenn mehrere Firmware-

Dateien eines Laufwerks mit demselben Laufwerk kompatibel sind, wird ein Dateikonflikt angezeigt. Legen Sie fest, welche Laufwerk-Firmware-Datei Sie für das Upgrade verwenden möchten, und entfernen Sie die andere.

c. Wählen Sie **Weiter**.

Select Drives listet die Laufwerke auf, die Sie mit den ausgewählten Firmware-Dateien aktualisieren können.

Es werden nur kompatible Laufwerke angezeigt.

Die ausgewählte Firmware für das Laufwerk wird in der Spalte **vorgeschlagene Firmware** angezeigt. Wenn Sie diese Firmware ändern müssen, wählen Sie **Zurück**.

d. Wählen Sie **Alle Laufwerke online aktualisieren** – Aktualisieren Sie die Laufwerke, die einen Firmware-Download unterstützen können, während das Speicherarray I/O-Vorgänge verarbeitet Sie müssen die I/O-Vorgänge für die zugehörigen Volumes, die diese Laufwerke verwenden, nicht stoppen, wenn Sie diese Aktualisierungsmethode auswählen.



Ein Online-Upgrade kann mehrere Stunden länger dauern als ein Offline-Upgrade.

Sie müssen den verwenden **"Offline-Methode"** Um die Firmware auf SSDs zu aktualisieren.

e. Wählen Sie in der ersten Spalte der Tabelle das Laufwerk oder die Laufwerke aus, die aktualisiert werden sollen.

Als Best Practice wird empfohlen, alle Laufwerke desselben Modells auf dieselbe Firmware-Version zu aktualisieren.

f. Wählen Sie **Start** und bestätigen Sie, dass Sie das Upgrade durchführen möchten.

Wenn Sie das Upgrade beenden möchten, wählen Sie **Stopp**. Alle derzeit ausgeführten Firmware-Downloads abgeschlossen. Alle nicht gestarteten Firmware-Downloads werden abgebrochen.



Das Anhalten der Laufwerk-Firmware-Aktualisierung kann zu Datenverlust oder nicht verfügbaren Laufwerken führen.

g. (Optional) um eine Liste der aktualisierten Versionen anzuzeigen, wählen Sie **Protokoll speichern**.

Die Protokolldatei wird im Download-Ordner für Ihren Browser mit dem Namen gespeichert `latest-upgrade-log-timestamp.txt`.

["Beheben Sie bei Bedarf Fehler bei der Aktualisierung der Treiber-Firmware"](#).

Aktualisieren Sie die Firmware des SG6000-Laufwerks mithilfe von SANtricity System Manager über die Offline-Methode

Verwenden Sie die Offline-Methode von SANtricity System Manager, um die Firmware auf den Laufwerken in Ihrer Appliance zu aktualisieren, um sicherzustellen, dass Sie über die neuesten Funktionen und Fehlerbehebungen verfügen.

Bevor Sie beginnen

- Die Storage Appliance hat einen optimalen Status.

- Alle Laufwerke haben einen optimalen Status.
- Das ist schon "[Versetzen Sie die StorageGRID Appliance in den Wartungsmodus](#)".



Während sich die Appliance im Wartungsmodus befindet, wird die I/O-Aktivität (Eingabe/Ausgabe) für den Storage Controller angehalten, um störende Storage-Vorgänge zu sichern.



Aktualisieren Sie nicht gleichzeitig die Laufwerk-Firmware auf mehr als einer StorageGRID Appliance. Dies kann je nach Bereitstellungsmodell und ILM-Richtlinie zu einer Nichtverfügbarkeit von Daten führen.

Über diese Aufgabe

Die Laufwerke werden parallel aktualisiert, während sich die Appliance im Wartungsmodus befindet. Wenn der Pool oder die Volume-Gruppe keine Redundanz unterstützt oder herabgesetzt ist, müssen Sie die Offline-Methode verwenden, um die Laufwerk-Firmware zu aktualisieren. Sie sollten auch die Offline-Methode für alle Laufwerke verwenden, die mit dem Flash-Lese-Cache oder einem Pool oder einer Volume-Gruppe verbunden sind, die derzeit heruntergestuft ist. Die Offline-Methode aktualisiert die Firmware nur, wenn alle I/O-Aktivitäten auf den zu aktualisierenden Laufwerken angehalten werden. Um die I/O-Aktivität zu beenden, versetzen Sie den Node in den Wartungsmodus.

Die Offline-Methode ist schneller als die Online-Methode und wird deutlich schneller sein, wenn viele Laufwerke in einer einzigen Appliance Upgrades erfordern. Allerdings müssen Nodes außer Betrieb genommen werden. Dies erfordert unter Umständen ein Wartungsfenster und ein Monitoring des Fortschritts. Wählen Sie die Methode aus, die am besten zu Ihren betrieblichen Verfahren passt und die Anzahl der Laufwerke, die aktualisiert werden müssen.



Es gibt zwei Laufwerkstypen: SSD und HDD. Sie müssen die Offline-Methode verwenden, um die Firmware auf den SSDs zu aktualisieren (z. B. SSD-Laufwerke im SG6060). Sie können entweder die Online- oder die Offline-Methode verwenden, um die Firmware auf HDDs zu aktualisieren.

Schritte

1. Vergewissern Sie sich, dass das Gerät in ist "[Wartungsmodus](#)".



Wenn Sie die Firmware in SSD-Laufwerken aktualisieren, die Teil einer Cache-Gruppe sind, müssen Sie sicherstellen, dass keine I/O-Vorgänge an zwischengespeicherte Volumes gesendet werden, während das Upgrade ausgeführt wird. Wenn sich die Appliance im Wartungsmodus befindet, werden keine I/O-Vorgänge an Volumes gesendet, während das Upgrade durchgeführt wird.

2. Greifen Sie mit einer der folgenden Methoden auf SANtricity System Manager zu:

- Verwenden Sie das StorageGRID-Appliance-Installationsprogramm, und wählen Sie **Erweitert > SANtricity-Systemmanager**
- Verwenden Sie den Grid-Manager, und wählen Sie **NODES > Storage Node > SANtricity System Manager** aus
- Verwenden Sie SANtricity System Manager, indem Sie zur Storage Controller-IP navigieren:

`https://Storage_Controller_IP`

3. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des SANtricity System Manager-Administrators ein.
4. Überprüfen Sie die Version der Laufwerk-Firmware, die derzeit in der Speicher-Appliance installiert ist:
 - a. Wählen Sie im SANtricity System Manager **SUPPORT > Upgrade-Center** aus.
 - b. Wählen Sie unter Laufwerk-Firmware-Upgrade die Option **Upgrade starten** aus.

Auf der Seite Laufwerksfirmware aktualisieren werden die aktuell installierten Laufwerksfirmware-Dateien angezeigt.

- c. Beachten Sie die aktuellen Versionen der Laufwerk-Firmware und die Laufwerkskennungen in der Spalte Aktueller Laufwerk-Firmware.

Upgrade Drive Firmware

1 Select Upgrade Files

Review your current drive firmware and select upgrade files below...

[What do I need to know before upgrading drive firmware?](#)

Current Drive Firmware

MS02, KPM51VUG800G

Total rows: 1 | ↻

In diesem Beispiel:

- Die Version der Laufwerk-Firmware lautet **MS02**.
 - Die Laufwerk-ID lautet **KPM51VUG800G**.
- d. Wählen Sie in der Spalte „verbundene Laufwerke“ die Option **Laufwerke anzeigen** aus, um anzuzeigen, wo diese Laufwerke in Ihrem Speichergerät installiert sind.
 - e. Schließen Sie das Fenster Upgrade Drive Firmware.
 5. Laden Sie das verfügbare Laufwerk-Firmware-Upgrade herunter, und bereiten Sie es vor:
 - a. Wählen Sie unter Laufwerk-Firmware-Upgrade **NetApp Support** aus.
 - b. Wählen Sie auf der NetApp Support-Website die Registerkarte **Downloads** aus und wählen Sie dann **E-Series Festplatten-Firmware** aus.

Die Seite E-Series Festplatten-Firmware wird angezeigt.

- c. Suchen Sie nach jedem in Ihrer Speicheranwendung installierten **Drive Identifier**, und stellen Sie sicher, dass jeder Laufwerkennung die neueste Firmware-Version hat.
 - Wenn die Firmware-Version kein Link ist, hat diese Laufwerkennung die neueste Firmware-Version.

- Wenn eine oder mehrere Laufwerk-Teilenummern für eine Laufwerksidentifikation aufgeführt sind, ist für diese Laufwerke ein Firmware-Upgrade verfügbar. Sie können einen beliebigen Link auswählen, um die Firmware-Datei herunterzuladen.

Drive Part Number	Descriptions	Drive Identifier	Firmware Rev. (Download)	Notes and Config Info	Release Date
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	MS03	MS02 Fixes Bug 1194908 MS03 Fixes Bug 1334862	04-Sep-2020

- Wenn eine spätere Firmware-Version aufgeführt wird, wählen Sie den Link im Firmware-Rev. Aus (Download) Spalte zum Herunterladen einer .zip Archiv mit der Firmware-Datei.
- Extrahieren Sie die von der Support-Website heruntergeladenen Archivdateien der Laufwerk-Firmware (entpacken).

6. Installieren Sie das Laufwerk-Firmware-Upgrade:

- Wählen Sie im SANtricity System Manager unter Upgrade der Laufwerk-Firmware die Option **Upgrade starten** aus.
- Wählen Sie **Durchsuchen** aus, und wählen Sie die neuen Laufwerk-Firmware-Dateien aus, die Sie von der Support-Website heruntergeladen haben.

Die Firmware-Dateien des Laufwerks haben einen ähnlichen Dateinamen wie
D_HUC101212CSS600_30602291_MS01_2800_0002.dlp.

Sie können bis zu vier Laufwerk-Firmware-Dateien auswählen, jeweils eine. Wenn mehrere Firmware-Dateien eines Laufwerks mit demselben Laufwerk kompatibel sind, wird ein Dateikonflikt angezeigt. Legen Sie fest, welche Laufwerk-Firmware-Datei Sie für das Upgrade verwenden möchten, und entfernen Sie die andere.

- Wählen Sie **Weiter**.

Select Drives listet die Laufwerke auf, die Sie mit den ausgewählten Firmware-Dateien aktualisieren können.

Es werden nur kompatible Laufwerke angezeigt.

Die ausgewählte Firmware für das Laufwerk wird in der Spalte **vorgeschlagene Firmware** angezeigt. Wenn Sie diese Firmware ändern müssen, wählen Sie **Zurück**.

- Wählen Sie **Alle Laufwerke offline aktualisieren (parallel)** – aktualisiert die Laufwerke, die einen Firmware-Download unterstützen können, nur während alle I/O-Aktivitäten auf allen Volumes angehalten werden, die die Laufwerke verwenden.



Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie diese Methode verwenden. Sie sollten die Methode **Offline** verwenden, um die Laufwerksfirmware zu aktualisieren.



Wenn Sie die Offline-Aktualisierung (parallel) verwenden möchten, fahren Sie nur dann fort, wenn Sie sicher sind, dass sich das Gerät im Wartungsmodus befindet. Wenn die Appliance nicht in den Wartungsmodus versetzt wird, bevor ein Offline-Update der Laufwerk-Firmware initiiert wird, kann dies zu einem Datenverlust führen.

- e. Wählen Sie in der ersten Spalte der Tabelle das Laufwerk oder die Laufwerke aus, die aktualisiert werden sollen.

Als Best Practice wird empfohlen, alle Laufwerke desselben Modells auf dieselbe Firmware-Version zu aktualisieren.

- f. Wählen Sie **Start** und bestätigen Sie, dass Sie das Upgrade durchführen möchten.

Wenn Sie das Upgrade beenden möchten, wählen Sie **Stopp**. Alle derzeit ausgeführten Firmware-Downloads abgeschlossen. Alle nicht gestarteten Firmware-Downloads werden abgebrochen.



Das Anhalten der Laufwerk-Firmware-Aktualisierung kann zu Datenverlust oder nicht verfügbaren Laufwerken führen.

- g. (Optional) um eine Liste der aktualisierten Versionen anzuzeigen, wählen Sie **Protokoll speichern**.

Die Protokolldatei wird im Download-Ordner für Ihren Browser mit dem Namen gespeichert `latest-upgrade-log-timestamp.txt`.

["Beheben Sie bei Bedarf Fehler bei der Aktualisierung der Treiber-Firmware"](#).

7. Führen Sie nach erfolgreichem Abschluss des Verfahrens alle weiteren Wartungsmaßnahmen durch, während sich der Node im Wartungsmodus befindet. Wenn Sie fertig sind oder Fehler aufgetreten sind und neu gestartet werden möchten, gehen Sie zum StorageGRID-Installationsprogramm und wählen Sie **Erweitert > Neustart-Controller** aus. Wählen Sie dann eine der folgenden Optionen aus:

- **Neustart in StorageGRID.**
- **Neustart im Wartungsmodus.** Booten Sie den Controller neu, und belassen Sie den Node im Wartungsmodus. Wählen Sie diese Option aus, wenn während des Verfahrens Fehler auftreten und Sie von vorne beginnen möchten. Nachdem der Node das Neubooten in den Wartungsmodus abgeschlossen hat, starten Sie den entsprechenden Schritt während des ausgefallenen Verfahrens neu.

Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite Knoten sollte ein normaler Status angezeigt werden (grünes Häkchen-Symbol  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

DASHBOARD

ALERTS ✓ ^

Current

Resolved

Silences

Rules

Email setup

NODES

TENANTS

ILM ∨

CONFIGURATION

MAINTENANCE

SUPPORT

Nodes

View the list and status of sites and grid nodes.

Search...

Total node count: 14

Name ? ∨	Type ∨	Object data used ? ∨	Object metadata used ? ∨	CPU usage ? ∨
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Fehler beim Upgrade der Laufwerk-Firmware beheben

Beheben Sie Fehler, die auftreten können, wenn Sie SANtricity System Manager zum Aktualisieren der Firmware auf den Laufwerken in Ihrer Appliance verwenden.

- **Fehlgeschlagene zugewiesene Laufwerke**

- Ein Grund für den Fehler könnte sein, dass das Laufwerk nicht über die entsprechende Signatur verfügt. Stellen Sie sicher, dass es sich bei dem betroffenen Laufwerk um ein autorisiertes Laufwerk handelt. Weitere Informationen erhalten Sie vom technischen Support.
- Stellen Sie beim Austausch eines Laufwerks sicher, dass das Ersatzlaufwerk eine Kapazität hat, die der des ausgefallenen Laufwerks entspricht oder größer ist als das ausgefallene Laufwerk, das Sie ersetzen.
- Sie können das ausgefallene Laufwerk ersetzen, während das Speicher-Array I/O-Vorgänge erhält

- **Speicher-Array prüfen**

- Stellen Sie sicher, dass jedem Controller eine IP-Adresse zugewiesen wurde.
- Stellen Sie sicher, dass alle Kabel, die an den Controller angeschlossen sind, nicht beschädigt sind.
- Stellen Sie sicher, dass alle Kabel fest angeschlossen sind.

- * Integrierte Hot-Spare-Laufwerke*

Diese Fehlerbedingung muss korrigiert werden, bevor Sie die Firmware aktualisieren können.

- **Unvollständige Volume-Gruppen**

Wenn eine oder mehrere Volume-Gruppen oder Disk Pools unvollständig sind, müssen Sie diese Fehlerbedingung korrigieren, bevor Sie die Firmware aktualisieren können.

- **Exklusive Operationen (außer Hintergrund-Medien/Paritäts-Scan), die derzeit auf beliebigen Volume-Gruppen ausgeführt werden**

Wenn ein oder mehrere exklusive Vorgänge ausgeführt werden, müssen die Vorgänge abgeschlossen

sein, bevor die Firmware aktualisiert werden kann. Überwachen Sie den Fortschritt des Betriebs mit System Manager.

- **Fehlende Volumen**

Sie müssen den fehlenden Datenträgerzustand korrigieren, bevor die Firmware aktualisiert werden kann.

- **Entweder Controller in einem anderen Zustand als optimal**

Einer der Controller des Storage Arrays muss Aufmerksamkeit schenken. Diese Bedingung muss korrigiert werden, bevor die Firmware aktualisiert werden kann.

- **Unpassende Speicherpartitionsdaten zwischen Controller-Objektgrafiken**

Beim Validieren der Daten auf den Controllern ist ein Fehler aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **SPM Überprüfung des Datenbankcontrollers schlägt fehl**

Auf einem Controller ist ein Fehler bei der Zuordnung von Speicherpartitionen zur Datenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Überprüfung der Konfigurationsdatenbank (sofern von der Controller-Version des Speicherarrays unterstützt)**

Auf einem Controller ist ein Fehler in der Konfigurationsdatenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **MEL-bezogene Prüfungen**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **In den letzten 7 Tagen wurden mehr als 10 DDE Informations- oder kritische MEL-Ereignisse gemeldet**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Mehr als 2 Seiten 2C kritische MEL-Ereignisse wurden in den letzten 7 Tagen gemeldet**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **In den letzten 7 Tagen wurden mehr als 2 heruntergestuften Drive Channel-kritische MEL-Ereignisse gemeldet**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Mehr als 4 kritische MEL-Einträge in den letzten 7 Tagen**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

Ein- und Ausschalten der Controller-ID-LED

Die blaue Identify-LED auf der Vorder- und Rückseite des Controllers kann eingeschaltet werden, um das Gerät in einem Datacenter zu lokalisieren.

Bevor Sie beginnen

Sie haben die BMC-IP-Adresse des Controllers, den Sie identifizieren möchten.

Schritte

1. Greifen Sie auf die BMC-Schnittstelle des Controllers zu.
2. Wählen Sie **Server Identify** Aus.

Der aktuelle Status der Identifizieren-LED ist ausgewählt.

3. Wählen Sie **EIN** oder **AUS**, und wählen Sie dann **Aktion ausführen**.

Wenn Sie **EIN** auswählen, leuchten die blauen Identifizieren-LEDs auf der Vorderseite (abgebildet) und der Rückseite des Geräts.



Wenn eine Blende auf dem Controller installiert ist, kann es schwierig sein, die vordere Identify-LED zu erkennen.

4. Schalten Sie die LED nach Bedarf ein und aus.

Verwandte Informationen

["Überprüfen Sie, ob der Fibre-Channel-HBA ersetzt werden soll"](#)

["Controller im Datacenter finden"](#)

["Greifen Sie auf die BMC-Schnittstelle zu"](#)

Controller im Datacenter finden

Suchen Sie den Controller, um Hardware-Wartungsarbeiten oder Upgrades durchzuführen.

Bevor Sie beginnen

- Sie haben festgestellt, welcher Controller gewartet werden muss.

(Optional) um den Controller in Ihrem Rechenzentrum zu finden, schalten Sie die blaue Identify-LED ein.

["Ein- und Ausschalten der Controller-ID-LED"](#)

Schritte

1. Ermitteln Sie den für die Wartung im Datacenter erforderlichen Controller.

- Suchen Sie nach einer blau leuchtenden LED an der Vorder- oder Rückseite des Controllers.

Die vordere Identify-LED befindet sich hinter der Frontblende des Controllers und kann schwierig feststellen, ob die Blende montiert ist.



- Überprüfen Sie, ob die an der Vorderseite des jeden Controllers angebrachten Tags eine übereinstimmende Teilenummer erhalten.
2. Entfernen Sie die Frontverkleidung des Controllers, wenn eine installiert ist, um auf die Bedienelemente und Anzeigen auf der Vorderseite zuzugreifen.
3. Optional: Schalten Sie die blaue Identify-LED aus, wenn Sie sie zur Lokalisierung des Controllers verwendet haben.
- Drücken Sie den Schalter Identifikation LED an der Vorderseite des Controllers.
 - Verwenden Sie die BMC-Schnittstelle des Controllers.

["Ein- und Ausschalten der Controller-ID-LED"](#)

Verwandte Informationen

["Entfernen Sie den Fibre Channel HBA"](#)

["Entfernen Sie den SG6000-CN Controller aus dem Schrank oder Rack"](#)

["Fahren Sie den SG6000-CN-Controller herunter"](#)

Ein- und Ausschalten des Controllers

Fahren Sie den SG6000-CN-Controller herunter

Fahren Sie den SG6000-CN-Controller herunter, um die Hardware zu warten.

Bevor Sie beginnen

- Der SG6000-CN Controller ist physisch zu finden, der im Datacenter gewartet werden muss. Siehe ["Controller im Datacenter finden"](#).

Über diese Aufgabe

Um Serviceunterbrechungen zu vermeiden, vergewissern Sie sich, dass alle anderen Storage-Nodes mit dem Grid verbunden sind, bevor Sie den Controller herunterfahren oder den Controller während eines geplanten

Wartungsfensters herunterfahren, wenn die Serviceunterbrechungen akzeptabel sind. Weitere Informationen finden Sie unter "[Monitoring der Verbindungsstatus der Nodes](#)".



Wenn Sie jemals eine ILM-Regel verwendet haben, die nur eine Kopie eines Objekts erstellt, müssen Sie den Controller während eines geplanten Wartungsfensters herunterfahren. Andernfalls verlieren Sie während dieses Verfahrens vorübergehend den Zugriff auf diese Objekte. + Weitere Informationen zum Verwalten von Objekten mit Information Lifecycle Management finden Sie unter.

Schritte

1. Fahren Sie den SG6000-CN-Controller herunter.



Sie müssen ein kontrolliertes Herunterfahren des Geräts durchführen, indem Sie die unten angegebenen Befehle eingeben. Es ist eine Best Practice, nach Möglichkeit eine kontrollierte Abschaltung durchzuführen, um unnötige Warnmeldungen zu vermeiden, sicherzustellen, dass vollständige Protokolle verfügbar sind und Serviceunterbrechungen zu vermeiden.

- a. Wenn Sie sich noch nicht beim Grid-Knoten angemeldet haben, melden Sie sich mit PuTTY oder einem anderen ssh-Client an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

- b. Fahren Sie den SG6000-CN-Controller herunter:
shutdown -h now

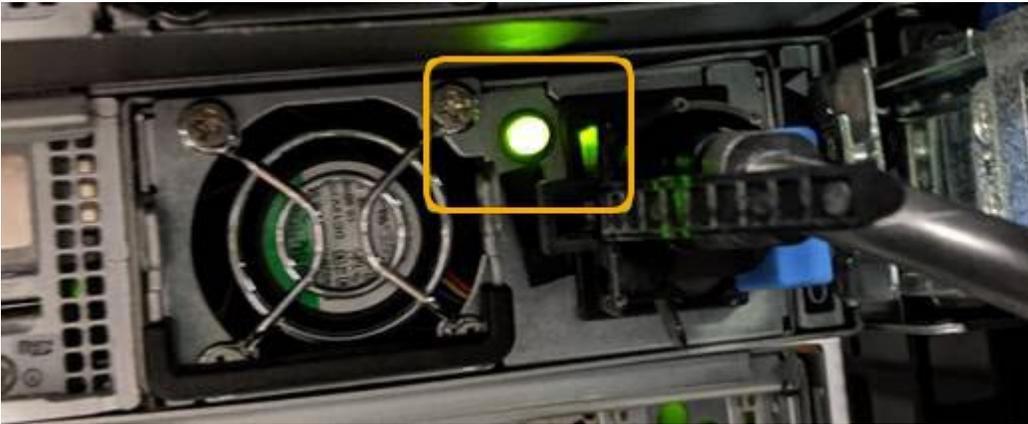
Dieser Befehl kann bis zu 10 Minuten in Anspruch nehmen.

2. Überprüfen Sie anhand einer der folgenden Methoden, ob der SG6000-CN-Controller ausgeschaltet ist:
 - Schauen Sie sich die blaue ein/aus-LED an der Vorderseite des Controllers an und bestätigen Sie, dass sie ausgeschaltet ist.



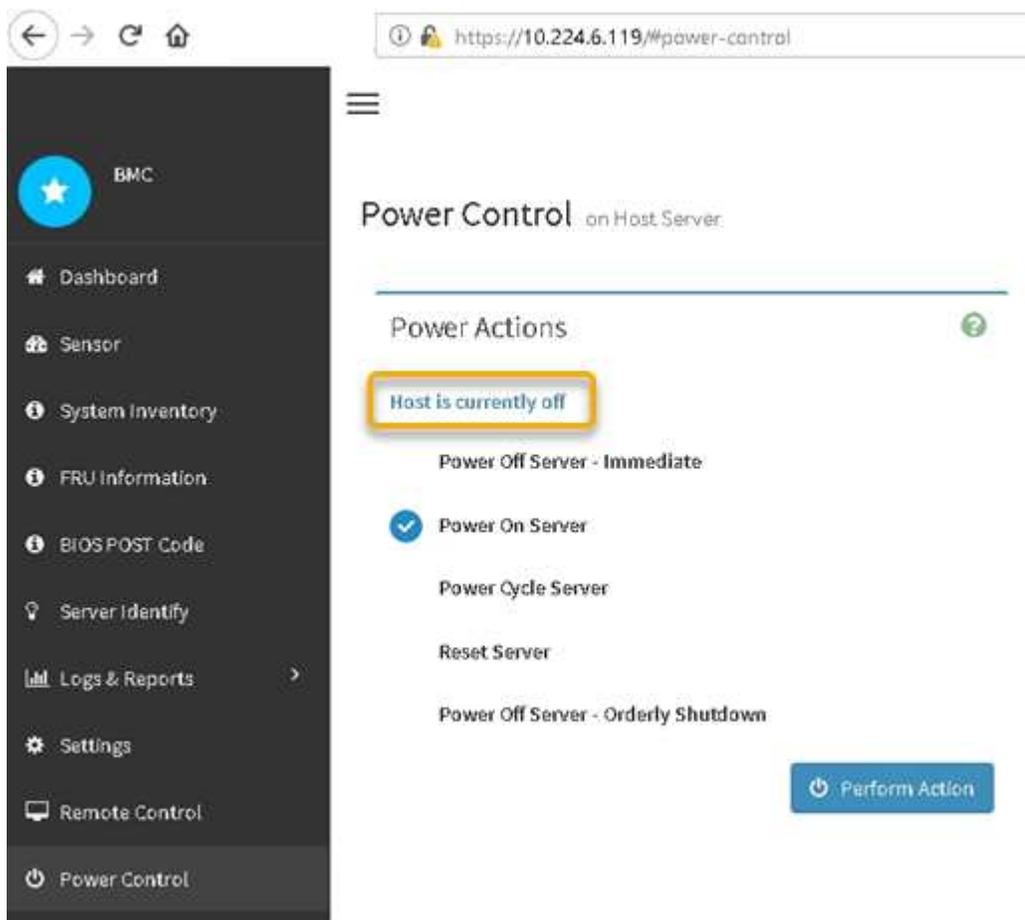
- Schauen Sie sich die grünen LEDs an den beiden Netzteilen auf der Rückseite des Controllers an und

bestätigen Sie, dass sie mit einer normalen Geschwindigkeit (etwa ein Blinken pro Sekunde) blinken.



- Verwenden Sie die BMC-Schnittstelle des Controllers:
 - i. Greifen Sie auf die BMC-Schnittstelle des Controllers zu.

"Greifen Sie auf die BMC-Schnittstelle zu"
 - ii. Wählen Sie **Power Control**.
 - iii. Stellen Sie sicher, dass die Strommaßnahmen darauf hindeuten, dass der Host derzeit ausgeschaltet ist.



Verwandte Informationen

["Entfernen Sie den SG6000-CN Controller aus dem Schrank oder Rack"](#)

Schalten Sie den SG6000-CN Controller ein, und überprüfen Sie den Betrieb

Schalten Sie den Controller nach dem Abschluss der Wartung ein.

Bevor Sie beginnen

- Der Controller wurde in einem Rack oder Rack installiert und die Daten- und Stromkabel angeschlossen.

["Installieren Sie den SG6000-CN Controller wieder in den Schrank oder Rack"](#)

- Der Controller befindet sich physisch im Datacenter.

["Controller im Datacenter finden"](#)

Schritte

1. Schalten Sie den SG6000-CN-Controller ein, und überwachen Sie die Controller-LEDs und den Startcode mithilfe einer der folgenden Methoden:

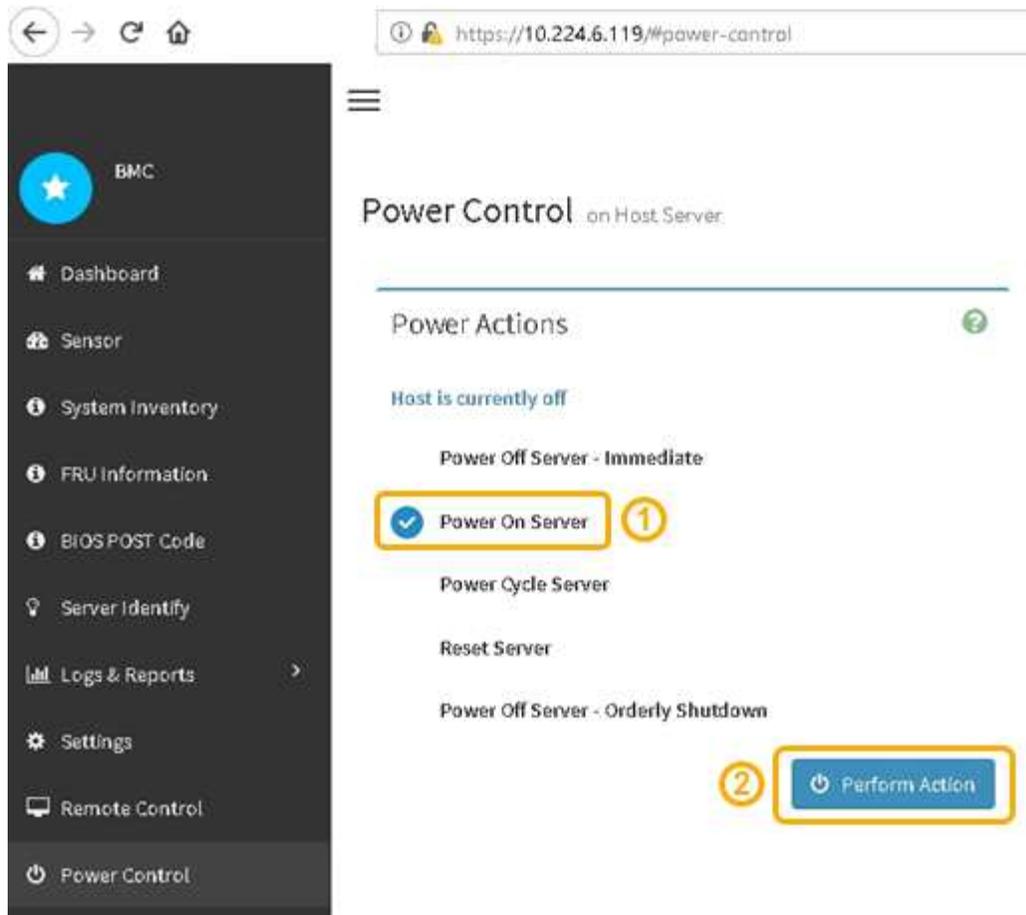
- Drücken Sie den Netzschalter an der Vorderseite des Controllers.



- Verwenden Sie die BMC-Schnittstelle des Controllers:
 - i. Greifen Sie auf die BMC-Schnittstelle des Controllers zu.

["Greifen Sie auf die BMC-Schnittstelle zu"](#)

- ii. Wählen Sie **Power Control**.
- iii. Wählen Sie **Power on Server** und dann **Perform Action**.



Verwenden Sie die BMC-Schnittstelle, um den Startstatus zu überwachen.

2. Vergewissern Sie sich, dass der Appliance-Controller im Grid Manager und ohne Warnungen angezeigt wird.

Es kann bis zu 20 Minuten dauern, bis der Controller im Grid Manager angezeigt wird.

3. Vergewissern Sie sich, dass der neue SG6000-CN-Controller voll funktionsfähig ist:

- a. Melden Sie sich mit PuTTY oder einem anderen SSH-Client am Grid-Knoten an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

- b. Geben Sie den folgenden Befehl ein, und überprüfen Sie, ob die erwartete Ausgabe zurückgegeben wird:

```
cat /sys/class/fc_host/*/port_state
```

Erwartete Ausgabe:

```
Online
Online
Online
Online
```

Wenn die erwartete Ausgabe nicht zurückgegeben wird, wenden Sie sich an den technischen Support.

- c. Geben Sie den folgenden Befehl ein, und überprüfen Sie, ob die erwartete Ausgabe zurückgegeben wird:

```
cat /sys/class/fc_host/*/speed
```

Erwartete Ausgabe:

```
16 Gbit
16 Gbit
16 Gbit
16 Gbit
```

+

Wenn die erwartete Ausgabe nicht zurückgegeben wird, wenden Sie sich an den technischen Support.

- a. Stellen Sie auf der Seite Knoten im Grid Manager sicher, dass der Appliance-Node mit dem Raster verbunden ist und keine Warnmeldungen enthält.



Nehmen Sie einen anderen Appliance-Node nur offline, wenn diese Appliance über ein grünes Symbol verfügt.

4. Optional: Befestigen Sie die Frontverkleidung, falls eine entfernt wurde.

Verwandte Informationen

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

Ändern der Link-Konfiguration des SG6000-CN Controllers

Sie können die Ethernet-Link-Konfiguration des SG6000-CN Controllers ändern. Sie können den Port Bond-Modus, den Netzwerk-Bond-Modus und die Verbindungsgeschwindigkeit ändern.

Bevor Sie beginnen

Das Gerät war ["In den Wartungsmodus versetzt"](#).

Über diese Aufgabe

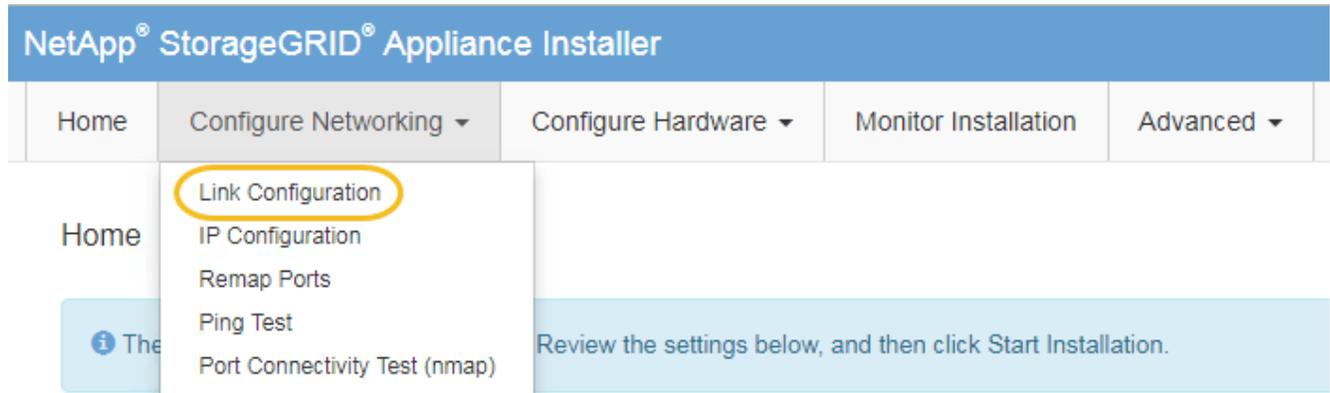
Zum Ändern der Ethernet-Link-Konfiguration des SG6000-CN Controllers gehören folgende Optionen:

- Ändern des **Port Bond Modus** von Fixed zu Aggregate oder von Aggregate zu Fixed
- Ändern des **Netzwerk-Bond-Modus** von Active-Backup zu LACP oder von LACP zu Active-Backup
- Aktivieren oder Deaktivieren von VLAN-Tagging oder Ändern des Werts einer VLAN-Tag-Nummer

- Ändern der Verbindungsgeschwindigkeit.

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren** > **Link-Konfiguration** aus.



2. Geben Sie die gewünschten Änderungen an der Linkkonfiguration an.

Weitere Informationen zu den Optionen finden Sie unter "[Netzwerkverbindungen konfigurieren](#)".

3. Wenn Sie mit Ihrer Auswahl zufrieden sind, klicken Sie auf **Speichern**.



Wenn Sie Änderungen am Netzwerk oder an der Verbindung vorgenommen haben, über die Sie verbunden sind, können Sie die Verbindung verlieren. Wenn die Verbindung nicht innerhalb von 1 Minute wiederhergestellt wird, geben Sie die URL für den StorageGRID-Appliance-Installer erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:

`https://Appliance_Controller_IP:8443`

Wenn Sie Änderungen an den VLAN-Einstellungen vorgenommen haben, hat sich das Subnetz für die Appliance möglicherweise geändert. Wenn Sie die IP-Adressen für die Appliance ändern müssen, befolgen Sie die "[Konfigurieren Sie IP-Adressen](#)" Anweisungen.

["Konfigurieren Sie StorageGRID-IP-Adressen"](#)

4. Wählen Sie im Menü die Option **Netzwerk konfigurieren** > **Ping-Test** aus.
5. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in allen Netzwerken zu überprüfen, die möglicherweise von den in vorgenommenen Änderungen der Verbindungskonfiguration betroffen sind [Änderungen der Linkkonfiguration](#) Schritt:

Zusätzlich zu allen anderen Tests, die Sie durchführen möchten, bestätigen Sie, dass Sie die Grid-Netzwerk-IP-Adresse des primären Admin-Knotens und die Grid-Netzwerk-IP-Adresse von mindestens einem anderen Speicherknoten pinggen können. Falls erforderlich, kehren Sie zum zurück [Änderungen der Linkkonfiguration](#) Führen Sie Schritte aus, und beheben Sie alle Probleme mit der Link-Konfiguration.

6. Wenn Sie zufrieden sind, dass die Änderungen an der Link-Konfiguration funktionieren und zusätzliche Verfahren erforderlich sind, während der Node sich im Wartungsmodus befindet, führen Sie diese jetzt aus. Wenn Sie fertig sind oder Fehler auftreten und von vorne beginnen möchten, wählen Sie **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

- Wählen Sie **Neustart in StorageGRID** aus
- Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. Wählen Sie diese Option aus, wenn während des Verfahrens Fehler auftreten und neu starten möchten. Nachdem der Node das Neubooten in den Wartungsmodus abgeschlossen hat, starten Sie den entsprechenden Schritt während des ausgefallenen Verfahrens neu.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden (✓ Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Hardware-Verfahren

Erweiterungs-Shelf für das implementierte SG6060 hinzufügen

Zur Erhöhung der Storage-Kapazität können Sie ein oder zwei Erweiterungs-Shelfs zu einem SG6060 hinzufügen, das bereits in einem StorageGRID System implementiert ist.

Bevor Sie beginnen

- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen StorageGRID 11.4 oder höher ausführen.
- Sie haben das Erweiterungs-Shelf und zwei SAS-Kabel für jedes Erweiterungs-Shelf.
- Dort befinden sich die Storage Appliance physisch, wo das Erweiterungs-Shelf im Datacenter hinzugefügt wird.

["Controller im Datacenter finden"](#)

Über diese Aufgabe

Um ein Erweiterungs-Shelf hinzuzufügen, führen Sie die folgenden grundlegenden Schritte aus:

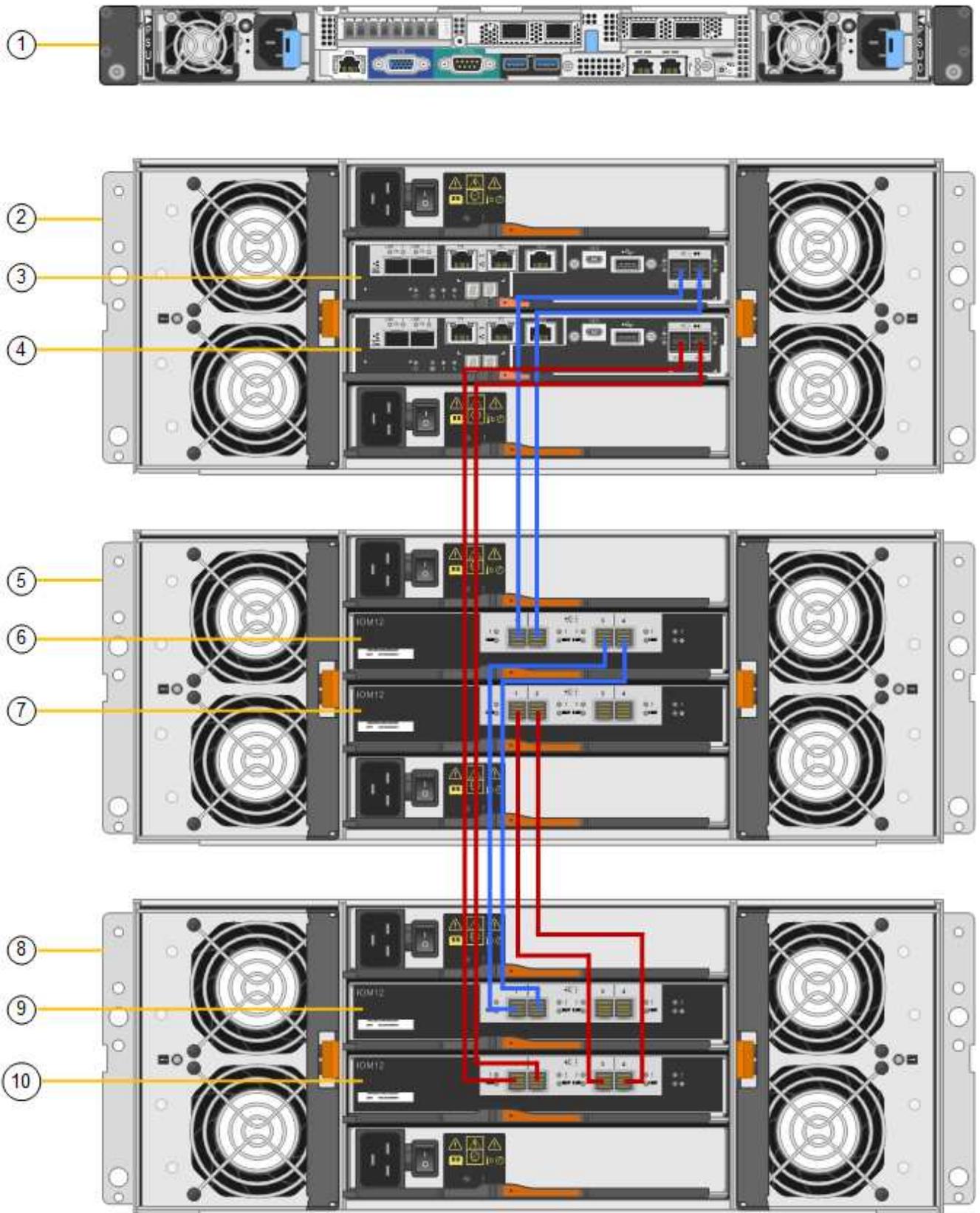
- Installieren Sie die Hardware in den Schrank oder Rack.
- Platzieren Sie das SG6060 in den Wartungsmodus.
- Verbinden Sie das Erweiterungs-Shelf mit dem E2860 Controller-Shelf oder mit einem anderen Erweiterungs-Shelf.
- Starten Sie die Erweiterung mithilfe des StorageGRID-Appliance-Installationsprogramms
- Warten Sie, bis die neuen Volumes konfiguriert sind.

Das Abschließen des Vorgangs für ein oder zwei Erweiterungs-Shelfs sollte eine Stunde oder weniger pro Appliance-Node dauern. Zur Minimierung von Ausfallzeiten werden Sie in den folgenden Schritten aufgefordert, die neuen Erweiterungs-Shelfs und Laufwerke zu installieren, bevor Sie das SG6060 in den Wartungsmodus versetzen. Die verbleibenden Schritte sollten etwa 20 bis 30 Minuten pro Appliance-Node in Anspruch nehmen.

Schritte

1. Befolgen Sie die Anweisungen für ["Installieren von Shelves mit 60 Laufwerken in einem Schrank oder Rack"](#).
2. Befolgen Sie die Anweisungen für ["Installieren der Laufwerke"](#).
3. Vom Grid Manager ["Versetzen Sie den SG6000-CN Controller in den Wartungsmodus"](#).
4. Verbinden Sie jedes Erweiterungs-Shelf mit dem E2860 Controller-Shelf, wie in der Abbildung dargestellt.

Diese Zeichnung zeigt zwei Erweiterungs-Shelfs. Wenn nur einer vorhanden ist, verbinden Sie IOM A mit Controller A und verbinden Sie IOM B mit Controller B



Legende	Beschreibung
1	SG6000-CN

Legende	Beschreibung
2	E2860 Controller-Shelf
3	Controller A
4	Controller B
5	Erweiterungs-Shelf 1
6	IOM A für Erweiterungs-Shelf 1
7	IOM B für Erweiterungs-Shelf 1
8	Erweiterungs-Shelf 2
9	IOM A für Erweiterungs-Shelf 2
10	IOM B für Erweiterungs-Shelf 2

5. Schließen Sie die Stromkabel an, und setzen Sie Strom auf die Erweiterungs-Shelves.
 - a. Schließen Sie ein Netzkabel an jede der beiden Netzteile in jedem Erweiterungs-Shelf an.
 - b. Verbinden Sie die beiden Netzkabel jedes Erweiterungs-Shelf mit zwei verschiedenen PDUs im Schrank oder Rack.
 - c. Schalten Sie die beiden Netzschalter für jedes Erweiterungs-Shelf ein.
 - Schalten Sie die Netzschalter während des Einschalters nicht aus.
 - Die Lüfter in den Erweiterungsregalen sind beim ersten Start möglicherweise sehr laut. Das laute Geräusch beim Anfahren ist normal.
6. Überwachen Sie die Startseite des Installationsprogramms für StorageGRID-Geräte.

Die Erweiterungs-Shelves wurden in etwa fünf Minuten eingeschaltet und vom System erkannt. Auf der Startseite wird die Anzahl der neu erkannten Erweiterungs-Shelves angezeigt, und die Schaltfläche Expansion starten ist aktiviert.

Der Screenshot zeigt Beispiele für Meldungen, die auf der Startseite angezeigt werden können, je nach Anzahl der vorhandenen oder neuen Erweiterungs-Shelves, wie folgt:

- Das oben auf der Seite eingekreiste Banner zeigt die Gesamtzahl der erkannten Erweiterungs-Shelves an.
 - Das Banner zeigt die Gesamtzahl der Erweiterungs-Shelves an, unabhängig davon, ob die Shelves konfiguriert und implementiert oder neu und nicht konfiguriert sind.
 - Wenn keine Erweiterungs-Shelves erkannt werden, wird das Banner nicht angezeigt.
- Die Nachricht, die unten auf der Seite eingekreist wurde, zeigt an, dass eine Erweiterung bereit ist, gestartet zu werden.
 - Die Meldung gibt die Anzahl der neu erkannten Erweiterungs-Shelves StorageGRID an. „Attached“ gibt an, dass das Shelf erkannt wird. „Unconfigured“ gibt an, dass das Shelf neu und noch nicht

mit dem Installationsprogramm für StorageGRID Appliance konfiguriert ist.



Bereits bereitgestellte Erweiterungs-Shelfs sind in dieser Meldung nicht enthalten. Sie werden in die Zählung in das Banner oben auf der Seite aufgenommen.

- Die Meldung wird nicht angezeigt, wenn keine neuen Erweiterungseinschübe erkannt werden.

The screenshot displays the configuration interface for a StorageGRID Appliance. At the top, a blue banner contains two messages: "The expansion is ready to be started. Make sure this page accurately indicates the number of new storage shelves you are trying to add, then click Start Expansion." and "The storage system contains 2 expansion shelves." Below this, the "This Node" section shows "Node type" set to "Storage" and "Node name" set to "NetApp-SGA", with "Cancel" and "Save" buttons. The "Primary Admin Node connection" section has "Enable Admin Node discovery" checked, "Primary Admin Node IP" set to "172.16.4.71", and "Connection state" as "Connection to 172.16.4.71 ready", also with "Cancel" and "Save" buttons. The "Installation" section shows the "Current state" as "Ready to start configuration of 1 attached but unconfigured expansion shelf." and a prominent "Start Expansion" button.

7. Lösen Sie bei Bedarf alle in den Meldungen auf der Startseite beschriebenen Probleme.

Verwenden Sie beispielsweise den SANtricity System Manager, um alle Probleme mit der Storage-Hardware zu beheben.

8. Überprüfen Sie, ob die Anzahl der auf der Startseite angezeigten Erweiterungs-Shelfs mit der Anzahl der hinzuzufügenden Erweiterungs-Shelfs übereinstimmt.



Wenn die neuen Erweiterungs-Shelfs nicht erkannt wurden, überprüfen Sie, ob sie ordnungsgemäß verkabelt und eingeschaltet sind.

9. Klicken Sie auf **Erweiterung starten**, um die Erweiterungs-Shelfs zu konfigurieren und für den Objekt-Storage verfügbar zu machen.
10. Überwachen Sie den Fortschritt der Erweiterungs-Shelf-Konfiguration.

Fortschrittsbalken werden auf der Webseite angezeigt, genau wie bei der Erstinstallation.

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete	
Clear existing configuration	<div style="width: 100%; height: 10px; background-color: green;"></div>	Skipped	
Configure volumes	<div style="width: 30%; height: 10px; background-color: blue;"></div>	Creating volume StorageGRID-obj-22	
Configure caching	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Pending	
Configure host settings	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Pending	

2. Complete storage expansion			Pending

Nach Abschluss der Konfiguration wird das Gerät automatisch neu gestartet, um den Wartungsmodus zu beenden und wieder in das Raster einzusteigen. Dieser Vorgang kann bis zu 20 Minuten dauern.



Um die Konfiguration des Erweiterungs-Shelfs erneut zu versuchen, falls dies fehlschlägt, wechseln Sie zum Installationsprogramm der StorageGRID-Appliance, wählen Sie **Erweitert** > **Controller neu starten** und wählen Sie dann **Neustart im Wartungsmodus** aus. Nachdem der Node neu gebootet wurde, versuchen Sie den erneut [Konfiguration des Erweiterungs-Shelfs](#).

Wenn der Neustart abgeschlossen ist, sieht die Registerkarte **Tasks** wie der folgende Screenshot aus:

The screenshot shows a navigation bar with tabs: Overview, Hardware, Network, Storage, Objects, ILM, Events, and Tasks (selected). Below the navigation bar, there are two main sections:

- Reboot**: Shuts down and restarts the node. A blue button labeled "Reboot" is visible.
- Maintenance Mode**: Places the appliance's compute controller into maintenance mode. A blue button labeled "Maintenance Mode" is visible.

11. Überprüfen Sie den Status des Appliance Storage Node und der neuen Erweiterungs-Shelfs.

- Wählen Sie im Grid Manager **NODES** aus, und überprüfen Sie, ob der Storage Node der Appliance über ein grünes Häkchen verfügt.

Das grüne Häkchen bedeutet, dass keine Meldungen aktiv sind und der Node mit dem Raster verbunden ist. Eine Beschreibung der Knotensymbole finden Sie unter "[Überwachen Sie die Status der Node-Verbindung](#)".

- Wählen Sie die Registerkarte **Storage** aus, und bestätigen Sie, dass in der Objektspeichertabelle für jedes hinzugefügte Erweiterungs-Shelf 16 neue Objektspeichern angezeigt werden.
- Vergewissern Sie sich, dass jedes neue Erweiterungs-Shelf den Shelf-Status „Nominal“ sowie den Konfigurationsstatus von „konfiguriert“ aufweist.

Tauschen Sie den Speicher-Controller in der SG6000 aus

Möglicherweise müssen Sie einen E2800 Series Controller oder einen EF570 Controller austauschen, wenn er nicht optimal funktioniert oder wenn er ausgefallen ist.

Bevor Sie beginnen

- Sie verfügen über einen Ersatzcontroller mit derselben Teilenummer wie der zu ersetzenden Controller.
- Sie verfügen über Etiketten, um jedes Kabel, das mit dem Controller verbunden ist, zu identifizieren.
- Sie haben ein ESD-Armband oder andere antistatische Vorsichtsmaßnahmen getroffen.
- Sie haben einen #1 Kreuzschlitzschraubendreher.
- Sie haben die Storage Appliance physisch gefunden, an der der Controller im Datacenter ausgetauscht wird.

"Controller im Datacenter finden"



Verlassen Sie sich beim Austausch eines Controllers in der StorageGRID Appliance nicht auf die Anweisungen zur E-Series, da die Vorgehensweisen nicht identisch sind.

Über diese Aufgabe

Sie haben zwei Möglichkeiten zur Feststellung, ob ein ausgefallener Controller aufgetreten ist:

- Der Recovery Guru im SANtricity System Manager führt Sie dazu, den Controller zu ersetzen.
- Die gelbe Warn-LED am Controller leuchtet und gibt an, dass der Controller einen Fehler aufweist.



Wenn die Warn-LEDs für beide Controller im Shelf leuchten, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

Wenn Ihre Appliance zwei Storage-Controller enthält, können Sie einen der Controller austauschen, während das Gerät eingeschaltet ist und Lese-/Schreibvorgänge ausführt, sofern die folgenden Bedingungen erfüllt sind:

- Der zweite Controller im Shelf hat optimalen Status.
- Im Feld **OK to remove** im Bereich Details des Recovery Guru im SANtricity System Manager wird **Ja** angezeigt, was darauf hinweist, dass es sicher ist, diese Komponente zu entfernen.



Wenn möglich, schalten Sie das Gerät für dieses Ersatzverfahren in den Wartungsmodus, um die potenziellen Auswirkungen unvorhergesehener Fehler oder Ausfälle zu minimieren.



Wenn der zweite Controller im Shelf nicht über den optimalen Status verfügt oder wenn der Recovery Guru angibt, dass er nicht in Ordnung ist, den Controller zu entfernen, wenden Sie sich an den technischen Support.

Wenn Sie einen Controller austauschen, müssen Sie den Akku aus dem ursprünglichen Controller entfernen und in den Ersatzcontroller einsetzen. In einigen Fällen müssen Sie möglicherweise auch die Host-Schnittstellenkarte vom ursprünglichen Controller entfernen und im Ersatzcontroller installieren.



Die Storage Controller in den meisten Appliance-Modellen umfassen keine Host Interface Cards (HIC).

Schritt 1: Bereiten Sie die Ersatzsteuerung vor

Bereiten Sie den neuen E2800A- oder E2800B-Controller vor.

Schritte

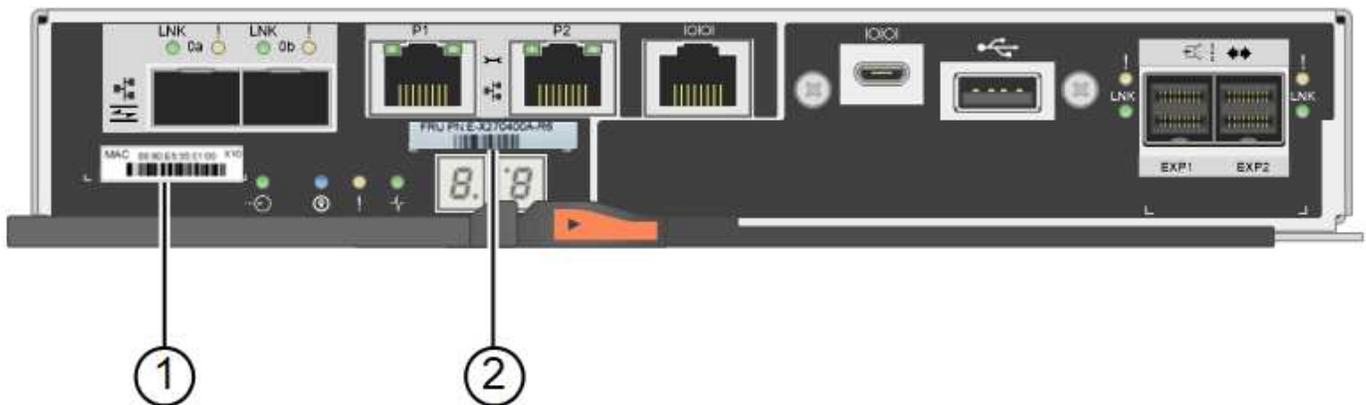
1. Packen Sie die neue Steuerung aus und stellen Sie sie auf eine flache, statische Oberfläche.

Bewahren Sie das Verpackungsmaterial auf, das beim Versand der fehlerhaften Steuerung verwendet werden soll.

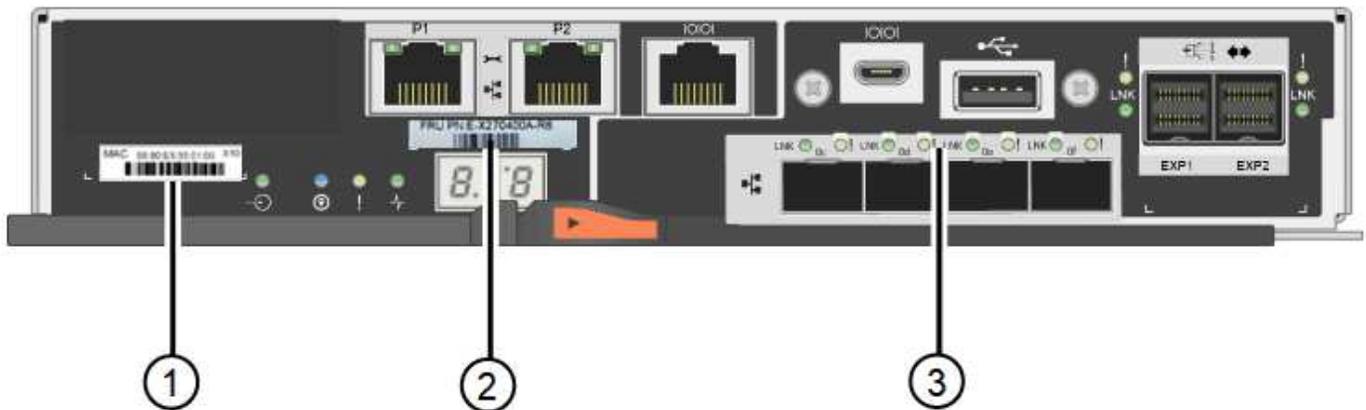
2. Suchen Sie die Etiketten für MAC-Adresse und FRU-Teilenummer auf der Rückseite des Ersatzcontrollers.

Diese Abbildungen zeigen den E2800A-Controller und den E2800B-Controller. Das Verfahren zum Austausch der E2800 Controller der Serie und des EF570 Controllers ist identisch.

E2800A Storage-Controller:



E2800B Storage-Controller:



Etikett	Komponente	Beschreibung
1	MAC-Adresse	Die MAC-Adresse für Management-Port 1 („P1 auf E2800A und 0a auf E2800B“). Wenn Sie die IP-Adresse des Original-Controllers über DHCP erhalten haben, benötigen Sie diese Adresse, um eine Verbindung zum neuen Controller herzustellen.

Etikett	Komponente	Beschreibung
2	FRU-Teilenummer	Die FRU-Teilenummer. Diese Nummer muss der Teilenummer des derzeit installierten Controllers entsprechen.
3	4-Port-HIC	Die Host Interface Card (HIC) mit 4 Ports. Diese Karte muss auf den neuen Controller verschoben werden, wenn Sie den Austausch durchführen. Hinweis: Der E2800A Controller besitzt keine HIC.

Ste 2: Controller offline schalten

Bereiten Sie vor, den ausgefallenen Controller zu entfernen und in den Offline-Modus zu versetzen.

Schritte

1. Bereiten Sie das Entfernen des Controllers vor. Sie führen die folgenden Schritte mit SANtricity System Manager aus.

- a. Vergewissern Sie sich, dass die Ersatzteilnummer des ausgefallenen Controllers mit der FRU-Teilenummer für den Ersatz-Controller identisch ist.

Wenn ein Controller einen Fehler aufweist und ausgetauscht werden muss, wird im Bereich Details des Recovery Guru die Ersatzteilnummer angezeigt. Wenn Sie diese Nummer manuell finden müssen, können Sie auf der Registerkarte **Base** des Controllers nachsehen.



Möglicher Verlust des Datenzugriffs — Wenn die beiden Teilenummern nicht identisch sind, versuchen Sie nicht, dieses Verfahren durchzuführen.

- a. Sichern Sie die Konfigurationsdatenbank.

Wenn beim Entfernen eines Controllers ein Problem auftritt, können Sie die gespeicherte Datei verwenden, um Ihre Konfiguration wiederherzustellen.

- b. Sammeln von Support-Daten für die Appliance



Durch das Erfassen von Support-Daten vor und nach dem Ersetzen einer Komponente wird sichergestellt, dass Sie einen vollständigen Satz von Protokollen an den technischen Support senden können, wenn der Austausch das Problem nicht behebt.

- c. Nehmen Sie den Controller, den Sie ersetzen möchten, in den Offline-Modus.

2. Schaltet das Controller-Shelf aus.

Schritt 3: Entfernen Sie die Steuerung

Entfernen Sie den Controller aus dem Gerät.

Schritte

1. Setzen Sie ein ESD-Armband an oder ergreifen Sie andere antistatische Vorsichtsmaßnahmen.
2. Beschriften Sie die Kabel, und trennen Sie dann die Kabel und SFPs.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

- Lösen Sie die Steuerung vom Gerät, indem Sie die Verriegelung am Nockengriff so lange drücken, bis sie sich löst, und öffnen Sie dann den Nockengriff nach rechts.
- Schieben Sie den Regler mit zwei Händen und dem Nockengriff aus dem Gerät.



Verwenden Sie immer zwei Hände, um das Gewicht der Steuerung zu unterstützen.

- Stellen Sie den Controller auf eine flache, statische Oberfläche, wobei die abnehmbare Abdeckung nach oben zeigt.
- Entfernen Sie die Abdeckung, indem Sie die Taste nach unten drücken und die Abdeckung abnehmen.

Schritt 4: Batterie auf den neuen Controller bringen

Entfernen Sie den Akku aus dem fehlerhaften Controller, und setzen Sie ihn in den Ersatz-Controller ein.

Schritte

- Vergewissern Sie sich, dass die grüne LED im Controller (zwischen Akku und DIMMs) aus ist.

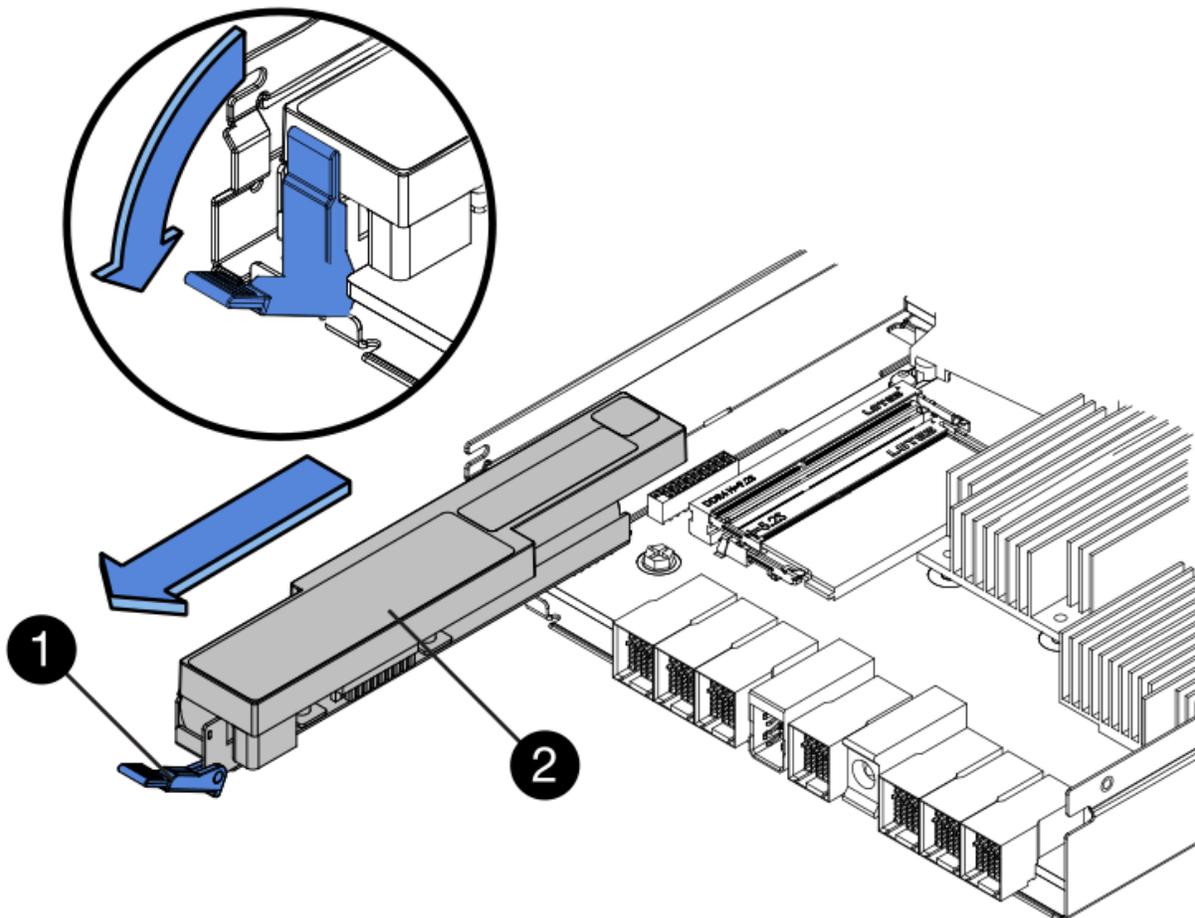
Wenn diese grüne LED leuchtet, wird der Controller weiterhin mit Strom versorgt. Sie müssen warten, bis diese LED erlischt, bevor Sie Komponenten entfernen.



Element	Beschreibung
1	Interne LED für aktiven Cache

Element	Beschreibung
2	Batterie

- Suchen Sie den blauen Freigabehebel für die Batterie.
- Entriegeln Sie den Akku, indem Sie den Entriegelungshebel nach unten und aus dem Controller entfernen.



Element	Beschreibung
1	Akkufreigaberiegel
2	Batterie

- Heben Sie den Akku an, und schieben Sie ihn aus dem Controller.
- Entfernen Sie die Abdeckung vom Ersatzcontroller.
- Richten Sie den Ersatz-Controller so aus, dass der Steckplatz für die Batterie zu Ihnen zeigt.
- Setzen Sie den Akku in einem leichten Abwärtswinkel in den Controller ein.

Sie müssen den Metallflansch an der Vorderseite der Batterie in den Schlitz an der Unterseite des Controllers einsetzen und die Oberseite der Batterie unter den kleinen Ausrichtstift auf der linken Seite des

Controllers schieben.

8. Schieben Sie die Akkuverriegelung nach oben, um die Batterie zu sichern.

Wenn die Verriegelung einrastet, Haken unten an der Verriegelung in einen Metallschlitz am Gehäuse.

9. Drehen Sie den Controller um, um zu bestätigen, dass der Akku korrekt installiert ist.



Mögliche Hardware-Schäden — der Metallflansch an der Vorderseite der Batterie muss vollständig in den Schlitz am Controller eingesetzt werden (wie in der ersten Abbildung dargestellt). Wenn die Batterie nicht richtig eingesetzt ist (wie in der zweiten Abbildung dargestellt), kann der Metallflansch die Controllerplatine kontaktieren, was zu Schäden führt.

◦ **Korrekt** — der Metallflansch der Batterie ist vollständig in den Schlitz am Controller eingesetzt:



◦ **Falsch** — der Metallflansch der Batterie ist nicht in den Steckplatz an der Steuerung eingefügt:



10. Bringen Sie die Controllerabdeckung wieder an.

Schritt 5: HIC bei Bedarf auf neuen Controller verschieben

Wenn der ausgefallene Controller eine Host Interface Card (HIC) enthält, verschieben Sie die HIC vom ausgefallenen Controller auf den Ersatz-Controller.

Eine separate HIC wird nur für den E2800B-Controller verwendet. Die HIC wird auf der Haupt-Controller-

Platine montiert und enthält zwei SPF-Anschlüsse.



Die Abbildungen in diesem Verfahren zeigen eine HIC mit 2 Ports. Die HIC in Ihrem Controller hat möglicherweise eine andere Anzahl von Ports.

E2800A

Ein E2800A-Controller verfügt nicht über eine HIC.

Die Abdeckung des E2800A-Controllers wieder anbringen und mit fortfahren [Schritt 6: Controller austauschen](#)

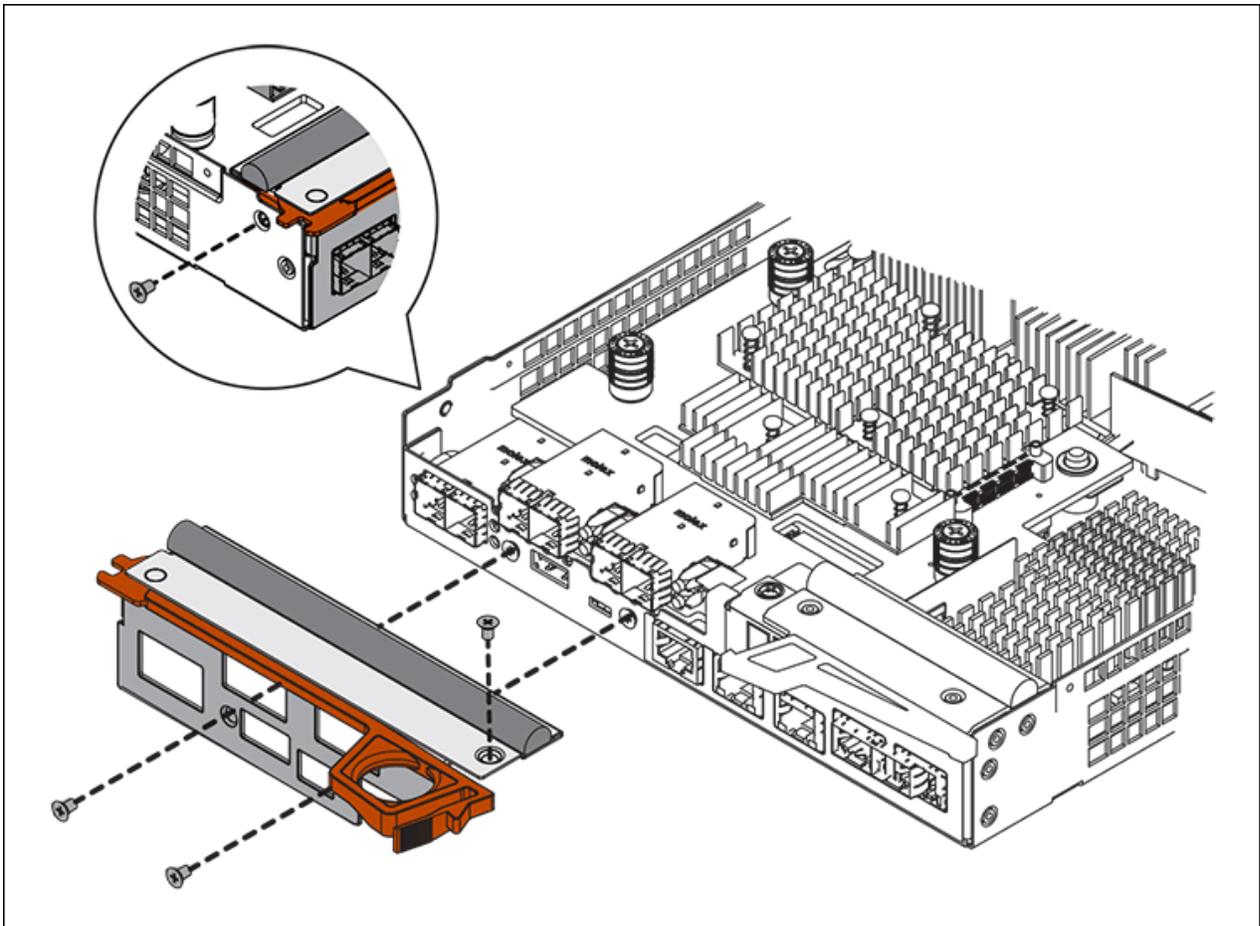
E2800B

Setzen Sie die HIC vom ausgefallenen E2800B-Controller auf den Ersatz-Controller.

Schritte

1. Entfernen Sie alle SFPs von der HIC.
2. Entfernen Sie mit einem #1 Kreuzschlitzschraubendreher die Schrauben, mit denen die HIC-Frontplatte am Controller befestigt ist.

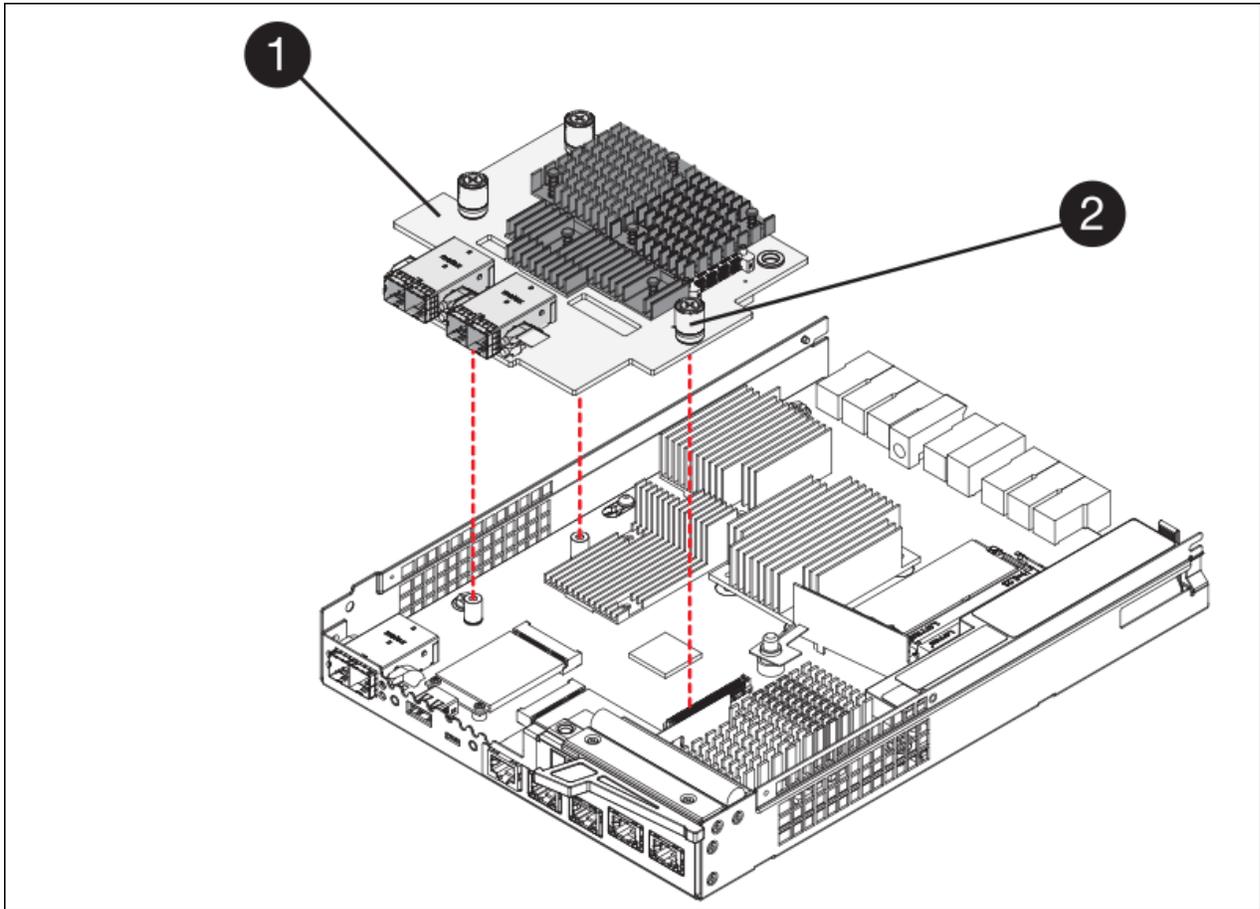
Es gibt vier Schrauben: Eine auf der Oberseite, eine auf der Seite und zwei auf der Vorderseite.



3. Entfernen Sie die HIC-Frontplatte.
4. Lösen Sie mit den Fingern oder einem Kreuzschlitzschraubendreher die drei Rändelschrauben, mit denen die HIC an der Controllerkarte befestigt ist.
5. Lösen Sie die HIC vorsichtig von der Controllerkarte, indem Sie die Karte nach oben heben und wieder zurückschieben.



Achten Sie darauf, dass die Komponenten auf der Unterseite der HIC oder auf der Oberseite der Controller-Karte nicht verkratzen oder stoßen.



Etikett	Beschreibung
1	Host-Schnittstellenkarte
2	Rändelschrauben

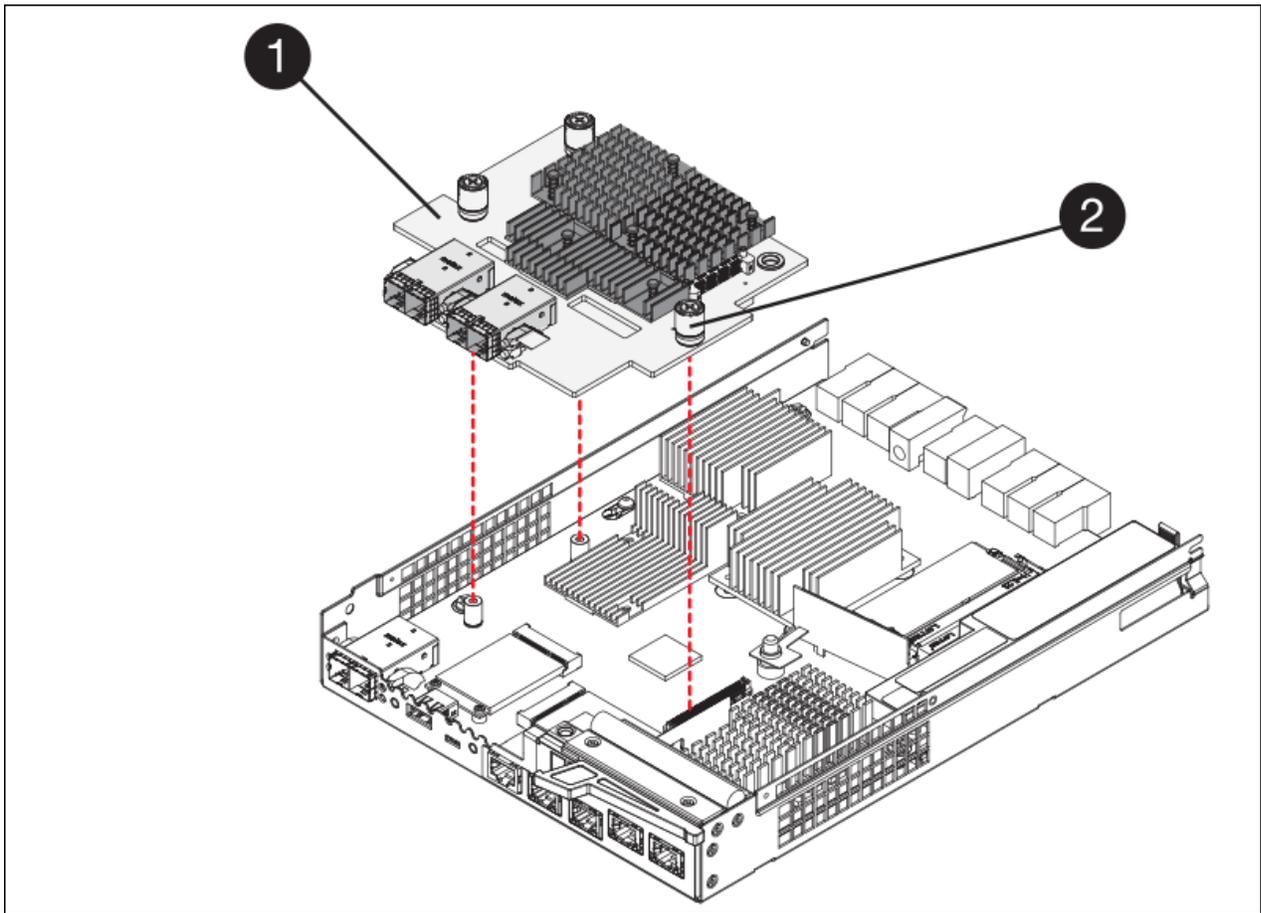
- Platzieren Sie die HIC auf einer statischen Oberfläche.
- Entfernen Sie mit einem #1 Kreuzschlitzschraubendreher die vier Schrauben, mit denen die leere Frontplatte an der Ersatzsteuerung befestigt ist, und entfernen Sie die Frontplatte.
- Richten Sie die drei Rändelschrauben der HIC an den entsprechenden Löchern am Ersatz-Controller aus, und richten Sie den Anschluss an der Unterseite der HIC an dem HIC-Schnittstellenanschluss auf der Controllerkarte aus.

Achten Sie darauf, dass die Komponenten auf der Unterseite der HIC oder auf der Oberseite der Controller-Karte nicht verkratzen oder stoßen.

- Senken Sie die HIC vorsichtig ab, und setzen Sie den HIC-Anschluss ein, indem Sie vorsichtig auf die HIC drücken.



Mögliche Geräteschäden — Vorsicht, den goldenen Bandanschluss für die Controller-LEDs nicht zwischen der HIC und den Rändelschrauben zu quetschen.

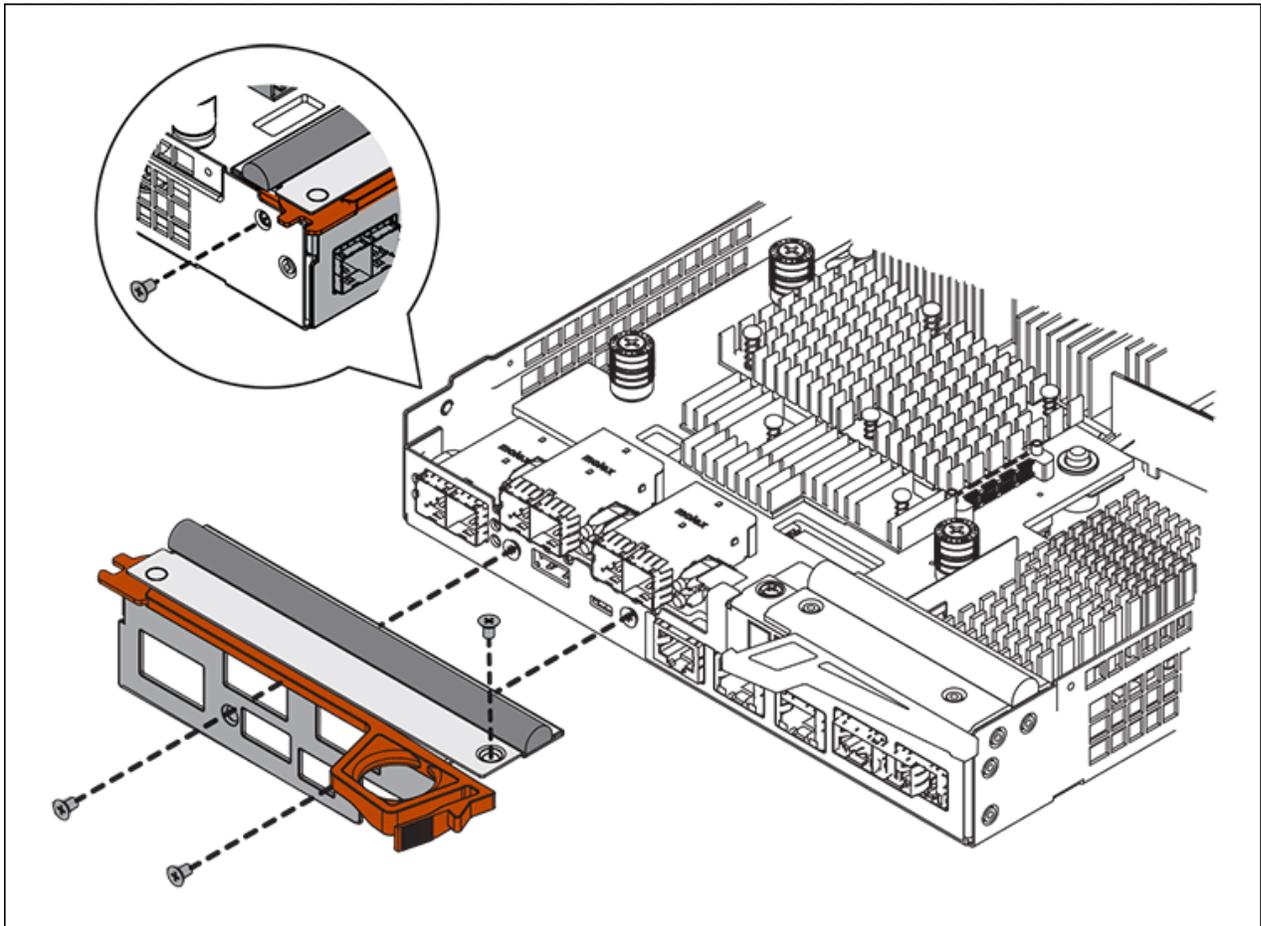


Etikett	Beschreibung
1	Host-Schnittstellenkarte
2	Rändelschrauben

10. Ziehen Sie die HIC-Rändelschrauben manuell fest.

Verwenden Sie keinen Schraubendreher, da Sie die Schrauben sonst möglicherweise zu fest anziehen.

11. Befestigen Sie mit einem #1 Kreuzschlitzschraubendreher die HIC-Frontplatte, die Sie vom ursprünglichen Controller entfernt haben, mit vier Schrauben an der neuen Steuerung.



12. Installieren Sie alle entfernten SFPs wieder auf der HIC.

Schritt 6: Controller austauschen

Installieren Sie den Ersatz-Controller und überprüfen Sie, ob er wieder an das Raster angeschlossen ist.

Schritte

1. Setzen Sie den Ersatzcontroller in das Gerät ein.
 - a. Drehen Sie den Controller um, so dass die abnehmbare Abdeckung nach unten zeigt.
 - b. Schieben Sie den Steuerknebel in die geöffnete Stellung, und schieben Sie ihn bis zum Gerät.
 - c. Bewegen Sie den Nockengriff nach links, um die Steuerung zu verriegeln.
 - d. Ersetzen Sie die Kabel und SFPs.
 - e. Schalten Sie das Controller-Shelf ein.
 - f. Wenn der ursprüngliche Controller DHCP für die IP-Adresse verwendet hat, suchen Sie die MAC-Adresse auf dem Etikett auf der Rückseite des Ersatzcontrollers. Bitten Sie den Netzwerkadministrator, die DNS/Netzwerk- und IP-Adresse des entfernten Controllers mit der MAC-Adresse des Ersatzcontrollers zu verknüpfen.



Wenn der ursprüngliche Controller DHCP für die IP-Adresse nicht verwendet hat, übernimmt der neue Controller die IP-Adresse des entfernten Controllers.

2. Stellen Sie den Controller mit SANtricity System Manager online:

- a. Wählen Sie **Hardware**.
 - b. Wenn die Grafik die Laufwerke anzeigt, wählen Sie **Zurück von Regal anzeigen**.
 - c. Wählen Sie den Controller aus, den Sie online platzieren möchten.
 - d. Wählen Sie im Kontextmenü * Online platzieren* aus, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.
 - e. Vergewissern Sie sich, dass auf der 7-Segment-Anzeige ein Status von angezeigt wird 99.
3. Vergewissern Sie sich, dass der neue Controller optimal ist, und sammeln Sie Support-Daten.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Verwandte Informationen

["NetApp E-Series Systems Documentation Site"](#)

Hardwarekomponenten in das Storage-Controller-Shelf austauschen

Wenn ein Hardwareproblem auftritt, müssen Sie möglicherweise eine Komponente im Storage-Controller-Shelf ersetzen.

Bevor Sie beginnen

- Sie haben das Verfahren zum Austausch der E-Series Hardware.
- Sie haben die Storage Appliance physisch gefunden, bei der die Storage Shelf-Hardwarekomponenten im Datacenter ausgetauscht werden.

["Controller im Datacenter finden"](#)

Über diese Aufgabe

Informationen zum Austauschen der Batterie im Speicher-Controller finden Sie in den Schritten in der Anleitung für "[Austauschen eines Speicher-Controllers](#)". Diese Anweisungen beschreiben, wie Sie einen Controller aus dem Gerät entfernen, den Akku aus dem Controller entfernen, den Akku einbauen und den Controller austauschen.

Anweisungen zu den anderen Field Replaceable Units (FRUs) in den Controller-Shelfs finden Sie in den Verfahren der E-Series zur Systemwartung.

FRU	Siehe Anweisungen
Batterie	StorageGRID (diese Anleitung): Ersetzen eines Storage-Controllers
Laufwerk	E-Series: <ul style="list-style-type: none"> • Laufwerk austauschen (60 Laufwerke) • Auswechseln des Laufwerks (12 Laufwerke oder 24 Laufwerke)
Leistungsbehälter	E-Series <ul style="list-style-type: none"> • Ersetzen Sie den Netzbehälter (60 Laufwerke). • Ersetzen Sie das Netzteil (12 oder 24 Laufwerke).

FRU	Siehe Anweisungen
Lüfterbehälter (nur Shelves mit 60 Laufwerken)	E-Series: Lüfterbehälter ersetzen (60 Laufwerke)
Laufwerkseinschub (nur Shelves mit 60 Laufwerken)	E-Series: Auswechseln der Laufwerkschublade (60 Laufwerke)

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Verwandte Informationen

["NetApp E-Series Systems Documentation Site"](#)

["Austausch des Storage Controllers"](#)

Ersetzen Sie Hardwarekomponenten in dem optionalen Erweiterungs-Shelf für 60 Laufwerke

Möglicherweise müssen Sie ein ein-/Ausgabemodul, ein Netzteil oder einen Lüfter im Erweiterungs-Shelf ersetzen.

Bevor Sie beginnen

- Sie haben das Verfahren zum Austausch der E-Series Hardware.
- Sie haben die Storage Appliance physisch gefunden, wo Sie im Datacenter Erweiterungs-Shelf-Hardware-Komponenten ersetzen.

["Controller im Datacenter finden"](#)

Über diese Aufgabe

Informationen zum Austauschen eines E/A-Moduls (IOM) in einem Erweiterungs-Shelf für 60 Laufwerke finden Sie in den Schritten in der Anleitung für ["Austauschen eines Speicher-Controllers"](#).

Um ein Netzteil oder einen Lüfter in einem Erweiterungs-Shelf mit 60 Laufwerken zu ersetzen, rufen Sie die E-Series Verfahren zur Wartung von Hardware mit 60 Laufwerken auf.

FRU	Weitere Informationen finden Sie in den Anweisungen zur E-Series
Eingangs-/Ausgangsmodul (IOM)	Ersetzen eines EAM
Leistungsbehälter	Ersetzen Sie den Netzbehälter (60 Laufwerke).
Gebälsebehälter	Lüfterbehälter austauschen (60 Laufwerke)

Tauschen Sie den SG6000-CN Controller aus

Möglicherweise müssen Sie den SG6000-CN-Controller austauschen, wenn er nicht optimal funktioniert oder ausgefallen ist.

Bevor Sie beginnen

- Sie verfügen über einen Ersatzcontroller mit derselben Teilenummer wie der zu ersetzenden Controller.
- Sie verfügen über Etiketten, um jedes Kabel, das mit dem Controller verbunden ist, zu identifizieren.
- Der Controller ist physisch zu finden, der im Datacenter ersetzt werden soll.

["Controller im Datacenter finden"](#)

Über diese Aufgabe

Der Gerätespeicherknoten kann nicht aufgerufen werden, wenn Sie den SG6000-CN-Controller austauschen. Wenn der SG6000-CN-Controller ausreichend funktioniert, können Sie zu Beginn dieses Verfahrens ein kontrolliertes Herunterfahren durchführen.



Wenn Sie den Controller vor dem Installieren der StorageGRID-Software ersetzen, können Sie nach Abschluss dieses Verfahrens möglicherweise nicht sofort auf den StorageGRID Appliance Installer zugreifen. Sie können zwar von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm der StorageGRID-Appliance zugreifen, können jedoch nicht von Hosts in anderen Subnetzen darauf zugreifen. Diese Bedingung sollte sich innerhalb von 15 Minuten lösen (wenn Einträge im ARP-Cache für die ursprüngliche Controller-Zeit erforderlich sind), oder Sie können den Zustand sofort löschen, indem Sie alle alten ARP-Cacheeinträge manuell vom lokalen Router oder Gateway löschen.

Schritte

1. Zeigt die aktuellen Konfigurationen des Geräts an und zeichnet sie auf.
 - a. Melden Sie sich bei der zu ersetzenden Appliance an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

- b. Geben Sie Ein: **run-host-command ipmitool lan print** Zeigt die aktuellen BMC-Konfigurationen für die Appliance an.
2. Wenn der SG6000-CN-Controller ausreichend funktioniert, um ein kontrolliertes Herunterfahren zu ermöglichen, fahren Sie den SG6000-CN-Controller herunter.

["Fahren Sie den SG6000-CN-Controller herunter"](#)

3. Wenn eine der Netzwerkschnittstellen auf dieser StorageGRID-Appliance für DHCP konfiguriert ist, müssen Sie möglicherweise die permanenten DHCP-Lease-Zuordnungen auf den DHCP-Servern aktualisieren, um auf die MAC-Adressen der Ersatz-Appliance zu verweisen. Das Update stellt sicher, dass der Appliance die erwarteten IP-Adressen zugewiesen werden. Siehe ["Aktualisieren Sie die MAC-Adressenverweise"](#).
4. Entfernen und ersetzen Sie den SG6000-CN-Controller:
 - a. Beschriften Sie die Kabel und trennen Sie dann die Kabel und alle SFP+ oder SFP28 Transceiver.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

- b. Entfernen Sie den fehlerhaften Controller aus dem Schrank oder Rack.
 - c. Setzen Sie den Ersatzcontroller in den Schrank oder Rack ein.
 - d. Ersetzen Sie die Kabel und alle SFP+ oder SFP28 Transceiver.
 - e. Schalten Sie den Controller ein, und überwachen Sie die Controller-LEDs und die Boot-Codes.
5. Wenn die Appliance, bei der Sie den Controller ausgetauscht haben, zur Verschlüsselung von Daten einen Schlüsselverwaltungsserver (KMS) verwendet hat, ist möglicherweise eine zusätzliche Konfiguration erforderlich, bevor der Node dem Grid beitreten kann. Wenn der Node nicht automatisch dem Grid hinzugefügt wird, stellen Sie sicher, dass die folgenden Konfigurationseinstellungen auf den neuen Controller übertragen wurden, und konfigurieren Sie manuell alle Einstellungen, für die nicht die erwartete Konfiguration vorhanden ist:
- ["Netzwerkverbindungen konfigurieren"](#)
 - ["Konfigurieren Sie StorageGRID-IP-Adressen"](#)
 - ["Konfigurieren Sie die Node-Verschlüsselung für die Appliance"](#)
6. Melden Sie sich bei der Appliance mit dem ausgetauschten Controller an:
- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
7. Stellen Sie die BMC-Netzwerkverbindung für die Appliance wieder her. Es gibt zwei Möglichkeiten:
- Verwenden Sie statische IP, Netzmaske und Gateway
 - Verwenden Sie DHCP, um eine IP, eine Netzmaske und ein Gateway zu erhalten
- i. Geben Sie zum Wiederherstellen der BMC-Konfiguration für die Verwendung einer statischen IP, Netzmaske und eines Gateways die folgenden Befehle ein:

```
run-host-command ipmitool lan set 1 ipsrc static
```



```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP
```



```
run-host-command ipmitool lan set 1 netmask Netmask_IP
```



```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```
- i. Geben Sie den folgenden Befehl ein, um die BMC-Konfiguration so wiederherzustellen, dass DHCP zum Abrufen einer IP, einer Netmask und eines Gateways verwendet wird:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```
8. Stellen Sie nach dem Wiederherstellen der BMC-Netzwerkverbindung eine Verbindung zur BMC-Schnittstelle her, um die zusätzlich angewendete benutzerdefinierte BMC-Konfiguration zu prüfen und wiederherzustellen. Sie sollten beispielsweise die Einstellungen für SNMP-Trap-Ziele und E-Mail-Benachrichtigungen bestätigen. Siehe ["Konfigurieren Sie die BMC-Schnittstelle"](#).

9. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Verwandte Informationen

["Installieren Sie SG6000-CN im Schrank oder Rack"](#)

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

["Anzeigen von Boot-Codes für SG6000-CN-Controller"](#)

Tauschen Sie ein oder beide Netzteile im SG6000-CN Controller aus

Der SG6000-CN Controller verfügt über zwei Netzteile für Redundanz. Wenn eines der Netzteile ausfällt, müssen Sie es so schnell wie möglich ersetzen, um sicherzustellen, dass der Compute-Controller über redundante Stromversorgung verfügt. Beide im Controller ausgeführten Netzteile müssen das gleiche Modell und die gleiche Stromleistung aufweisen.

Bevor Sie beginnen

- Sie haben den physischen Standort im Datacenter des Controllers ermittelt und das zu ersetzende Netzteil verwendet.

["Lokalisierung des Controllers in einem Rechenzentrum"](#)

- Wenn Sie nur ein Netzteil ersetzen:
 - Sie haben das Ersatznetzteil entpackt und sichergestellt, dass es das gleiche Modell und die gleiche Stromleistung wie das Netzteil ist, das Sie ersetzen.
 - Sie haben bestätigt, dass das andere Netzteil installiert ist und in Betrieb ist.
- Wenn Sie beide Netzteile gleichzeitig ersetzen:
 - Sie haben die Ersatz-Netzteile entpackt und sichergestellt, dass sie das gleiche Modell und die gleiche Wattzahl haben.

Über diese Aufgabe

Die Abbildung zeigt die beiden Netzteile des SG6000-CN Controllers, auf die über die Rückseite des Controllers zugegriffen werden kann. Gehen Sie folgendermaßen vor, um ein oder beide Netzteile zu ersetzen. Wenn Sie beide Netzteile austauschen, müssen Sie zunächst ein kontrolliertes Herunterfahren des Geräts durchführen.

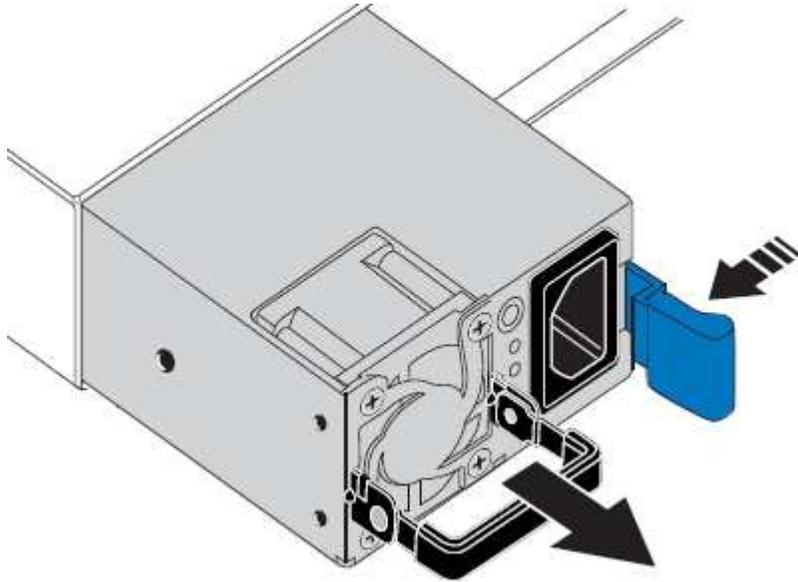


Schritte

1. Wenn Sie nur ein Netzteil ersetzen, müssen Sie das Gerät nicht herunterfahren. Wechseln Sie zum [Ziehen Sie das Netzkabel ab](#) Schritt: Wenn Sie beide Netzteile gleichzeitig ersetzen, gehen Sie folgendermaßen vor, bevor Sie die Netzkabel abziehen:

a. "Schalten Sie das Gerät aus".

2. [[Trenne den Netzstecker_Power_cordel, Start=2]] Trennen Sie das Netzkabel von jedem zu ersetzenden Netzteil.
3. Den Nockengriff an der ersten zu ersetzenden Versorgung anheben.
4. Drücken Sie auf den blauen Riegel, und ziehen Sie das Netzteil heraus.

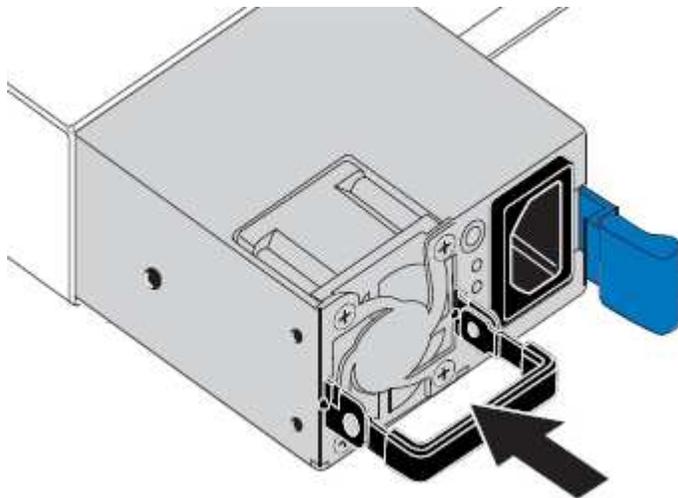


5. Schieben Sie das Ersatznetzteil mit der blauen Verriegelung nach rechts in das Gehäuse.



Beide Netzteile müssen das gleiche Modell und die gleiche Wattzahl haben.

Stellen Sie sicher, dass sich die blaue Verriegelung auf der rechten Seite befindet, wenn Sie die Ersatzeinheit einschieben.



6. Drücken Sie den Nockengriff nach unten, um die Ersatzstromversorgung zu sichern.
7. Wenn Sie beide Netzteile austauschen, wiederholen Sie die Schritte 2 bis 6, um das zweite Netzteil auszutauschen.
8. "Schließen Sie die Stromkabel an die ersetzten Geräte an, und wenden Sie Strom an".

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Controller im Rack austauschen

Entfernen Sie den SG6000-CN Controller aus dem Schrank oder Rack

Entfernen Sie den SG6000-CN-Controller aus einem Schrank oder Rack, um auf die obere Abdeckung zuzugreifen oder um den Controller an einen anderen Ort zu bewegen.

Bevor Sie beginnen

- Sie verfügen über Etiketten, um jedes Kabel zu identifizieren, das mit dem SG6000-CN-Controller verbunden ist.
- Der SG6000-CN-Controller ist in einem physischen Standort untergebracht, an dem Wartungsarbeiten im Datacenter durchgeführt werden.

["Controller im Datacenter finden"](#)

- Sie haben den SG6000-CN-Controller heruntergefahren.

["Fahren Sie den SG6000-CN-Controller herunter"](#)



Fahren Sie den Controller nicht mit dem Netzschalter herunter.

Schritte

1. Kennzeichnen und trennen Sie die Controller-Stromkabel.
2. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
3. Beschriften und trennen Sie dann die Controller-Datenkabel und alle SFP+ oder SFP28-Transceiver.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

4. Lösen Sie die beiden unverlierbaren Schrauben an der Vorderseite des Controllers.



5. Schieben Sie den SG6000-CN-Controller nach vorn aus dem Rack, bis die Befestigungsschienen vollständig ausgefahren sind, und hören Sie, dass die Verriegelungen auf beiden Seiten einrasten.

Die obere Abdeckung des Controllers ist zugänglich.

6. Optional: Wenn Sie den Controller vollständig aus dem Schrank oder Rack entfernen, befolgen Sie die Anweisungen für den Schienensatz, um den Controller aus den Schienen zu entfernen.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Verwandte Informationen

"Entfernen Sie die SG6000-CN Controller-Abdeckung"

Installieren Sie den SG6000-CN Controller wieder in den Schrank oder Rack

Setzen Sie den Controller nach Abschluss der Hardwarewartung in ein Rack oder Rack ein.

Bevor Sie beginnen

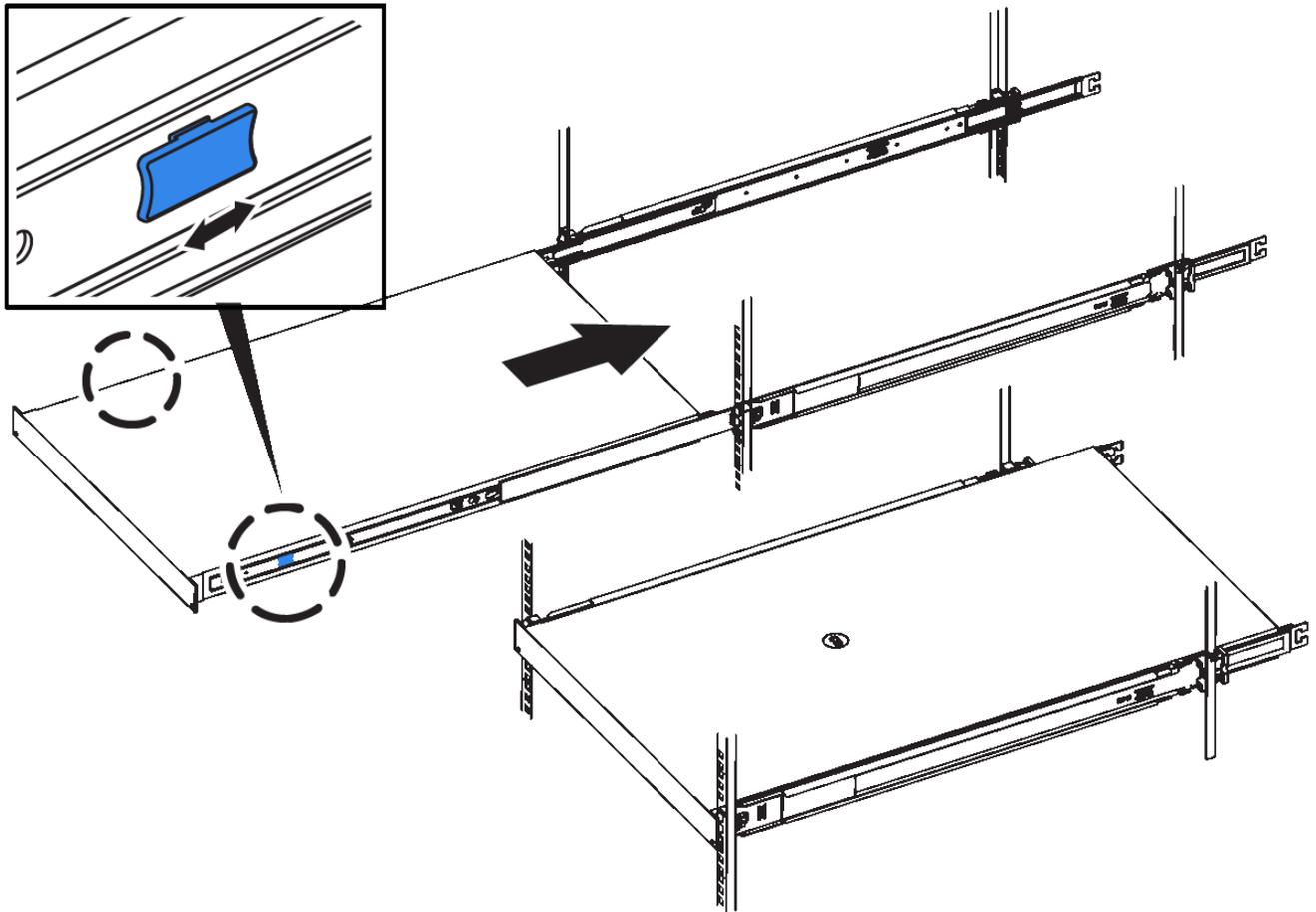
Sie haben die Controller-Abdeckung wieder installiert.

"Bringen Sie die SG6000-CN Controller-Abdeckung wieder an"

Schritte

1. Durch Drücken der blauen Schiene werden beide Rack-Schienen gleichzeitig freigegeben, und der SG6000-CN Controller in das Rack schieben, bis er vollständig eingesetzt ist.

Wenn Sie den Controller nicht weiter bewegen können, ziehen Sie die blauen Laschen auf beiden Seiten des Chassis, um den Controller vollständig einzuschieben.



Bringen Sie die Frontverkleidung erst an, nachdem Sie den Controller eingeschaltet haben.

2. Ziehen Sie die unverlierbaren Schrauben an der Vorderseite des Controllers fest, um den Controller im Rack zu befestigen.



3. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
4. Schließen Sie die Controller-Datenkabel und alle SFP+- oder SFP28-Transceiver wieder an.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

"Kabelgerät (SG6000)"

5. Schließen Sie die Controller-Stromkabel wieder an.

"Anschließen des Netzes und Anwenden der Stromversorgung (SG6000)"

Nachdem Sie fertig sind

Der Controller kann neu gestartet werden.

"Schalten Sie den SG6000-CN Controller ein, und überprüfen Sie den Betrieb"

Bringen Sie die Controllerabdeckung wieder an

Entfernen Sie die SG6000-CN Controller-Abdeckung

Entfernen Sie die Controllerabdeckung, um zu Wartungszwecken auf interne Komponenten zuzugreifen.

Bevor Sie beginnen

Entfernen Sie den Controller aus dem Schrank oder Rack, um auf die obere Abdeckung zuzugreifen.

"Entfernen Sie den SG6000-CN Controller aus dem Schrank oder Rack"

Schritte

1. Stellen Sie sicher, dass die Verriegelung der SG6000-CN-Controllerabdeckung nicht verriegelt ist. Falls erforderlich, drehen Sie die blaue Kunststoffverriegelung um eine Vierteldrehung in die Entsperrungsrichtung, wie auf der Verriegelung gezeigt.
2. Drehen Sie den Riegel nach oben und zurück zur Rückseite des SG6000-CN Controller-Chassis, bis er anhält. Heben Sie dann die Abdeckung vorsichtig vom Chassis an, und legen Sie sie beiseite.



Wickeln Sie das Riemen eines ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern, wenn Sie im SG6000-CN-Controller arbeiten.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Verwandte Informationen

["Entfernen Sie den Fibre Channel HBA"](#)

Bringen Sie die SG6000-CN Controller-Abdeckung wieder an

Setzen Sie die Controllerabdeckung wieder ein, wenn die interne Hardwarewartung abgeschlossen ist.

Bevor Sie beginnen

Sie haben alle Wartungsarbeiten im Controller abgeschlossen.

Schritte

1. Halten Sie bei geöffneter Abdeckungsverriegelung die Abdeckung über dem Gehäuse und richten Sie die Öffnung in der oberen Abdeckung an dem Stift im Gehäuse aus. Wenn die Abdeckung ausgerichtet ist, senken Sie sie auf das Gehäuse ab.



2. Drehen Sie die Verriegelung nach vorne und unten, bis sie anhält und die Abdeckung vollständig im Gehäuse sitzt. Stellen Sie sicher, dass an der Vorderkante der Abdeckung keine Lücken vorhanden sind.

Wenn die Abdeckung nicht vollständig eingesetzt ist, können Sie den SG6000-CN-Controller möglicherweise nicht in das Rack schieben.

3. Optional: Drehen Sie die blaue Kunststoffverriegelung um eine Vierteldrehung in die Schlossrichtung, wie auf der Verriegelung gezeigt, um sie zu verriegeln.

Nachdem Sie fertig sind

Setzen Sie den Controller wieder in den Schrank oder Rack ein.

["Installieren Sie den SG6000-CN Controller wieder in den Schrank oder Rack"](#)

Tauschen Sie den Fibre-Channel-HBA in den SG6000-CN-Controller aus

Überprüfen Sie, ob der Fibre-Channel-HBA ersetzt werden soll

Wenn Sie sich nicht sicher sind, welcher Fibre Channel-Host Bus Adapter (HBA) ersetzt werden soll, führen Sie dieses Verfahren aus, um ihn zu identifizieren.

Bevor Sie beginnen

- Sie haben die Seriennummer der Speicher-Appliance oder SG6000-CN-Controller, wo der Fibre Channel HBA ersetzt werden muss.



Wenn die Seriennummer der Speicheranwendung, die den Fibre-Channel-HBA enthält, den Sie ersetzen, mit dem Buchstaben Q beginnt, wird sie nicht im Grid Manager aufgeführt. Sie müssen die an der Vorderseite der einzelnen SG6000-CN-Controller im Rechenzentrum angebrachten Tags überprüfen, bis Sie eine Übereinstimmung finden.

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).

Schritte

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie in der Tabelle auf der Seite Knoten einen Appliance Storage Node aus.
3. Wählen Sie die Registerkarte **Hardware** aus.

Überprüfen Sie im Abschnitt StorageGRID-Gerät die Seriennummer * des Chassis für die Speichergeräte* und die Seriennummer für den Rechencontroller*. Finden Sie heraus, ob eine dieser Seriennummern der

Storage Appliance entspricht, an der Sie den Fibre Channel HBA ersetzen. Wenn eine der Seriennummern übereinstimmt, haben Sie die richtige Appliance gefunden.

StorageGRID Appliance

Appliance model: ?	SG5660	
Storage controller name: ?	StorageGRID-SGA-Lab11	
Storage controller A management IP: ?	10.224.2.192	
Storage controller WWID: ?	600a098000a4a707000000005e8ed5fd	
Storage appliance chassis serial number: ?	1142FG000135	
Storage controller firmware version: ?	08.40.60.01	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	2.00 TB	
Storage RAID mode: ?	RAID6	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller serial number: ?	SV54365519	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	

Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?
SN SV13304553	0	Nominal	N/A

- Wenn der Abschnitt StorageGRID-Appliance nicht angezeigt wird, ist der ausgewählte Node keine StorageGRID-Appliance. Wählen Sie einen anderen Knoten in der Strukturansicht aus.
- Wenn das Appliance-Modell nicht SG6060 oder SG6060X ist, wählen Sie einen anderen Node aus der Baumstruktur aus.
- Wenn die Seriennummern nicht übereinstimmen, wählen Sie einen anderen Knoten aus der Strukturansicht aus.

4. Nachdem Sie den Node gefunden haben, an dem der Fibre Channel HBA ausgetauscht werden muss, notieren Sie die BMC IP-Adresse des Computing-Controllers im Abschnitt „StorageGRID Appliance“.

Sie können diese IP-Adresse verwenden, um die LED für die Identifikation des Computing-Controllers einzuschalten, um Ihnen bei der Suche nach der Appliance im Datacenter zu helfen.

["Schalten Sie die Controller-ID-LED ein und aus"](#)

Verwandte Informationen

["Entfernen Sie den Fibre Channel HBA"](#)

Entfernen Sie den Fibre Channel HBA

Möglicherweise müssen Sie den Fibre-Channel-Hostbus-Adapter (HBA) im SG6000-CN-Controller ersetzen, wenn dieser nicht optimal funktioniert oder wenn er ausgefallen ist.

Bevor Sie beginnen

- Sie haben den richtigen Fibre Channel HBA für den Austausch.
- Das ist schon ["Festgestellt, welcher SG6000-CN-Controller den zu ersetzenden Fibre-Channel-HBA enthält"](#).
- Das ist schon ["Physikalischer Standort des SG6000-CN-Controllers"](#) Im Datacenter zu ermöglichen.
- Das ist schon ["Fahren Sie den SG6000-CN-Controller herunter"](#).



Vor dem Entfernen des Controllers aus dem Rack ist ein kontrolliertes Herunterfahren erforderlich.

- Das ist schon ["Controller aus Schrank oder Rack entfernt"](#).
- Das ist schon ["Die Controllerabdeckung entfernt"](#).

Über diese Aufgabe

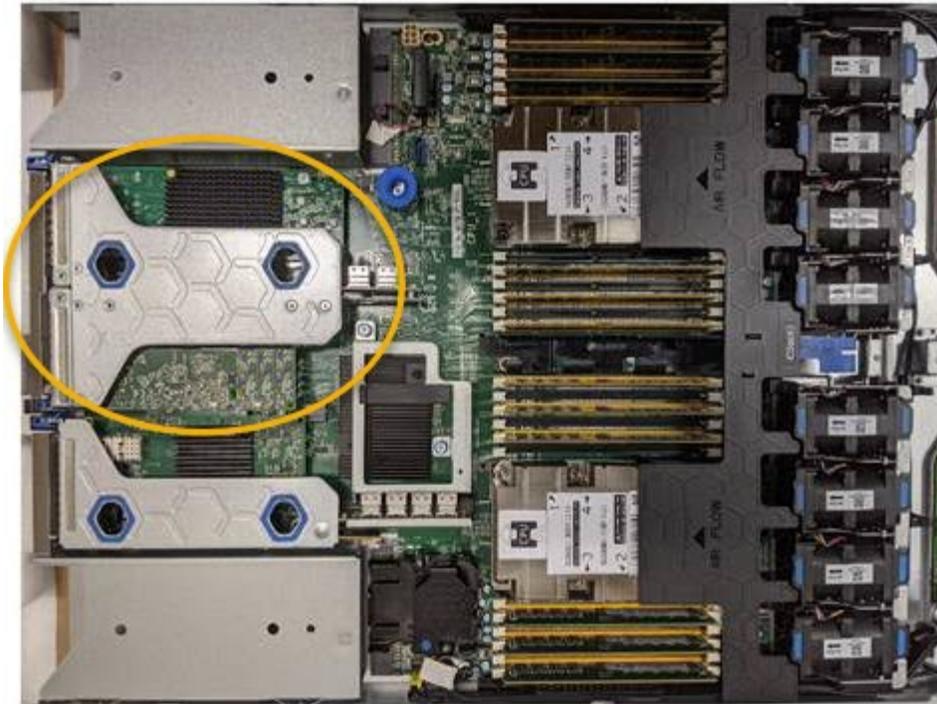
Um Serviceunterbrechungen zu vermeiden, vergewissern Sie sich, dass alle anderen Storage-Nodes mit dem Grid verbunden sind, bevor Sie den Austausch des Fibre Channel-HBA starten oder den Adapter während eines geplanten Wartungsfensters austauschen, wenn die Zeiten der Serviceunterbrechung normalerweise zu erwarten sind. Weitere Informationen finden Sie unter ["Monitoring der Verbindungsstatus der Nodes"](#).



Wenn Sie jemals eine ILM-Regel verwendet haben, die nur eine Kopie eines Objekts erstellt, müssen Sie den Fibre Channel HBA während eines geplanten Wartungsfensters ersetzen. Andernfalls verlieren Sie während dieses Verfahrens vorübergehend den Zugriff auf diese Objekte. + Siehe Informationen über ["Warum sollten Sie die Single-Copy-Replizierung nicht verwenden"](#).

Schritte

1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Suchen Sie die Riserbaugruppe auf der Rückseite des Controllers, der den Fibre Channel HBA enthält.



3. Fassen Sie die Riserbaugruppe durch die blau markierten Löcher und heben Sie sie vorsichtig nach oben. Bewegen Sie die Riser-Baugruppe zur Vorderseite des Gehäuses, während Sie sie anheben, damit die externen Anschlüsse der installierten Adapter das Gehäuse löschen können.
4. Legen Sie die Riser-Karte auf eine flache antistatische Oberfläche, wobei der Metallrahmen nach unten zeigt, um auf die Adapter zuzugreifen.



In der Riserbaugruppe befinden sich zwei Adapter: Ein Fibre-Channel-HBA und ein Ethernet-Netzwerkadapter. Der Fibre Channel HBA wird in der Abbildung angezeigt.

5. Öffnen Sie die blaue Adapterverriegelung (eingekreist), und entfernen Sie den Fibre Channel HBA vorsichtig aus der Riserbaugruppe. Den Adapter leicht einrocken, um ihn aus dem Anschluss zu entfernen. Verwenden Sie keine übermäßige Kraft.
6. Setzen Sie den Adapter auf eine flache antistatische Oberfläche.

Nachdem Sie fertig sind

"Installieren Sie den Ersatz-Fibre-Channel-HBA".

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit

gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Installieren Sie den Fibre Channel HBA neu

Der Ersatz-Fibre Channel HBA wird an demselben Standort installiert wie der zuvor entfernte.

Bevor Sie beginnen

- Sie haben den richtigen Fibre Channel HBA für den Austausch.
- Sie haben den vorhandenen Fibre Channel HBA entfernt.

["Entfernen Sie den Fibre Channel HBA"](#)

Schritte

1. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
2. Entfernen Sie den Ersatz-Fibre-Channel-HBA aus der Verpackung.
3. Richten Sie den Fibre Channel-HBA mit seinem Anschluss an der Riserbaugruppe aus, und drücken Sie dann vorsichtig den Adapter in den Anschluss, bis er vollständig sitzt.



In der Riserbaugruppe befinden sich zwei Adapter: Ein Fibre-Channel-HBA und ein Ethernet-Netzwerkadapter. Der Fibre Channel HBA wird in der Abbildung angezeigt.

4. Suchen Sie die Ausrichtbohrung an der Riserbaugruppe (eingekreist), die mit einem Führungsstift auf der Systemplatine ausgerichtet ist, um die korrekte Positionierung der Riserbaugruppe zu gewährleisten.



5. Positionieren Sie die Riserbaugruppe im Gehäuse, und stellen Sie sicher, dass sie am Anschluss und Führungsstift auf der Systemplatine ausgerichtet ist. Setzen Sie dann die Riserbaugruppe ein.
6. Drücken Sie die Riserbaugruppe vorsichtig entlang der Mittellinie neben den blau markierten Löchern, bis sie vollständig sitzt.
7. Entfernen Sie die Schutzkappen von den Fibre Channel HBA-Ports, an denen Sie die Kabel neu installieren.

Nachdem Sie fertig sind

Wenn Sie keine weiteren Wartungsvorgänge im Controller ausführen müssen, setzen Sie die Controllerabdeckung wieder ein.

["Bringen Sie die SG6000-CN Controller-Abdeckung wieder an"](#)

Instandhaltung der SG5700 Hardware

SG5700 Appliance warten

Möglicherweise müssen Sie auf dem E2800 Controller die SANtricity OS Software aktualisieren, die Ethernet-Link-Konfiguration des E5700SG Controllers ändern, den E2800 Controller oder den E5700SG Controller austauschen oder bestimmte Komponenten ersetzen. Bei den in diesem Abschnitt beschriebenen Verfahren wird davon ausgegangen, dass die Appliance bereits als Storage-Node in einem StorageGRID-System bereitgestellt wurde.

In diesem Abschnitt werden spezifische Verfahren zur Wartung Ihrer SG5700 Appliance beschrieben.

Siehe ["Allgemeine Verfahren"](#) Für Wartungsverfahren, die von allen Geräten verwendet werden.

Siehe ["Richten Sie die Hardware ein"](#) Für Wartungsverfahren, die auch während der Erstinstallation und -Konfiguration der Appliance durchgeführt werden.

Verfahren zur Wartungskonfiguration

Upgrade von SANtricity OS auf Storage Controller

Um die optimale Funktion des Storage Controllers sicherzustellen, müssen Sie auf die neueste Wartungsversion des SANtricity-Betriebssystems aktualisieren, das für Ihre StorageGRID Appliance geeignet ist.

Konsultieren Sie die ["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#) Um zu bestimmen, welche Version Sie verwenden sollen.

Laden Sie die neue Datei für die SANtricity OS Software von herunter ["NetApp Downloads mit StorageGRID Appliance"](#).

Verwenden Sie eines der folgenden Verfahren, das auf der derzeit installierten Version von SANtricity OS basiert:

- Wenn der Storage-Controller SANtricity OS 08.42.20.00 (11.42) oder eine neuere Version verwendet, führen Sie das Upgrade mit dem Grid Manager durch.

"Aktualisieren Sie SANtricity OS auf Storage-Controllern mit Grid Manager"

- Wenn der Storage-Controller eine SANtricity OS-Version verwendet, die älter als 08.42.20.00 ist (11.42), führen Sie das Upgrade im Wartungsmodus durch.

"Aktualisieren Sie SANtricity OS auf einem E2800 Controller mithilfe des Wartungsmodus"

Aktualisieren Sie SANtricity OS auf Storage-Controllern mit Grid Manager

Bei Storage-Controllern, die derzeit SANtricity OS 08.42.20.00 (11.42) oder eine neuere Version verwenden, müssen Sie zum Anwenden eines Upgrades den Grid-Manager verwenden.

Bevor Sie beginnen

- Sie haben den konsultiert ["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#) Um sicherzustellen, dass die für das Upgrade verwendete SANtricity OS-Version mit Ihrer Appliance kompatibel ist.
- Sie haben die ["Berechtigung für Wartung oder Root-Zugriff"](#).
- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Provisionierungs-Passphrase.
- Sie haben Zugriff auf ["NetApp Downloads mit StorageGRID Appliance"](#).

Über diese Aufgabe

Andere Software-Updates (StorageGRID Software-Upgrade oder Hotfix) können erst nach Abschluss des SANtricity OS Upgrades durchgeführt werden. Wenn Sie versuchen, vor Abschluss des SANtricity OS-Upgrades einen Hotfix oder ein StorageGRID-Software-Upgrade zu starten, werden Sie zur Upgrade-Seite von SANtricity OS umgeleitet.

Das Verfahren ist erst abgeschlossen, wenn das SANtricity OS Upgrade erfolgreich auf alle zutreffenden Nodes angewendet wurde, die für das Upgrade ausgewählt wurden. Das SANtricity Betriebssystem kann länger als 30 Minuten dauern, bis das Betriebssystem auf jedem Node (sequenziell) und bis zu 90 Minuten zum Neustart jeder StorageGRID Storage Appliance benötigt wird. Alle Nodes in Ihrem Grid, die SANtricity OS nicht verwenden, sind von diesem Verfahren nicht betroffen.



Die folgenden Schritte sind nur anwendbar, wenn Sie den Grid Manager zur Durchführung des Upgrades verwenden. Die Storage Controller in der Appliance können nicht mit dem Grid-Manager aktualisiert werden, wenn die Controller SANtricity OS verwenden, die älter als 08.42.20.00 (11.42) sind.



Mit diesem Verfahren wird der NVSRAM automatisch auf die neueste Version aktualisiert, die mit dem Upgrade des SANtricity-Betriebssystems verknüpft ist. Sie müssen keine separate NVSRAM-Aktualisierungsdatei anwenden.



Stellen Sie sicher, dass Sie den aktuellen StorageGRID-Hotfix installieren, bevor Sie mit diesem Vorgang beginnen. Siehe ["StorageGRID Hotfix Verfahren"](#) Entsprechende Details.

Schritte

1. Laden Sie die neue SANtricity OS Softwaredatei von herunter ["NetApp Downloads mit StorageGRID Appliance"](#).

Achten Sie darauf, die SANtricity Betriebssystemversion für Ihre Storage Controller auszuwählen.

2. Wählen Sie **WARTUNG > System > Software-Update**.

Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade	StorageGRID hotfix	SANtricity OS update
Upgrade to the next StorageGRID version and apply the latest hotfix for that version.	Apply a hotfix to your current StorageGRID software version.	Update the SANtricity OS software on your StorageGRID storage appliances.
Upgrade →	Apply hotfix →	Update →

3. Wählen Sie im Abschnitt SANtricity OS Update die Option **Update** aus.

Die Seite SANtricity OS Upgrade wird angezeigt und enthält die Details zu den einzelnen Appliance-Nodes, einschließlich:

- Node-Name
- Standort
- Appliance-Modell
- Version des SANtricity Betriebssystems
- Status
- Status des letzten Upgrades

4. Lesen Sie die Informationen in der Tabelle für alle Upgrade-fähigen Geräte. Vergewissern Sie sich, dass alle Speicher-Controller den Status **nominal** haben. Wenn der Status eines Controllers **Unbekannt** lautet, gehen Sie zu **Nodes > Appliance Node > Hardware**, um das Problem zu untersuchen und zu beheben.

5. Wählen Sie die Upgrade-Datei für das SANtricity Betriebssystem aus, die Sie von der NetApp Support-Website heruntergeladen haben.

- Wählen Sie **Durchsuchen**.
- Suchen und wählen Sie die Datei aus.
- Wählen Sie **Offen**.

Die Datei wird hochgeladen und validiert. Wenn der Validierungsprozess abgeschlossen ist, wird der Dateiname mit einem grünen Häkchen neben der Schaltfläche **Browse** angezeigt. Ändern Sie den Dateinamen nicht, da er Teil des Überprüfungsprozesses ist.

6. Geben Sie die Provisionierungs-Passphrase ein und wählen Sie **Weiter**.

Ein Warnfeld zeigt an, dass die Verbindung Ihres Browsers vorübergehend unterbrochen wird, da Dienste auf Knoten, die aktualisiert werden, neu gestartet werden.

7. Wählen Sie **Ja**, um die SANtricity OS-Upgrade-Datei auf den primären Admin-Knoten zu übertragen.

Wenn das SANtricity OS Upgrade startet:

- a. Die Integritätsprüfung wird ausgeführt. Dieser Prozess überprüft, dass für keine Nodes der Status „Aufmerksamkeit erforderlich“ angezeigt wird.



Wenn Fehler gemeldet werden, beheben Sie sie, und wählen Sie erneut **Start**.

- b. Die Fortschrittstabelle für das SANtricity OS-Upgrade wird angezeigt. In dieser Tabelle werden alle Storage-Nodes in Ihrem Raster und die aktuelle Phase des Upgrades für jeden Node angezeigt.



In der Tabelle sind alle Appliance Storage-Nodes aufgeführt. Softwarebasierte Storage-Nodes werden nicht angezeigt. Wählen Sie für alle Nodes, die das Upgrade erfordern * genehmigen.

SANtricity OS

Upload files — 2 Upgrade

Approved nodes are added to a queue and upgraded sequentially. Each node can take up to 30 minutes, which includes updating NVSRAM. When the upgrade is complete, the node is rebooted.

Select **Approve all** or approve nodes one at a time. To remove nodes from the queue, select **Remove all** or remove nodes one at a time. If the uploaded file doesn't apply to an approved node, the upgrade process skips that node and moves to the next node in the queue.

Optionally, select **Skip nodes and finish** to end the upgrade and skip any unapproved nodes.

SANtricity OS upgrade file: RCB_11.70.3_280x_6283a64d.dlp

0 out of 3 completed

[Approve all](#) [Remove all](#)

Node name	Current version	Progress	Stage	Details	Status	Actions
10-224-2-24-S1	08.40.60.01	<div style="width: 100%;"></div>	Waiting for you to approve		Nominal	Approve
lab-37-sgws- quanta-10	08.73.00.00	<div style="width: 100%;"></div>	Waiting for you to approve		Nominal	Approve
storage-7	98.72.09.00	<div style="width: 100%;"></div>	Waiting for you to approve		Nominal	Approve

[Skip nodes and finish](#)

8. Sortieren Sie die Liste der Knoten wahlweise in aufsteigender oder absteigender Reihenfolge nach:

- Node-Name
- Aktuelle Version
- Fortschritt
- Stufe

- Status

Sie können auch einen Begriff in das Suchfeld eingeben, um nach bestimmten Knoten zu suchen.

9. Genehmigen Sie die Grid-Knoten, die Sie zur Upgrade-Warteschlange hinzufügen möchten. Genehmigte Nodes werden nacheinander aktualisiert.



Genehmigen Sie das SANtricity OS Upgrade für einen Appliance-Speicher-Node nur, wenn Sie sicher sind, dass der Node bereit ist, angehalten und neu gestartet zu werden. Wenn das Upgrade von SANtricity OS auf einem Node genehmigt wird, werden die Services auf diesem Node angehalten und der Upgrade-Prozess beginnt. Wenn die Aktualisierung des Node abgeschlossen ist, wird der Appliance-Node später neu gebootet. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren.

- Klicken Sie auf die Schaltfläche **Alle genehmigen**, um alle Speicher-Nodes der SANtricity OS Upgrade-Warteschlange hinzuzufügen.



Wenn die Reihenfolge, in der die Knoten aktualisiert werden, wichtig ist, genehmigen Sie nacheinander Knoten oder Gruppen von Knoten, und warten Sie, bis das Upgrade für jeden Knoten abgeschlossen ist, bevor Sie den nächsten Knoten genehmigen.

- Wählen Sie eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere Knoten zur SANtricity OS-Upgrade-Warteschlange hinzuzufügen. Die Schaltfläche **approve** ist deaktiviert, wenn der Status nicht nominal ist.

Nachdem Sie **Genehmigen** ausgewählt haben, bestimmt der Upgrade-Prozess, ob der Knoten aktualisiert werden kann. Wenn ein Knoten aktualisiert werden kann, wird er der Upgrade-Warteschlange hinzugefügt.

Bei einigen Nodes wird die ausgewählte Upgrade-Datei absichtlich nicht angewendet. Sie können das Upgrade abschließen, ohne dass Sie ein Upgrade dieser spezifischen Nodes durchführen müssen. Nodes, die absichtlich kein Upgrade durchgeführt wurden, zeigen eine Phase komplett (Upgrade versucht) und geben den Grund an, warum der Node nicht in der Spalte Details aktualisiert wurde.

10. Wenn Sie einen Knoten oder alle Knoten aus der SANtricity OS Upgrade-Warteschlange entfernen möchten, wählen Sie **Entfernen** oder **Alle entfernen**.

Wenn die Phase über Queued hinaus fortschreitet, wird die Schaltfläche **Entfernen** ausgeblendet und Sie können den Knoten nicht mehr aus dem SANtricity OS-Upgrade-Prozess entfernen.

11. Warten Sie, während das SANtricity OS Upgrade auf jeden genehmigten Grid-Node angewendet wird.

- Wenn bei einem Node während der Anwendung des SANtricity OS Upgrades eine Fehlerstufe angezeigt wird, ist das Upgrade für den Node fehlgeschlagen. Mithilfe des technischen Supports müssen Sie das Gerät möglicherweise in den Wartungsmodus versetzen, um es wiederherzustellen.
- Wenn die Firmware auf dem Node zu alt ist, um mit dem Grid-Manager aktualisiert zu werden, wird auf dem Node die Fehlerstufe angezeigt. Darin enthalten sind die Details, die Sie zum Upgrade von SANtricity OS auf dem Node mit dem Wartungsmodus verwenden müssen. Gehen Sie wie folgt vor, um den Fehler zu beheben:
 - i. Verwenden Sie den Wartungsmodus, um ein Upgrade von SANtricity OS auf dem Node durchzuführen, auf dem eine Fehlerstufe angezeigt wird.
 - ii. Verwenden Sie den Grid-Manager, um das SANtricity OS-Upgrade neu zu starten und abzuschließen.

Wenn das SANtricity OS Upgrade auf allen genehmigten Nodes abgeschlossen ist, wird die Fortschrittstabelle für SANtricity OS Upgrades geschlossen, und ein grünes Banner zeigt die Anzahl der aktualisierten Nodes sowie Datum und Uhrzeit des Upgrades an.

12. Wenn ein Knoten nicht aktualisiert werden kann, notieren Sie sich den Grund, der in der Spalte Details angezeigt wird, und führen Sie die entsprechende Aktion durch.



Das SANtricity OS-Upgrade ist erst abgeschlossen, wenn Sie das SANtricity OS-Upgrade auf allen aufgeführten Storage-Nodes genehmigen.

Grund	Empfohlene Maßnahmen
Storage-Node wurde bereits aktualisiert.	Keine weiteren Maßnahmen erforderlich.
Das SANtricity OS Upgrade ist für diesen Node nicht verfügbar.	Der Node verfügt nicht über einen Storage Controller, der vom StorageGRID System gemanagt werden kann. Schließen Sie das Upgrade ab, ohne den Node mit dieser Meldung zu aktualisieren.
Die SANtricity OS-Datei ist mit diesem Node nicht kompatibel.	Der Node erfordert eine andere SANtricity OS-Datei als die ausgewählte. Laden Sie nach Abschluss des aktuellen Upgrades die korrekte SANtricity OS-Datei für den Node herunter, und wiederholen Sie den Upgrade-Vorgang.

13. Wenn Sie die Genehmigung von Nodes beenden und zur Seite SANtricity OS zurückkehren möchten, um einen Upload einer neuen SANtricity OS-Datei zu ermöglichen, gehen Sie wie folgt vor:

- a. Wählen Sie **Knoten überspringen und beenden**.

Es wird eine Warnung angezeigt, in der Sie gefragt werden, ob Sie den Aktualisierungsvorgang wirklich beenden möchten, ohne alle zutreffenden Knoten zu aktualisieren.

- b. Wählen Sie * OK* aus, um zur Seite **SANtricity OS** zurückzukehren.

- c. Wenn Sie bereit sind, mit der Genehmigung von Knoten fortzufahren, [Laden Sie das SANtricity OS herunter](#) Um den Upgrade-Vorgang neu zu starten.



Nodes, die bereits genehmigt und ohne Fehler aktualisiert wurden, werden weiterhin aktualisiert.

14. Wiederholen Sie dieses Upgrade-Verfahren für alle Nodes in einer vollständigen Phase, für die eine andere SANtricity OS Upgrade-Datei erforderlich ist.



Verwenden Sie für alle Nodes, für die der Status als Warnung angezeigt wird, den Wartungsmodus, um das Upgrade durchzuführen.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

["Aktualisieren Sie SANtricity OS auf einem E2800 Controller mithilfe des Wartungsmodus"](#)

Aktualisieren Sie SANtricity OS auf einem E2800 Controller mithilfe des Wartungsmodus

Für Storage-Controller, die derzeit SANtricity OS verwenden, die älter als 08.42.20.00 (11.42) sind, müssen Sie das Verfahren des Wartungsmodus verwenden, um ein Upgrade durchzuführen.

Bevor Sie beginnen

- Sie haben den konsultiert "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um sicherzustellen, dass die für das Upgrade verwendete SANtricity OS-Version mit Ihrer Appliance kompatibel ist.
- Sie müssen den E5700SG Controller in platzieren "[Wartungsmodus](#)", Die die Verbindung zum E2800-Controller unterbricht.



In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den Wartungsmodus versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.

Über diese Aufgabe

Führen Sie keine Upgrades des SANtricity OS bzw. NVSRAM im E-Series Controller auf mehr als einer StorageGRID Appliance gleichzeitig durch.



Wenn Sie mehrere StorageGRID Appliances gleichzeitig aktualisieren, kann dies in Abhängigkeit von Ihrem Implementierungsmodell und den ILM-Richtlinien zu Datenunverfügbarkeit führen.

Schritte

1. Überprüfen Sie, ob das Gerät in ist "[Wartungsmodus](#)".
2. Greifen Sie über ein Service-Laptop auf den SANtricity System Manager zu und melden Sie sich an.
3. Laden Sie die neue SANtricity OS Software-Datei und die NVSRAM-Datei auf den Management-Client herunter.



Das NVSRAM bezieht sich auf die StorageGRID Appliance. Verwenden Sie den Standard-NVSRAM-Download nicht.

4. Folgen Sie den Anweisungen im Leitfaden zum Software- und Firmware-Upgrade *E2800 und E5700 SANtricity* oder der Online-Hilfe von SANtricity System Manager für ein Upgrade der Firmware und des NVSRAM des E2800 Controllers.



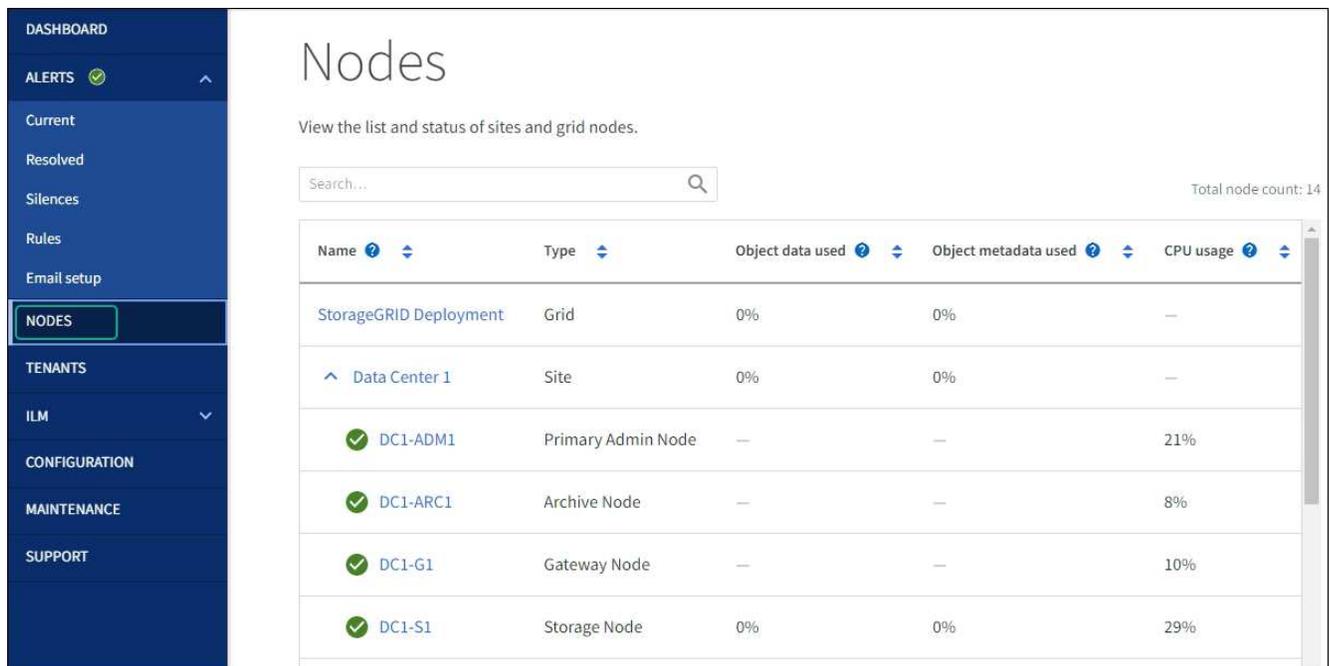
Aktivieren Sie die Upgrade-Dateien sofort. Die Aktivierung darf nicht verzögert werden.

5. Wenn diese Prozedur erfolgreich abgeschlossen ist und Sie weitere durchzuführenden Verfahren haben, während sich der Node im Wartungsmodus befindet, führen Sie sie jetzt aus. Wenn Sie fertig sind oder Fehler auftreten und von vorne beginnen möchten, wählen Sie **Erweitert > Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:
 - Wählen Sie **Neustart in StorageGRID** aus
 - Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. Wählen Sie diese Option aus, wenn während des Verfahrens Fehler auftreten und neu starten möchten. Nachdem der Node das Neubooten in den Wartungsmodus abgeschlossen hat, starten Sie den entsprechenden Schritt während des ausgefallenen Verfahrens

neu.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite Knoten sollte ein normaler Status angezeigt werden (grünes Häkchen-Symbol  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

["Aktualisieren Sie SANtricity OS auf Storage-Controllern mit Grid Manager"](#)

Aktualisieren Sie die Laufwerk-Firmware mit SANtricity System Manager

Aktualisieren Sie die Firmware des SG5700-Laufwerks mithilfe der Online-Methode von SANtricity System Manager

Aktualisieren Sie mit der Online-Methode des SANtricity System Managers die Firmware auf den Laufwerken in Ihrer Appliance, um sicherzustellen, dass Sie über die neuesten

Funktionen und Fehlerbehebungen verfügen.

Bevor Sie beginnen

- Die Storage Appliance hat einen optimalen Status.
- Alle Laufwerke haben einen optimalen Status.



Aktualisieren Sie nicht gleichzeitig die Laufwerk-Firmware auf mehr als einer StorageGRID Appliance. Dies kann je nach Bereitstellungsmodell und ILM-Richtlinie zu einer Nichtverfügbarkeit von Daten führen.

Über diese Aufgabe

Die Laufwerke werden nacheinander aktualisiert, während die Appliance I/O-Vorgänge durchführt. Bei dieser Methode müssen Sie das Gerät nicht in den Wartungsmodus versetzen. Allerdings kann die System-Performance beeinträchtigt sein und das Upgrade kann mehrere Stunden länger dauern als die Offline-Methode.



Laufwerke, die zu Volumes ohne Redundanz gehören, müssen mithilfe der Offline-Methode aktualisiert werden. Die Offline-Methode sollte für alle Laufwerke verwendet werden, die mit dem Flash-Lese-Cache verbunden sind, oder für alle Pools oder Volume-Gruppen, die derzeit heruntergestuft sind. Sie müssen die Offline-Methode beim Upgrade von SSD-Laufwerken verwenden.

Schritte

1. Greifen Sie mit einer der folgenden Methoden auf SANtricity System Manager zu:
 - Verwenden Sie das StorageGRID-Appliance-Installationsprogramm, und wählen Sie **Erweitert > SANtricity-Systemmanager**
 - Verwenden Sie den Grid-Manager, und wählen Sie **NODES > Storage Node > SANtricity System Manager** aus
 - Verwenden Sie SANtricity System Manager, indem Sie zur Storage Controller-IP navigieren:
`https://Storage_Controller_IP`
2. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des SANtricity System Manager-Administrators ein.
3. Überprüfen Sie die Version der Laufwerk-Firmware, die derzeit in der Speicher-Appliance installiert ist:
 - a. Wählen Sie im SANtricity System Manager **SUPPORT > Upgrade-Center** aus.
 - b. Wählen Sie unter Laufwerk-Firmware-Upgrade die Option **Upgrade starten** aus.

Auf der Seite Laufwerksfirmware aktualisieren werden die aktuell installierten Laufwerksfirmware-Dateien angezeigt.

- c. Beachten Sie die aktuellen Versionen der Laufwerk-Firmware und die Laufwerkskennungen in der Spalte Aktueller Laufwerk-Firmware.

Upgrade Drive Firmware

1 Select Upgrade Files

Review your current drive firmware and select upgrade files below...

[What do I need to know before upgrading drive firmware?](#)

Current Drive Firmware

MS02, KPM51VUG800G

Total rows: 1



In diesem Beispiel:

- Die Version der Laufwerk-Firmware lautet **MS02**.
- Die Laufwerk-ID lautet **KPM51VUG800G**.

d. Wählen Sie in der Spalte „verbundene Laufwerke“ die Option **Laufwerke anzeigen** aus, um anzuzeigen, wo diese Laufwerke in Ihrem Speichergerät installiert sind.

e. Schließen Sie das Fenster Upgrade Drive Firmware.

4. Laden Sie das verfügbare Laufwerk-Firmware-Upgrade herunter, und bereiten Sie es vor:

a. Wählen Sie unter Laufwerk-Firmware-Upgrade **NetApp Support** aus.

b. Wählen Sie auf der NetApp Support-Website die Registerkarte **Downloads** aus und wählen Sie dann **E-Series Festplatten-Firmware** aus.

Die Seite E-Series Festplatten-Firmware wird angezeigt.

c. Suchen Sie nach jedem in Ihrer Speicheranwendung installierten **Drive Identifier**, und stellen Sie sicher, dass jeder Laufwerkennung die neueste Firmware-Version hat.

- Wenn die Firmware-Version kein Link ist, hat diese Laufwerkennung die neueste Firmware-Version.
- Wenn eine oder mehrere Laufwerk-Teilenummern für eine Laufwerksidentifikation aufgeführt sind, ist für diese Laufwerke ein Firmware-Upgrade verfügbar. Sie können einen beliebigen Link auswählen, um die Firmware-Datei herunterzuladen.

PRODUCTS ▾ SYSTEMS ▾ DOCS & KNOWLEDGEBASE ▾ COMMUNITY ▾ DOWNLOADS ▾ TOOLS ▾ CASES ▾ PARTS ▾

Downloads > Firmware > E-Series Disk Firmware

E-Series Disk Firmware

Download all current E-Series Disk Firmware

Drive Part Number ▾	Descriptions ▾	Drive Identifier ▾	Firmware Rev. (Download)	Notes and Config Info	Release Date ▾
Drive Part Number	Descriptions	KPM51VUG800G	Firmware Rev. (Download)		
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	MS03	MS02 Fixes Bug 1194908 MS03 Fixes Bug 1334862	04-Sep-2020

- d. Wenn eine spätere Firmware-Version aufgeführt wird, wählen Sie den Link im Firmware-Rev. Aus (Download) Spalte zum Herunterladen einer .zip Archiv mit der Firmware-Datei.
 - e. Extrahieren Sie die von der Support-Website heruntergeladenen Archivdateien der Laufwerk-Firmware (entpacken).
5. Installieren Sie das Laufwerk-Firmware-Upgrade:

- a. Wählen Sie im SANtricity System Manager unter Upgrade der Laufwerk-Firmware die Option **Upgrade starten** aus.
- b. Wählen Sie **Durchsuchen** aus, und wählen Sie die neuen Laufwerk-Firmware-Dateien aus, die Sie von der Support-Website heruntergeladen haben.

Die Firmware-Dateien des Laufwerks haben einen ähnlichen Dateinamen wie
D_HUC101212CSS600_30602291_MS01_2800_0002.dlp.

Sie können bis zu vier Laufwerk-Firmware-Dateien auswählen, jeweils eine. Wenn mehrere Firmware-Dateien eines Laufwerks mit demselben Laufwerk kompatibel sind, wird ein Dateikonflikt angezeigt. Legen Sie fest, welche Laufwerk-Firmware-Datei Sie für das Upgrade verwenden möchten, und entfernen Sie die andere.

- c. Wählen Sie **Weiter**.

Select Drives listet die Laufwerke auf, die Sie mit den ausgewählten Firmware-Dateien aktualisieren können.

Es werden nur kompatible Laufwerke angezeigt.

Die ausgewählte Firmware für das Laufwerk wird in der Spalte **vorgeschlagene Firmware** angezeigt. Wenn Sie diese Firmware ändern müssen, wählen Sie **Zurück**.

- d. Wählen Sie **Alle Laufwerke online aktualisieren** – Aktualisieren Sie die Laufwerke, die einen Firmware-Download unterstützen können, während das Speicherarray I/O-Vorgänge verarbeitet Sie müssen die I/O-Vorgänge für die zugehörigen Volumes, die diese Laufwerke verwenden, nicht stoppen, wenn Sie diese Aktualisierungsmethode auswählen.



Ein Online-Upgrade kann mehrere Stunden länger dauern als ein Offline-Upgrade.

- e. Wählen Sie in der ersten Spalte der Tabelle das Laufwerk oder die Laufwerke aus, die aktualisiert werden sollen.

Als Best Practice wird empfohlen, alle Laufwerke desselben Modells auf dieselbe Firmware-Version zu

aktualisieren.

- f. Wählen Sie **Start** und bestätigen Sie, dass Sie das Upgrade durchführen möchten.

Wenn Sie das Upgrade beenden möchten, wählen Sie **Stopp**. Alle derzeit ausgeführten Firmware-Downloads abgeschlossen. Alle nicht gestarteten Firmware-Downloads werden abgebrochen.



Das Anhalten der Laufwerk-Firmware-Aktualisierung kann zu Datenverlust oder nicht verfügbaren Laufwerken führen.

- g. (Optional) um eine Liste der aktualisierten Versionen anzuzeigen, wählen Sie **Protokoll speichern**.

Die Protokolldatei wird im Download-Ordner für Ihren Browser mit dem Namen gespeichert `latest-upgrade-log-timestamp.txt`.

["Beheben Sie bei Bedarf Fehler bei der Aktualisierung der Treiber-Firmware"](#).

Aktualisieren Sie die Firmware des SG5700 Laufwerks mithilfe von SANtricity System Manager im Offline-Modus

Aktualisieren Sie mit der Online-Methode des SANtricity System Managers die Firmware auf den Laufwerken in Ihrer Appliance, um sicherzustellen, dass Sie über die neuesten Funktionen und Fehlerbehebungen verfügen.

Bevor Sie beginnen

- Die Storage Appliance hat einen optimalen Status.
- Alle Laufwerke haben einen optimalen Status.
- Das ist schon ["Versetzen Sie die StorageGRID Appliance in den Wartungsmodus"](#).



Während sich die Appliance im Wartungsmodus befindet, wird die I/O-Aktivität (Eingabe/Ausgabe) für den Storage Controller angehalten, um störende Storage-Vorgänge zu sichern.



Aktualisieren Sie nicht gleichzeitig die Laufwerk-Firmware auf mehr als einer StorageGRID Appliance. Dies kann je nach Bereitstellungsmodell und ILM-Richtlinie zu einer Nichtverfügbarkeit von Daten führen.

Über diese Aufgabe

Die Laufwerke werden parallel aktualisiert, während sich die Appliance im Wartungsmodus befindet. Wenn der Pool oder die Volume-Gruppe keine Redundanz unterstützt oder herabgesetzt ist, müssen Sie die Offline-Methode verwenden, um die Laufwerk-Firmware zu aktualisieren. Sie sollten auch die Offline-Methode für alle Laufwerke verwenden, die mit dem Flash-Lese-Cache oder einem Pool oder einer Volume-Gruppe verbunden sind, die derzeit heruntergestuft ist. Die Offline-Methode aktualisiert die Firmware nur, wenn alle I/O-Aktivitäten auf den zu aktualisierenden Laufwerken angehalten werden. Um die I/O-Aktivität zu beenden, versetzen Sie den Node in den Wartungsmodus.

Die Offline-Methode ist schneller als die Online-Methode und wird deutlich schneller sein, wenn viele Laufwerke in einer einzigen Appliance Upgrades erfordern. Allerdings müssen Nodes außer Betrieb genommen werden. Dies erfordert unter Umständen ein Wartungsfenster und ein Monitoring des Fortschritts. Wählen Sie die Methode aus, die am besten zu Ihren betrieblichen Verfahren passt und die Anzahl der Laufwerke, die aktualisiert werden müssen.

Schritte

1. Vergewissern Sie sich, dass das Gerät in ist "[Wartungsmodus](#)".
2. Greifen Sie mit einer der folgenden Methoden auf SANtricity System Manager zu:
 - Verwenden Sie das StorageGRID-Appliance-Installationsprogramm, und wählen Sie **Erweitert > SANtricity-Systemmanager**
 - Verwenden Sie den Grid-Manager, und wählen Sie **NODES > Storage Node > SANtricity System Manager** aus
 - Verwenden Sie SANtricity System Manager, indem Sie zur Storage Controller-IP navigieren:

`https://Storage_Controller_IP`

3. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des SANtricity System Manager-Administrators ein.
4. Überprüfen Sie die Version der Laufwerk-Firmware, die derzeit in der Speicher-Appliance installiert ist:
 - a. Wählen Sie im SANtricity System Manager **SUPPORT > Upgrade-Center** aus.
 - b. Wählen Sie unter Laufwerk-Firmware-Upgrade die Option **Upgrade starten** aus.

Auf der Seite Laufwerksfirmware aktualisieren werden die aktuell installierten Laufwerksfirmware-Dateien angezeigt.

- c. Beachten Sie die aktuellen Versionen der Laufwerk-Firmware und die Laufwerkskennungen in der Spalte Aktueller Laufwerk-Firmware.

Upgrade Drive Firmware

1 Select Upgrade Files

Review your current drive firmware and select upgrade files below...

[What do I need to know before upgrading drive firmware?](#)

Current Drive Firmware

MS02, KPM51VUG800G

Total rows: 1 |

In diesem Beispiel:

- Die Version der Laufwerk-Firmware lautet **MS02**.
 - Die Laufwerk-ID lautet **KPM51VUG800G**.
- d. Wählen Sie in der Spalte „verbundene Laufwerke“ die Option **Laufwerke anzeigen** aus, um anzuzeigen, wo diese Laufwerke in Ihrem Speichergerät installiert sind.
 - e. Schließen Sie das Fenster Upgrade Drive Firmware.

5. Laden Sie das verfügbare Laufwerk-Firmware-Upgrade herunter, und bereiten Sie es vor:

- a. Wählen Sie unter Laufwerk-Firmware-Upgrade **NetApp Support** aus.
- b. Wählen Sie auf der NetApp Support-Website die Registerkarte **Downloads** aus und wählen Sie dann **E-Series Festplatten-Firmware** aus.

Die Seite E-Series Festplatten-Firmware wird angezeigt.

- c. Suchen Sie nach jedem in Ihrer Speicheranwendung installierten **Drive Identifier**, und stellen Sie sicher, dass jeder Laufwerkennung die neueste Firmware-Version hat.
 - Wenn die Firmware-Version kein Link ist, hat diese Laufwerkennung die neueste Firmware-Version.
 - Wenn eine oder mehrere Laufwerk-Teilenummern für eine Laufwerksidentifikation aufgeführt sind, ist für diese Laufwerke ein Firmware-Upgrade verfügbar. Sie können einen beliebigen Link auswählen, um die Firmware-Datei herunterzuladen.

Drive Part Number	Descriptions	Drive Identifier	Firmware Rev. (Download)	Notes and Config Info	Release Date
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	MS03	MS02 Fixes Bug 1194908 MS03 Fixes Bug 1334862	04-Sep-2020

- d. Wenn eine spätere Firmware-Version aufgeführt wird, wählen Sie den Link im Firmware-Rev. Aus (Download) Spalte zum Herunterladen einer .zip Archiv mit der Firmware-Datei.
- e. Extrahieren Sie die von der Support-Website heruntergeladenen Archivdateien der Laufwerk-Firmware (entpacken).

6. Installieren Sie das Laufwerk-Firmware-Upgrade:

- a. Wählen Sie im SANtricity System Manager unter Upgrade der Laufwerk-Firmware die Option **Upgrade starten** aus.
- b. Wählen Sie **Durchsuchen** aus, und wählen Sie die neuen Laufwerk-Firmware-Dateien aus, die Sie von der Support-Website heruntergeladen haben.

Die Firmware-Dateien des Laufwerks haben einen ähnlichen Dateinamen wie
D_HUC101212CSS600_30602291_MS01_2800_0002.dlp.

Sie können bis zu vier Laufwerk-Firmware-Dateien auswählen, jeweils eine. Wenn mehrere Firmware-Dateien eines Laufwerks mit demselben Laufwerk kompatibel sind, wird ein Dateikonflikt angezeigt. Legen Sie fest, welche Laufwerk-Firmware-Datei Sie für das Upgrade verwenden möchten, und entfernen Sie die andere.

- c. Wählen Sie **Weiter**.

Select Drives listet die Laufwerke auf, die Sie mit den ausgewählten Firmware-Dateien aktualisieren können.

Es werden nur kompatible Laufwerke angezeigt.

Die ausgewählte Firmware für das Laufwerk wird in der Spalte **vorgeschlagene Firmware** angezeigt. Wenn Sie diese Firmware ändern müssen, wählen Sie **Zurück**.

- d. Wählen Sie **Alle Laufwerke offline aktualisieren (parallel)** – aktualisiert die Laufwerke, die einen Firmware-Download unterstützen können, nur während alle I/O-Aktivitäten auf allen Volumes angehalten werden, die die Laufwerke verwenden.



Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie diese Methode verwenden. Sie sollten die Methode **Offline** verwenden, um die Laufwerksfirmware zu aktualisieren.



Wenn Sie die Offline-Aktualisierung (parallel) verwenden möchten, fahren Sie nur dann fort, wenn Sie sicher sind, dass sich das Gerät im Wartungsmodus befindet. Wenn die Appliance nicht in den Wartungsmodus versetzt wird, bevor ein Offline-Update der Laufwerk-Firmware initiiert wird, kann dies zu einem Datenverlust führen.

- e. Wählen Sie in der ersten Spalte der Tabelle das Laufwerk oder die Laufwerke aus, die aktualisiert werden sollen.

Als Best Practice wird empfohlen, alle Laufwerke desselben Modells auf dieselbe Firmware-Version zu aktualisieren.

- f. Wählen Sie **Start** und bestätigen Sie, dass Sie das Upgrade durchführen möchten.

Wenn Sie das Upgrade beenden möchten, wählen Sie **Stopp**. Alle derzeit ausgeführten Firmware-Downloads abgeschlossen. Alle nicht gestarteten Firmware-Downloads werden abgebrochen.



Das Anhalten der Laufwerk-Firmware-Aktualisierung kann zu Datenverlust oder nicht verfügbaren Laufwerken führen.

- g. (Optional) um eine Liste der aktualisierten Versionen anzuzeigen, wählen Sie **Protokoll speichern**.

Die Protokolldatei wird im Download-Ordner für Ihren Browser mit dem Namen gespeichert `latest-upgrade-log-timestamp.txt`.

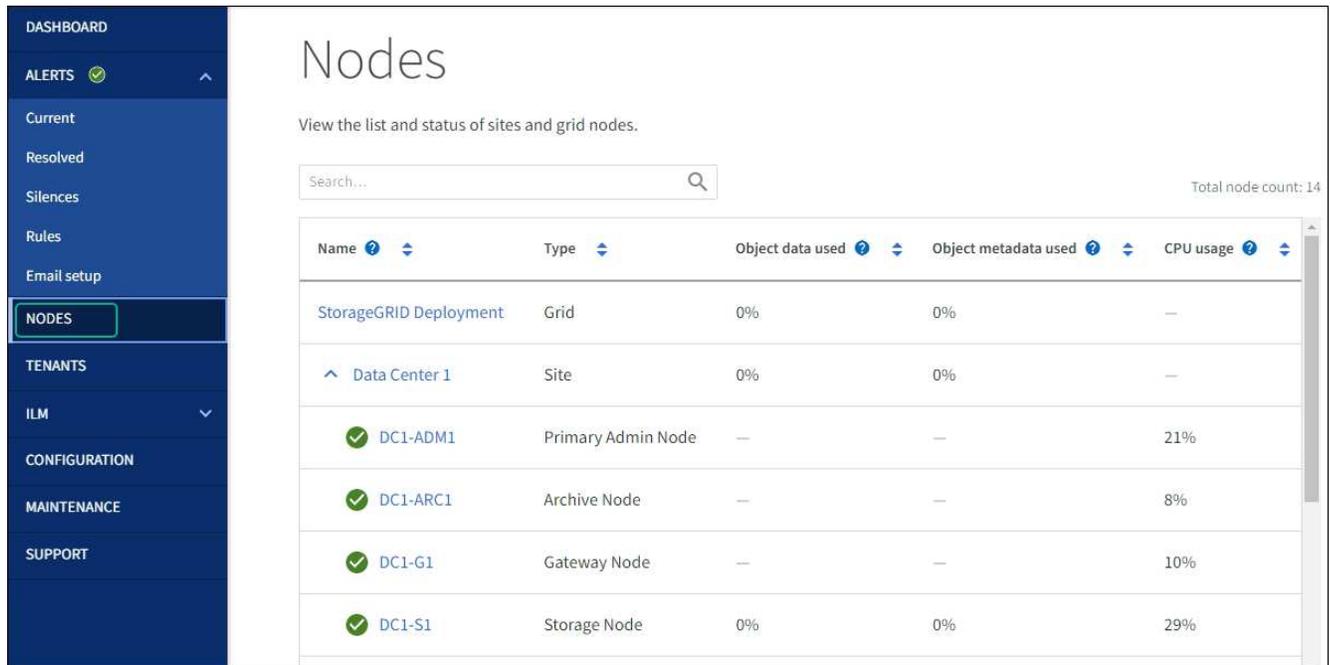
["Beheben Sie bei Bedarf Fehler bei der Aktualisierung der Treiber-Firmware"](#).

7. Führen Sie nach erfolgreichem Abschluss des Verfahrens alle weiteren Wartungsmaßnahmen durch, während sich der Node im Wartungsmodus befindet. Wenn Sie fertig sind oder Fehler aufgetreten sind und neu gestartet werden möchten, gehen Sie zum StorageGRID-Installationsprogramm und wählen Sie **Erweitert > Neustart-Controller** aus. Wählen Sie dann eine der folgenden Optionen aus:

- **Neustart in StorageGRID.**
- **Neustart im Wartungsmodus.** Booten Sie den Controller neu, und belassen Sie den Node im Wartungsmodus. Wählen Sie diese Option aus, wenn während des Verfahrens Fehler auftreten und Sie von vorne beginnen möchten. Nachdem der Node das Neubooten in den Wartungsmodus abgeschlossen hat, starten Sie den entsprechenden Schritt während des ausgefallenen Verfahrens neu.

Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid

beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite Knoten sollte ein normaler Status angezeigt werden (grünes Häkchen-Symbol  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.



Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	21%
 DC1-ARC1	Archive Node	—	—	8%
 DC1-G1	Gateway Node	—	—	10%
 DC1-S1	Storage Node	0%	0%	29%

Fehler beim Upgrade der Laufwerk-Firmware beheben

Beheben Sie Fehler, die auftreten können, wenn Sie SANtricity System Manager zum Aktualisieren der Firmware auf den Laufwerken in Ihrer Appliance verwenden.

• Fehlgeschlagene zugewiesene Laufwerke

- Ein Grund für den Fehler könnte sein, dass das Laufwerk nicht über die entsprechende Signatur verfügt. Stellen Sie sicher, dass es sich bei dem betroffenen Laufwerk um ein autorisiertes Laufwerk handelt. Weitere Informationen erhalten Sie vom technischen Support.
- Stellen Sie beim Austausch eines Laufwerks sicher, dass das Ersatzlaufwerk eine Kapazität hat, die der des ausgefallenen Laufwerks entspricht oder größer ist als das ausgefallene Laufwerk, das Sie ersetzen.
- Sie können das ausgefallene Laufwerk ersetzen, während das Speicher-Array I/O-Vorgänge erhält

• Speicher-Array prüfen

- Stellen Sie sicher, dass jedem Controller eine IP-Adresse zugewiesen wurde.
- Stellen Sie sicher, dass alle Kabel, die an den Controller angeschlossen sind, nicht beschädigt sind.
- Stellen Sie sicher, dass alle Kabel fest angeschlossen sind.

• * Integrierte Hot-Spare-Laufwerke*

Diese Fehlerbedingung muss korrigiert werden, bevor Sie die Firmware aktualisieren können.

• Unvollständige Volume-Gruppen

Wenn eine oder mehrere Volume-Gruppen oder Disk Pools unvollständig sind, müssen Sie diese Fehlerbedingung korrigieren, bevor Sie die Firmware aktualisieren können.

- **Exklusive Operationen (außer Hintergrund-Medien/Paritäts-Scan), die derzeit auf beliebigen Volume-Gruppen** ausgeführt werden

Wenn ein oder mehrere exklusive Vorgänge ausgeführt werden, müssen die Vorgänge abgeschlossen sein, bevor die Firmware aktualisiert werden kann. Überwachen Sie den Fortschritt des Betriebs mit System Manager.

- **Fehlende Volumen**

Sie müssen den fehlenden Datenträgerzustand korrigieren, bevor die Firmware aktualisiert werden kann.

- **Entweder Controller in einem anderen Zustand als optimal**

Einer der Controller des Storage Arrays muss Aufmerksamkeit schenken. Diese Bedingung muss korrigiert werden, bevor die Firmware aktualisiert werden kann.

- **Unpassende Speicherpartitionsdaten zwischen Controller-Objektgrafiken**

Beim Validieren der Daten auf den Controllern ist ein Fehler aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **SPM Überprüfung des Datenbankcontrollers schlägt fehl**

Auf einem Controller ist ein Fehler bei der Zuordnung von Speicherpartitionen zur Datenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Überprüfung der Konfigurationsdatenbank (sofern von der Controller-Version des Speicherarrays unterstützt)**

Auf einem Controller ist ein Fehler in der Konfigurationsdatenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **MEL-bezogene Prüfungen**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **In den letzten 7 Tagen wurden mehr als 10 DDE Informations- oder kritische MEL-Ereignisse gemeldet**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Mehr als 2 Seiten 2C kritische MEL-Ereignisse wurden in den letzten 7 Tagen gemeldet**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **In den letzten 7 Tagen wurden mehr als 2 heruntergestuften Drive Channel-kritische MEL-Ereignisse gemeldet**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Mehr als 4 kritische MEL-Einträge in den letzten 7 Tagen**

Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

Ändern Sie die Link-Konfiguration des E5700SG Controllers

Sie können die Ethernet-Link-Konfiguration des E5700SG-Controllers ändern. Sie können den Port Bond-Modus, den Netzwerk-Bond-Modus und die Verbindungsgeschwindigkeit ändern.

Bevor Sie beginnen

"Platzieren Sie den E5700SG Controller in den Wartungsmodus".



In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den Wartungsmodus versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.

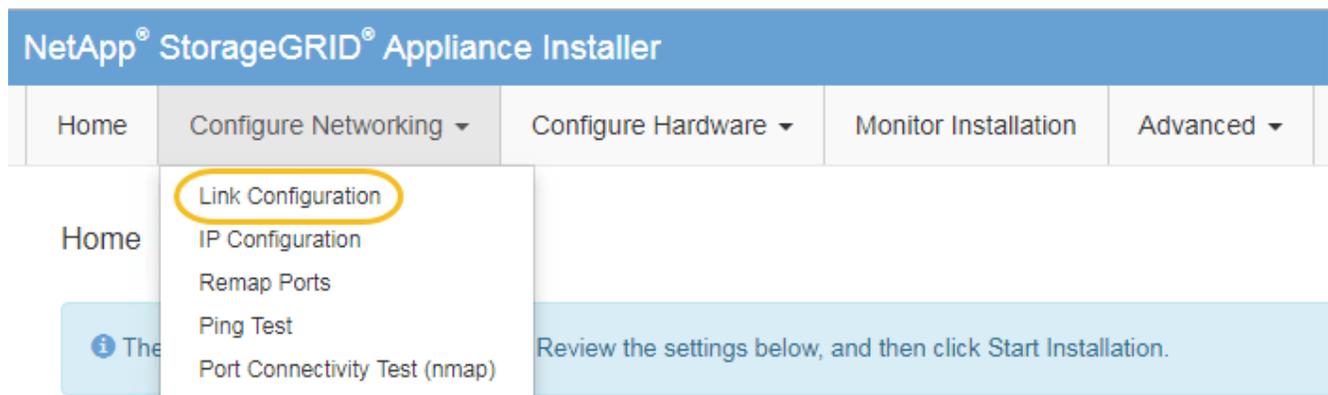
Über diese Aufgabe

Die Ethernet-Link-Konfiguration des E5700SG-Controllers kann wie folgt geändert werden:

- Ändern des **Port Bond Modus** von Fixed zu Aggregate oder von Aggregate zu Fixed
- Ändern des **Netzwerk-Bond-Modus** von Active-Backup zu LACP oder von LACP zu Active-Backup
- Aktivieren oder Deaktivieren von VLAN-Tagging oder Ändern des Werts einer VLAN-Tag-Nummer
- Ändern der Verbindungsgeschwindigkeit von 10-GbE auf 25-GbE oder von 25-GbE auf 10-GbE

Schritte

1. Wählen Sie im Menü die Option **Netzwerke konfigurieren > Link-Konfiguration** aus.



2. Ändern Sie die gewünschten Änderungen an der Link-Konfiguration.

Weitere Informationen zu den Optionen finden Sie unter "[Netzwerkverbindungen konfigurieren](#)".

3. Wenn Sie mit Ihrer Auswahl zufrieden sind, klicken Sie auf **Speichern**.



Wenn Sie Änderungen am Netzwerk oder an der Verbindung vorgenommen haben, über die Sie verbunden sind, können Sie die Verbindung verlieren. Wenn die Verbindung nicht innerhalb von 1 Minute wiederhergestellt wird, geben Sie die URL für den StorageGRID-Appliance-Installer erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:

`https://E5700SG_Controller_IP:8443`

Wenn Sie Änderungen an den VLAN-Einstellungen vorgenommen haben, hat sich das Subnetz für die Appliance möglicherweise geändert. Wenn Sie die IP-Adressen für die Appliance ändern müssen, befolgen

Sie die "[Konfigurieren Sie die StorageGRID-IP-Adressen](#)" Anweisungen.

4. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren > Ping-Test** aus.
5. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in allen Netzwerken zu überprüfen, die möglicherweise von den in vorgenommenen Änderungen der Verbindungskonfiguration betroffen sind [Verbindungskonfiguration ändern](#) Schritt:

Zusätzlich zu allen anderen Tests, die Sie durchführen möchten, bestätigen Sie, dass Sie die Grid-IP-Adresse des primären Admin-Knotens und die Grid-IP-Adresse von mindestens einem anderen Speicherknoten pingen können. Korrigieren Sie ggf. alle Probleme mit der Verbindungskonfiguration.

6. Sobald Sie zufrieden sind, dass die Änderungen an der Link-Konfiguration funktionieren, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:
 - Wählen Sie **Neustart in StorageGRID** aus, um den Controller neu zu starten, wobei der Knoten wieder in das Raster integriert wird. Wählen Sie diese Option, wenn Sie im Wartungsmodus ausgeführt werden und den Node in den normalen Betrieb zurückkehren möchten.
 - Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. (Diese Option ist nur verfügbar, wenn sich der Controller im Wartungsmodus befindet.) Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

Hardware-Verfahren

E2800 Series Storage-Controller in der SG5700 austauschen

Möglicherweise müssen Sie den E2800 Serie-Controller ersetzen, wenn er nicht optimal funktioniert oder ausgefallen ist.

Über diese Aufgabe

- Sie verfügen über einen Ersatzcontroller mit derselben Teilenummer wie der zu ersetzenden Controller.



Verlassen Sie sich beim Austausch eines Controllers in der StorageGRID Appliance nicht auf die Anweisungen zur E-Series, da die Vorgehensweisen nicht identisch sind.

- Sie verfügen über Etiketten, um jedes Kabel, das mit dem Controller verbunden ist, zu identifizieren.
- Wenn alle Laufwerke gesichert sind, haben Sie die Schritte im überprüft "[Controller-Austauschverfahren bei der simplex E2800 Serie](#)", Die das Herunterladen und Installieren der E-Serie SANtricity System Manager von der NetApp Support-Website und dann mit dem Enterprise Management Fenster (EMW), um die gesicherten Laufwerke nach dem Austausch des Controllers entsperren.



Sie können das Gerät erst dann verwenden, wenn Sie die Laufwerke mit dem gespeicherten Schlüssel entsperren.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

Sie können auf zwei Arten feststellen, ob ein ausgefallener Controller-Behälter besteht:

- Der Recovery Guru im SANtricity System Manager führt Sie dazu, den Controller zu ersetzen.
- Die gelbe Warn-LED am Controller leuchtet und gibt an, dass der Controller einen Fehler aufweist.

Auf den Appliance-Speicherknoten kann nicht zugegriffen werden, wenn Sie den Controller austauschen. Wenn der Controller der E2800 Serie ausreichend funktioniert, können Sie dies gerne tun ["Platzieren Sie den E5700SG Controller in den Wartungsmodus"](#).

Wenn Sie einen Controller austauschen, müssen Sie den Akku aus dem ursprünglichen Controller entfernen und in den Ersatzcontroller einsetzen. In einigen Fällen müssen Sie möglicherweise auch die Host-Schnittstellenkarte vom ursprünglichen Controller entfernen und im Ersatzcontroller installieren.

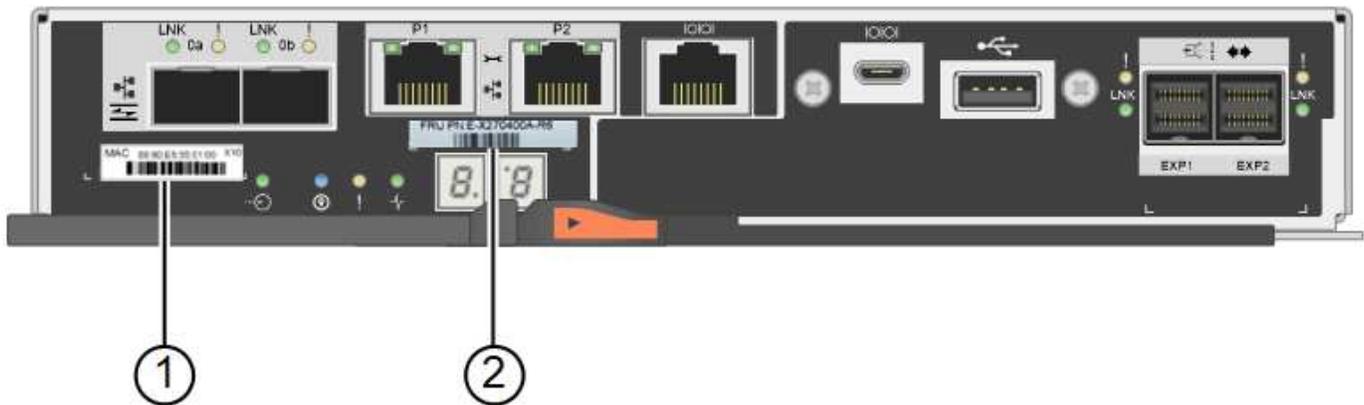


Die Storage Controller in den meisten Appliance-Modellen umfassen keine Host Interface Cards (HIC).

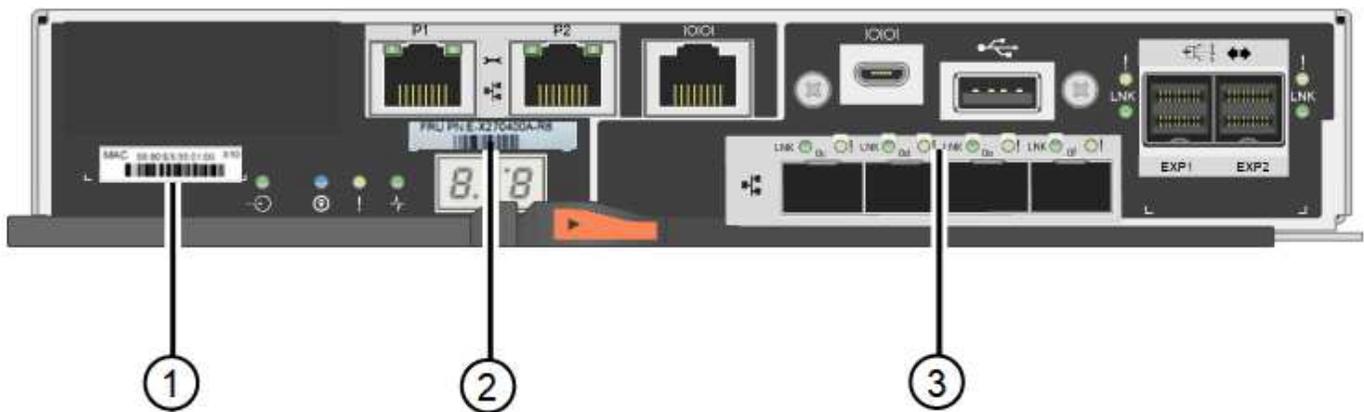
Schritt 1: Bereiten Sie vor, den Controller zu entfernen

Diese Abbildungen zeigen den E2800A-Controller und den E2800B-Controller. Das Verfahren zum Austausch der E2800 Controller der Serie und des EF570 Controllers ist identisch.

E2800A Storage-Controller:



E2800B Storage-Controller:



Etikett	Komponente	Beschreibung
1	MAC-Adresse	Die MAC-Adresse für Management-Port 1 („P1 auf E2800A und 0a auf E2800B“). Wenn Sie die IP-Adresse des Original-Controllers über DHCP erhalten haben, benötigen Sie diese Adresse, um eine Verbindung zum neuen Controller herzustellen.

Etikett	Komponente	Beschreibung
2	FRU-Teilenummer	Die FRU-Teilenummer. Diese Nummer muss der Teilenummer des derzeit installierten Controllers entsprechen.
3	4-Port-HIC	Die Host Interface Card (HIC) mit 4 Ports. Diese Karte muss auf den neuen Controller verschoben werden, wenn Sie den Austausch durchführen. Hinweis: Der E2800A Controller besitzt keine HIC.

Befolgen Sie die Anweisungen beim Austausch des E2800 Controllers, um das Entfernen des Controllers vorzubereiten.

Sie führen die folgenden Schritte mit SANtricity System Manager aus.

Schritte

1. Notieren Sie sich, welche Version der SANtricity OS Software derzeit auf dem Controller installiert ist.
2. Notieren Sie sich, welche NVSRAM-Version derzeit installiert ist.
3. Wenn die Laufwerksicherheit aktiviert ist, stellen Sie sicher, dass ein gespeicherter Schlüssel existiert und dass Sie den Passphrase kennen, der für die Installation erforderlich ist.



Möglicher Verlust des Datenzugriffs — Wenn alle Laufwerke in der Appliance sicherheitsaktiviert sind, kann der neue Controller erst dann auf die Appliance zugreifen, wenn Sie die gesicherten Laufwerke über das Enterprise Management Fenster in SANtricity System Manager entsperren.

4. Sichern Sie die Konfigurationsdatenbank.

Wenn beim Entfernen eines Controllers ein Problem auftritt, können Sie die gespeicherte Datei verwenden, um Ihre Konfiguration wiederherzustellen.

5. Sammeln von Support-Daten für die Appliance



Durch das Erfassen von Support-Daten vor und nach dem Ersetzen einer Komponente wird sichergestellt, dass Sie einen vollständigen Satz von Protokollen an den technischen Support senden können, wenn der Austausch das Problem nicht behebt.

Schritt 2: Den Controller offline schalten

Versetzen Sie den Controller in den Offline-Modus und vergewissern Sie sich, dass alle Vorgänge abgeschlossen sind.

Schritte

1. Wenn die StorageGRID Appliance in einem StorageGRID System ausgeführt wird, "[Platzieren Sie den E5700SG Controller in den Wartungsmodus](#)".
2. Wenn der E2800 Controller ausreichend funktioniert, um ein kontrolliertes Herunterfahren zu ermöglichen, bestätigen Sie, dass alle Operationen abgeschlossen wurden.
3. Wählen Sie auf der Startseite des SANtricity System Managers die Option **Vorgänge in Bearbeitung anzeigen**.

4. Vergewissern Sie sich, dass alle Vorgänge abgeschlossen sind.
5. Schaltet das Controller-Shelf aus.

Schritt 3: Entfernen Sie die Steuerung

Entfernen Sie den Controller aus dem Gerät.

Schritte

1. Setzen Sie ein ESD-Armband an oder ergreifen Sie andere antistatische Vorsichtsmaßnahmen.
2. Beschriften Sie die Kabel, und trennen Sie dann die Kabel und SFPs.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

3. Lösen Sie die Steuerung vom Gerät, indem Sie die Verriegelung am Nockengriff so lange drücken, bis sie sich löst, und öffnen Sie dann den Nockengriff nach rechts.
4. Schieben Sie den Regler mit zwei Händen und dem Nockengriff aus dem Gerät.



Verwenden Sie immer zwei Hände, um das Gewicht der Steuerung zu unterstützen.

5. Stellen Sie den Controller auf eine flache, statische Oberfläche, wobei die abnehmbare Abdeckung nach oben zeigt.
6. Entfernen Sie die Abdeckung, indem Sie die Taste nach unten drücken und die Abdeckung abnehmen.

Schritt 4: Batterie auf den neuen Controller bringen

Entfernen Sie den Akku aus dem fehlerhaften Controller, und setzen Sie ihn in den Ersatz-Controller ein.

Schritte

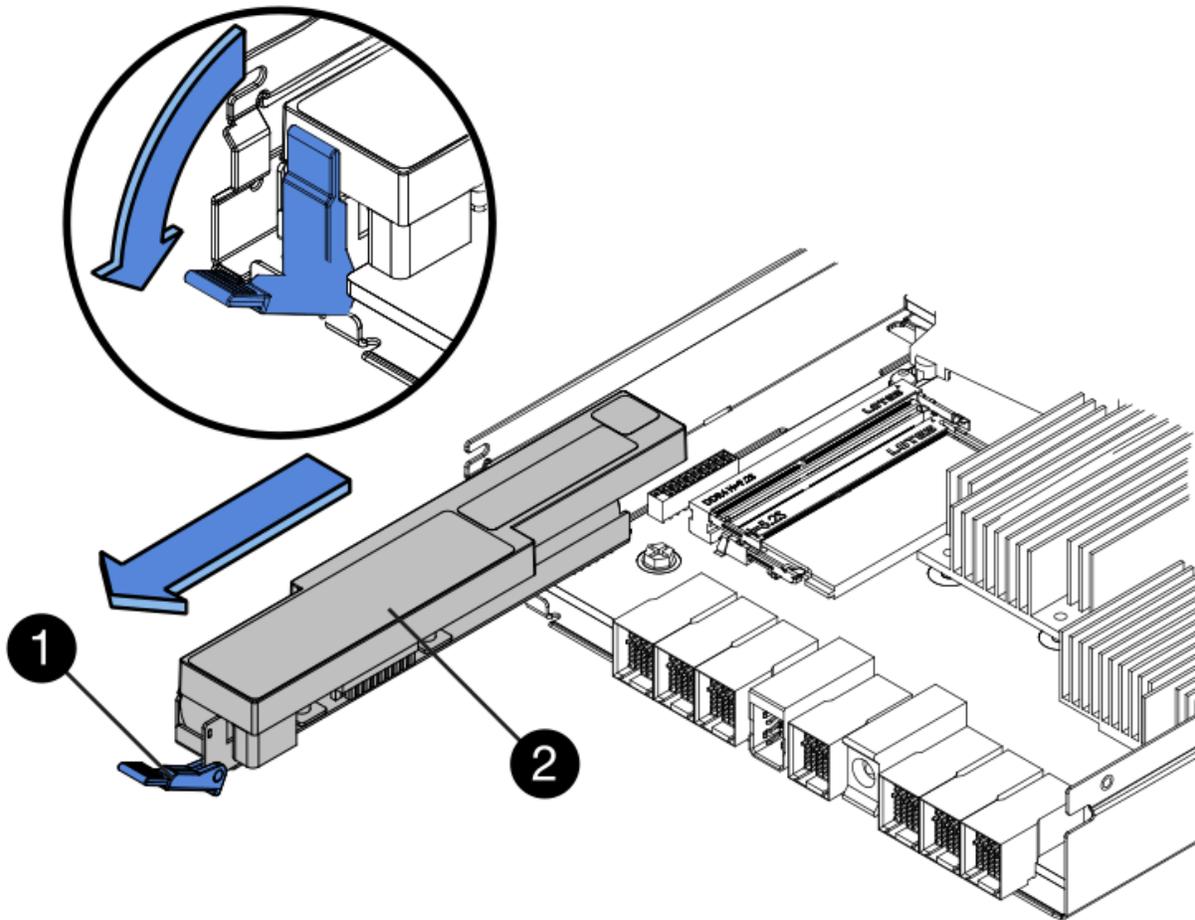
1. Vergewissern Sie sich, dass die grüne LED im Controller (zwischen Akku und DIMMs) aus ist.

Wenn diese grüne LED leuchtet, wird der Controller weiterhin mit Strom versorgt. Sie müssen warten, bis diese LED erlischt, bevor Sie Komponenten entfernen.



Element	Beschreibung
1	Interne LED für aktiven Cache
2	Batterie

2. Suchen Sie den blauen Freigabehebel für die Batterie.
3. Entriegeln Sie den Akku, indem Sie den Entriegelungshebel nach unten und aus dem Controller entfernen.



Element	Beschreibung
1	Akkufreigaberiegel
2	Batterie

4. Heben Sie den Akku an, und schieben Sie ihn aus dem Controller.
5. Entfernen Sie die Abdeckung vom Ersatzcontroller.
6. Richten Sie den Ersatz-Controller so aus, dass der Steckplatz für die Batterie zu Ihnen zeigt.
7. Setzen Sie den Akku in einem leichten Abwärtswinkel in den Controller ein.

Sie müssen den Metallflansch an der Vorderseite der Batterie in den Schlitz an der Unterseite des Controllers einsetzen und die Oberseite der Batterie unter den kleinen Ausrichtstift auf der linken Seite des Controllers schieben.

8. Schieben Sie die Akkuverriegelung nach oben, um die Batterie zu sichern.

Wenn die Verriegelung einrastet, Haken unten an der Verriegelung in einen Metallschlitz am Gehäuse.

9. Drehen Sie den Controller um, um zu bestätigen, dass der Akku korrekt installiert ist.



Mögliche Hardware-Schäden — der Metallflansch an der Vorderseite der Batterie muss vollständig in den Schlitz am Controller eingesetzt werden (wie in der ersten Abbildung dargestellt). Wenn die Batterie nicht richtig eingesetzt ist (wie in der zweiten Abbildung dargestellt), kann der Metallflansch die Controllerplatine kontaktieren, was zu Schäden führt.

- **Korrekt** — der Metallflansch der Batterie ist vollständig in den Schlitz am Controller eingesetzt:



- **Falsch** — der Metallflansch der Batterie ist nicht in den Steckplatz an der Steuerung eingefügt:



10. Bringen Sie die Controllerabdeckung wieder an.

Schritt 5: HIC bei Bedarf auf neuen Controller verschieben

Wenn der ausgefallene Controller eine Host Interface Card (HIC) enthält, verschieben Sie die HIC vom ausgefallenen Controller auf den Ersatz-Controller.

Eine separate HIC wird nur für den E2800B-Controller verwendet. Die HIC wird auf der Haupt-Controller-Platine montiert und enthält zwei SPF-Anschlüsse.



Die Abbildungen in diesem Verfahren zeigen eine HIC mit 2 Ports. Die HIC in Ihrem Controller hat möglicherweise eine andere Anzahl von Ports.

E2800A

Ein E2800A-Controller verfügt nicht über eine HIC.

Die Abdeckung des E2800A-Controllers wieder anbringen und mit fortfahren [Schritt 6: Controller austauschen](#)

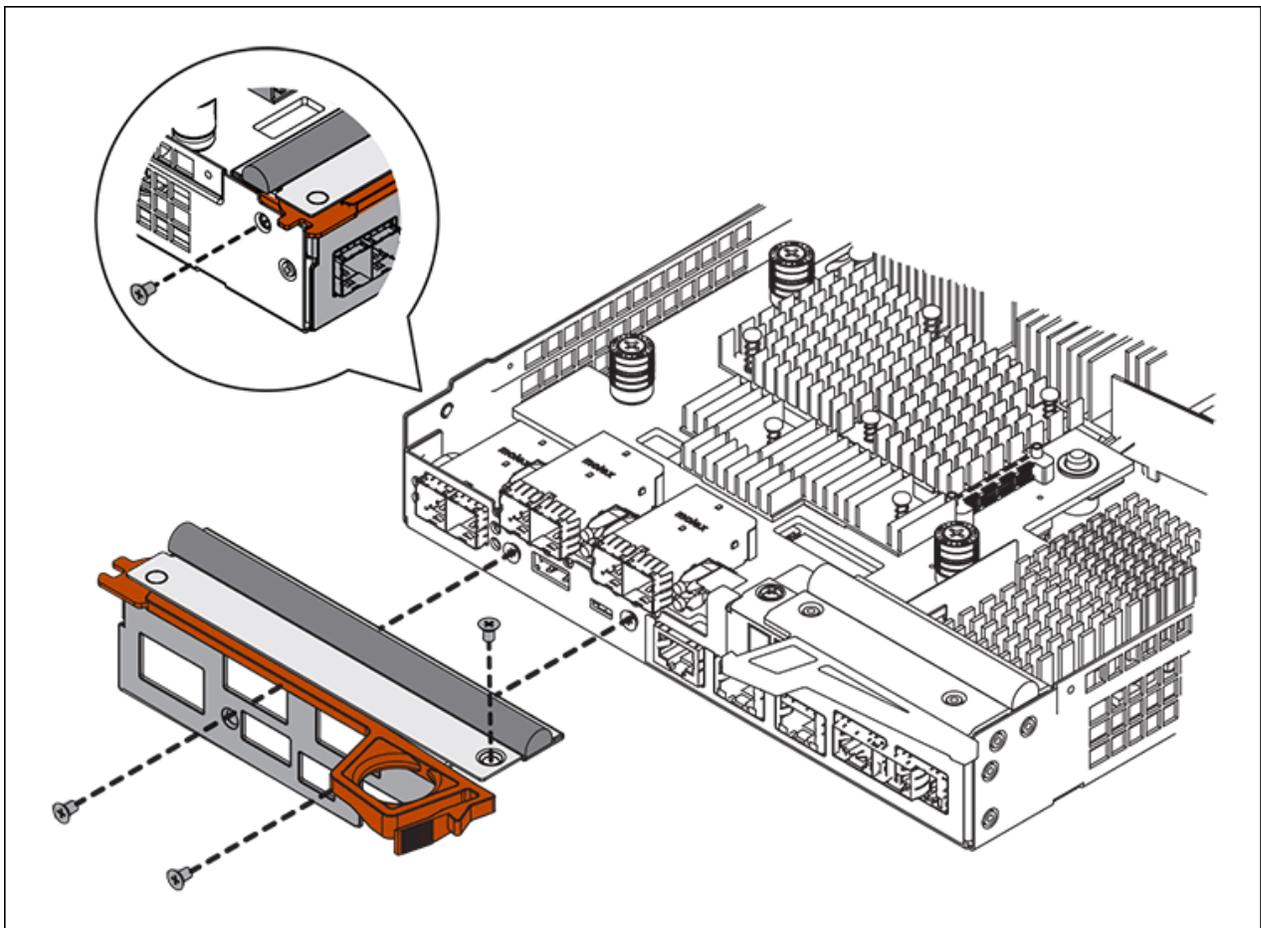
E2800B

Setzen Sie die HIC vom ausgefallenen E2800B-Controller auf den Ersatz-Controller.

Schritte

1. Entfernen Sie alle SFPs von der HIC.
2. Entfernen Sie mit einem #1 Kreuzschlitzschraubendreher die Schrauben, mit denen die HIC-Frontplatte am Controller befestigt ist.

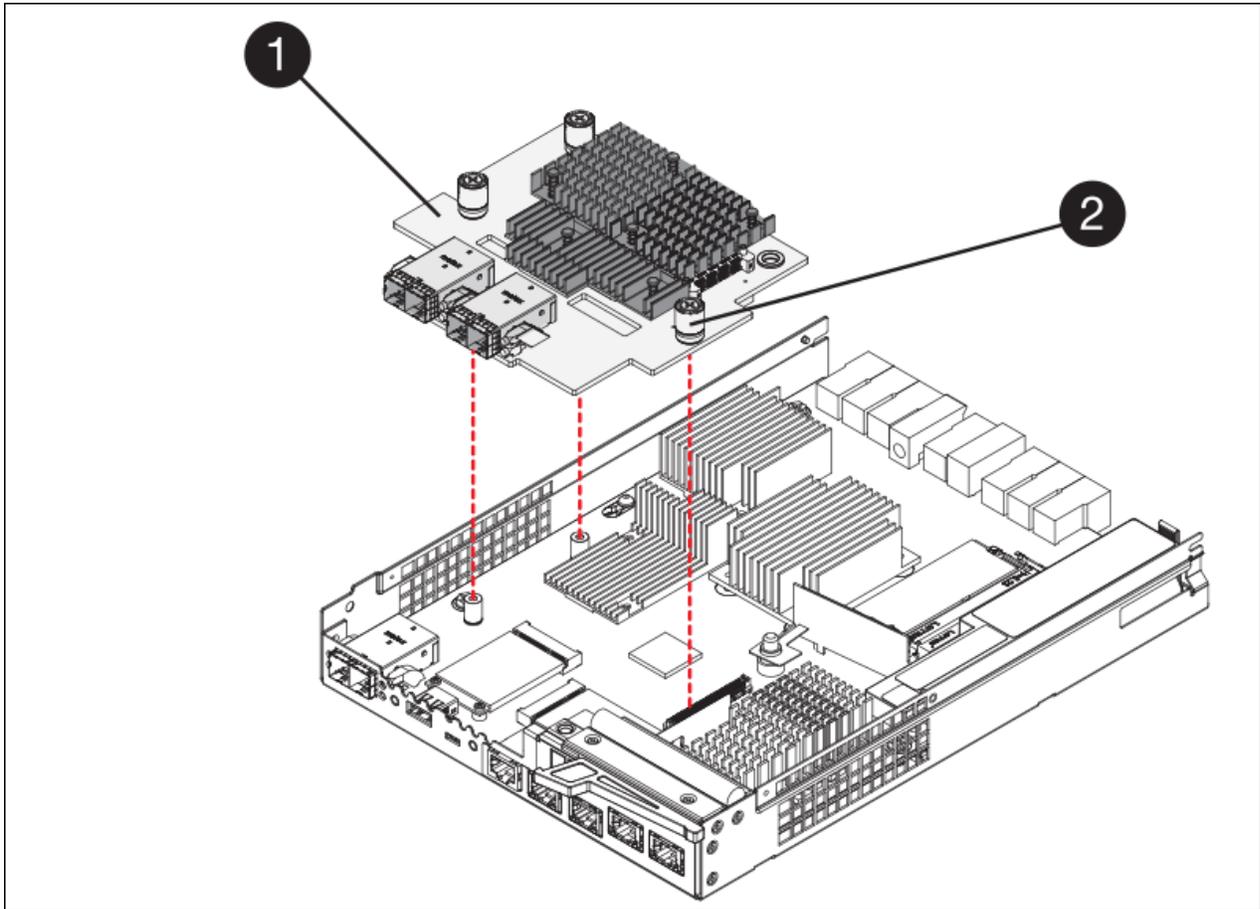
Es gibt vier Schrauben: Eine auf der Oberseite, eine auf der Seite und zwei auf der Vorderseite.



3. Entfernen Sie die HIC-Frontplatte.
4. Lösen Sie mit den Fingern oder einem Kreuzschlitzschraubendreher die drei Rändelschrauben, mit denen die HIC an der Controllerkarte befestigt ist.
5. Lösen Sie die HIC vorsichtig von der Controllerkarte, indem Sie die Karte nach oben heben und wieder zurückschieben.



Achten Sie darauf, dass die Komponenten auf der Unterseite der HIC oder auf der Oberseite der Controller-Karte nicht verkratzen oder stoßen.



Etikett	Beschreibung
1	Host-Schnittstellenkarte
2	Rändelschrauben

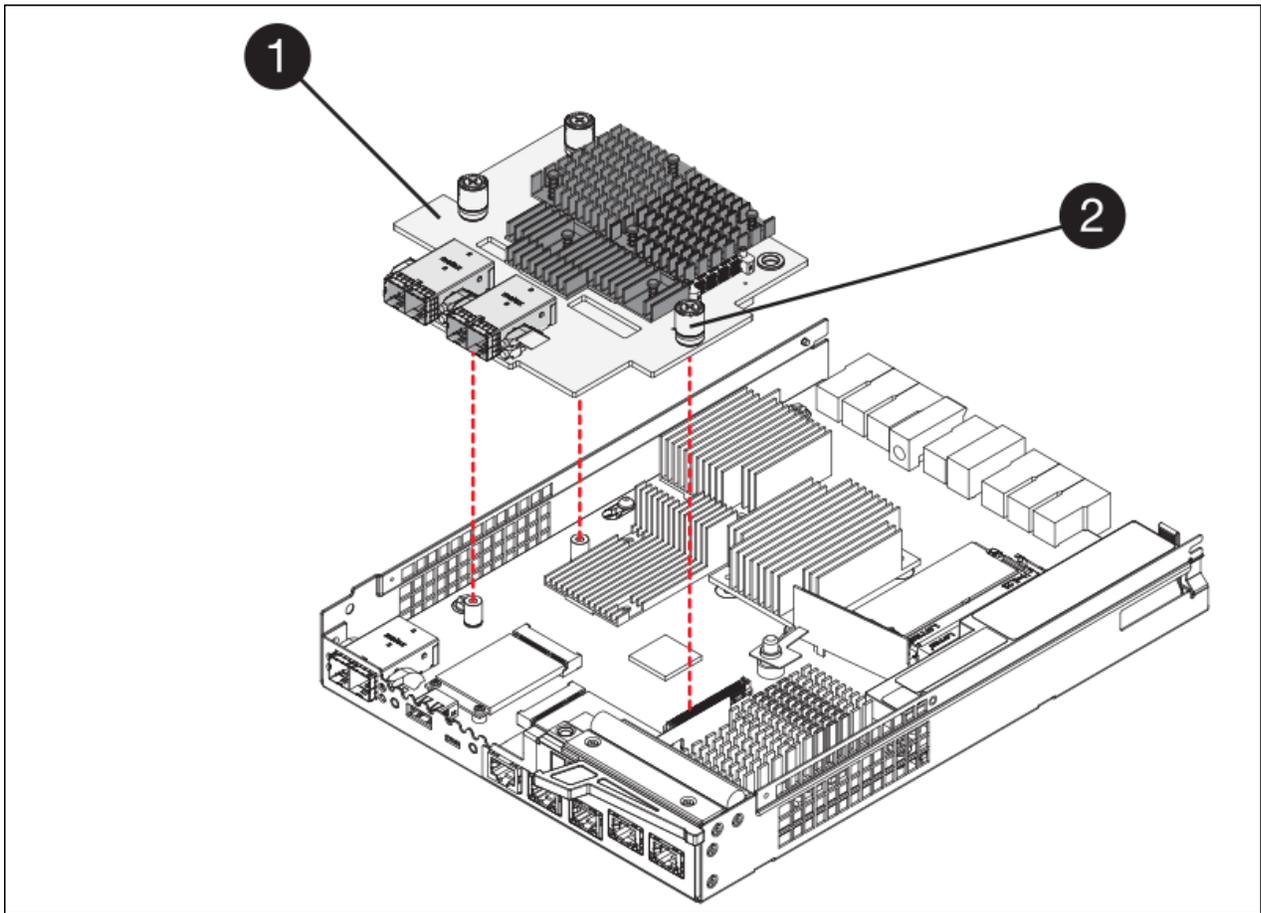
- Platzieren Sie die HIC auf einer statischen Oberfläche.
- Entfernen Sie mit einem #1 Kreuzschlitzschraubendreher die vier Schrauben, mit denen die leere Frontplatte an der Ersatzsteuerung befestigt ist, und entfernen Sie die Frontplatte.
- Richten Sie die drei Rändelschrauben der HIC an den entsprechenden Löchern am Ersatz-Controller aus, und richten Sie den Anschluss an der Unterseite der HIC an dem HIC-Schnittstellenanschluss auf der Controllerkarte aus.

Achten Sie darauf, dass die Komponenten auf der Unterseite der HIC oder auf der Oberseite der Controller-Karte nicht verkratzen oder stoßen.

- Senken Sie die HIC vorsichtig ab, und setzen Sie den HIC-Anschluss ein, indem Sie vorsichtig auf die HIC drücken.



Mögliche Geräteschäden — Vorsicht, den goldenen Bandanschluss für die Controller-LEDs nicht zwischen der HIC und den Rändelschrauben zu quetschen.

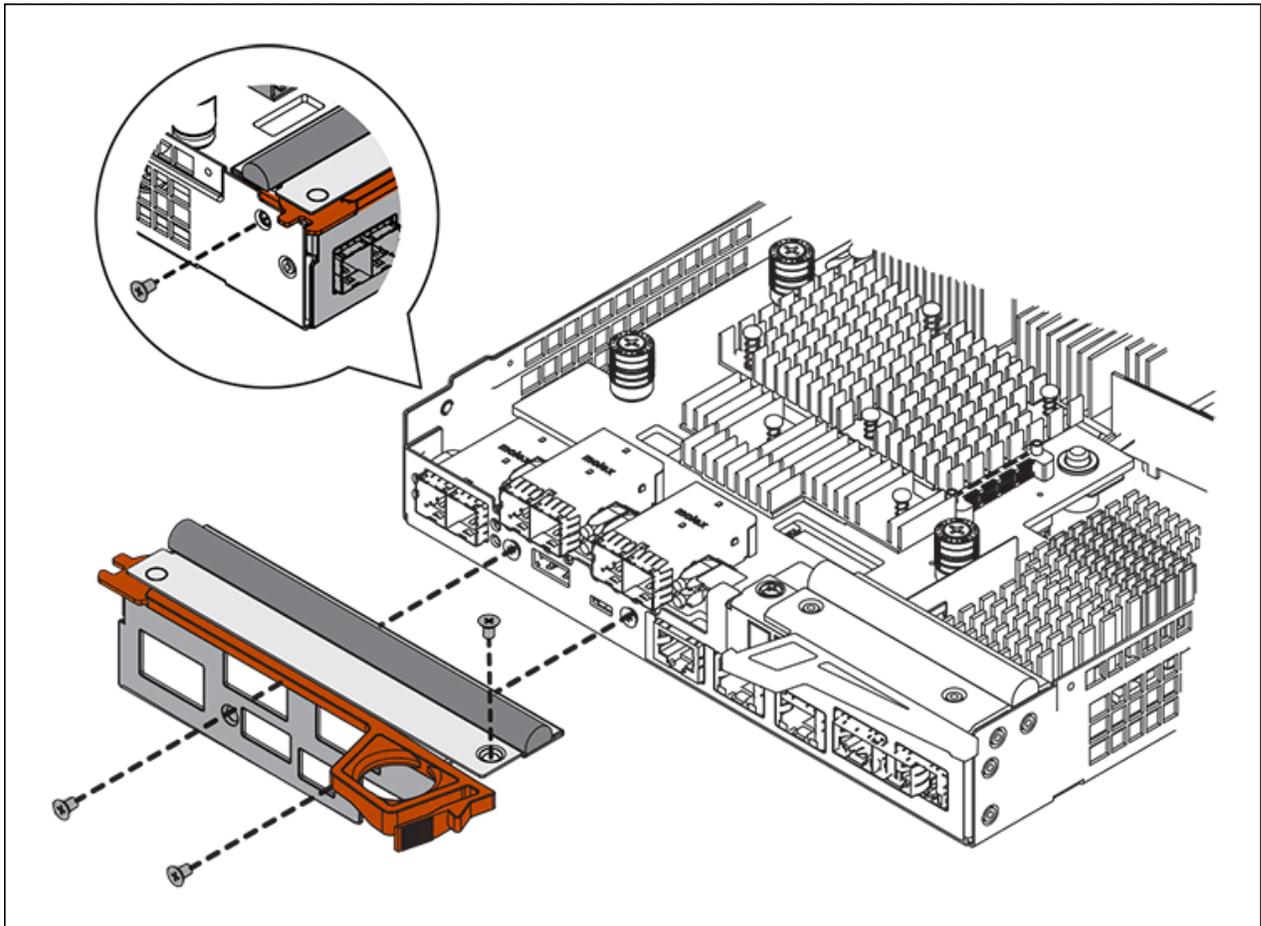


Etikett	Beschreibung
1	Host-Schnittstellenkarte
2	Rändelschrauben

10. Ziehen Sie die HIC-Rändelschrauben manuell fest.

Verwenden Sie keinen Schraubendreher, da Sie die Schrauben sonst möglicherweise zu fest anziehen.

11. Befestigen Sie mit einem #1 Kreuzschlitzschraubendreher die HIC-Frontplatte, die Sie vom ursprünglichen Controller entfernt haben, mit vier Schrauben an der neuen Steuerung.



12. Installieren Sie alle entfernten SFPs wieder auf der HIC.

Schritt 6: Controller austauschen

Installieren Sie den Ersatz-Controller und überprüfen Sie, ob er wieder an das Raster angeschlossen ist.

Schritte

1. Setzen Sie den Ersatzcontroller in das Gerät ein.
 - a. Drehen Sie den Controller um, so dass die abnehmbare Abdeckung nach unten zeigt.
 - b. Schieben Sie den Steuerknebel in die geöffnete Stellung, und schieben Sie ihn bis zum Gerät.
 - c. Bewegen Sie den Nockengriff nach links, um die Steuerung zu verriegeln.
 - d. Ersetzen Sie die Kabel und SFPs.
 - e. Schalten Sie das Controller-Shelf ein.
 - f. Warten Sie, bis der E2800 Controller neu gestartet wurde. Vergewissern Sie sich, dass auf der 7-Segment-Anzeige ein Status von angezeigt wird 99.
 - g. Legen Sie fest, wie Sie dem Ersatz-Controller eine IP-Adresse zuweisen.



Die Schritte zum Zuweisen einer IP-Adresse zum Ersatz-Controller hängen davon ab, ob Sie Management-Port 1 mit einem Netzwerk mit einem DHCP-Server verbunden haben und ob alle Laufwerke gesichert sind.

Wenn Management-Port 1 mit einem Netzwerk über einen DHCP-Server verbunden ist, erhält der neue Controller seine IP-Adresse vom DHCP-Server. Dieser Wert kann sich von der IP-Adresse des ursprünglichen Controllers unterscheiden.

2. Wenn die Appliance gesicherte Laufwerke verwendet, befolgen Sie die Anweisungen beim Austausch des E2800 Controllers, um den Sicherheitsschlüssel des Laufwerks zu importieren.
3. Stellen Sie den normalen Betriebsmodus des Geräts wieder ein. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert > Controller neu starten** aus, und wählen Sie dann **Neustart in StorageGRID** aus.



4. Überwachen Sie während des Neubootens den Status des Node, um zu bestimmen, wann er sich wieder im Raster angeschlossen hat.

Das Gerät wird neu gestartet und wieder in das Raster integriert. Dieser Vorgang kann bis zu 20 Minuten dauern.

5. Vergewissern Sie sich, dass das Neubooten abgeschlossen ist und dass der Node wieder dem Raster beigetreten ist. Überprüfen Sie im Grid Manager, ob auf der Seite Knoten ein normaler Status angezeigt wird (grünes Häkchen-Symbol  Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

DASHBOARD

ALERTS ✓

Current

Resolved

Silences

Rules

Email setup

NODES

TENANTS

ILM

CONFIGURATION

MAINTENANCE

SUPPORT

Nodes

View the list and status of sites and grid nodes.

Search...

Total node count: 14

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

6. Vom SANtricity System Manager sollte sichergestellt werden, dass der neue Controller optimal ist, und er sammelt Support-Daten.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Verwandte Informationen

["NetApp E-Series Systems Documentation Site"](#)

E5700SG Compute-Controller austauschen

Möglicherweise müssen Sie den E5700SG-Controller austauschen, wenn er nicht optimal funktioniert oder ausgefallen ist.

Bevor Sie beginnen

- Sie verfügen über einen Ersatzcontroller mit derselben Teilenummer wie der zu ersetzenden Controller.
- Sie haben die Anweisungen zur E-Series zum Austausch eines ausgefallenen E5700 Controllers heruntergeladen.



Wenn Sie weitere Details für einen bestimmten Schritt benötigen, sollten Sie die E-Series Anweisungen als Referenz verwenden. Verlassen Sie sich beim Austausch eines Controllers in der StorageGRID Appliance nicht auf die Anweisungen zur E-Series, da die Vorgehensweisen nicht identisch sind. In der Anleitung zur E-Series für den E5700 Controller wird beispielsweise beschrieben, wie Sie den Akku und die Host-Schnittstellenkarte (HIC) von einem ausgefallenen Controller entfernen und in einem Ersatz-Controller installieren. Diese Schritte gelten nicht für den E5700SG Controller.

- Sie verfügen über Etiketten, um jedes Kabel, das mit dem Controller verbunden ist, zu identifizieren.

Über diese Aufgabe

Auf den Appliance-Speicherknoten kann nicht zugegriffen werden, wenn Sie den Controller austauschen. Wenn der E5700SG-Controller ausreichend funktioniert, können Sie zu Beginn dieses Verfahrens ein

kontrolliertes Herunterfahren durchführen.



Wenn Sie den Controller vor dem Installieren der StorageGRID-Software ersetzen, können Sie nach Abschluss dieses Verfahrens möglicherweise nicht sofort auf den StorageGRID Appliance Installer zugreifen. Sie können zwar von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm der StorageGRID-Appliance zugreifen, können jedoch nicht von Hosts in anderen Subnetzen darauf zugreifen. Diese Bedingung sollte sich innerhalb von 15 Minuten lösen (wenn Einträge im ARP-Cache für die ursprüngliche Controller-Zeit erforderlich sind), oder Sie können den Zustand sofort löschen, indem Sie alle alten ARP-Cacheeinträge manuell vom lokalen Router oder Gateway löschen.

Schritte

1. Fahren Sie den E5700SG Controller herunter.

a. Melden Sie sich beim Grid-Node an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

b. Schalten Sie den E5700SG-Controller: + aus

shutdown -h now

c. Warten Sie, bis alle Daten im Cache-Speicher auf die Laufwerke geschrieben werden.

Die grüne LED „Cache aktiv“ auf der Rückseite des E2800 Controllers leuchtet, wenn Daten im Cache auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist.

2. Schalten Sie den Strom aus.

a. Wählen Sie auf der Startseite des SANtricity System Managers die Option **Vorgänge in Bearbeitung anzeigen**.

b. Vergewissern Sie sich, dass alle Vorgänge abgeschlossen sind.

c. Schalten Sie beide Netzschalter am Gerät aus.

d. Warten Sie, bis alle LEDs ausgeschaltet sind.

3. Wenn die mit dem Controller verbundenen StorageGRID-Netzwerke DHCP-Server verwenden:

a. Beachten Sie die MAC-Adressen für die Ports am Ersatz-Controller (auf Etiketten am Controller).

b. Bitten Sie den Netzwerkadministrator, die IP-Adresseinstellungen für den ursprünglichen Controller zu aktualisieren, um die MAC-Adressen für den Ersatz-Controller zu reflektieren.



Sie müssen sicherstellen, dass die IP-Adressen für den ursprünglichen Controller aktualisiert wurden, bevor Sie den Ersatz-Controller mit Strom versorgen. Andernfalls erhält der Controller neue DHCP-IP-Adressen, wenn er gebootet wird und kann möglicherweise nicht die Verbindung mit StorageGRID wiederherstellen. Dieser Schritt gilt für alle StorageGRID-Netzwerke, die mit dem Controller verbunden sind.

4. Entfernen Sie den Controller aus dem Gerät:

- a. Setzen Sie ein ESD-Armband an oder ergreifen Sie andere antistatische Vorsichtsmaßnahmen.
- b. Beschriften Sie die Kabel, und trennen Sie dann die Kabel und SFPs.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

- c. Lösen Sie die Steuerung vom Gerät, indem Sie die Verriegelung am Nockengriff so lange drücken, bis sie sich löst, und öffnen Sie dann den Nockengriff nach rechts.
- d. Schieben Sie den Regler mit zwei Händen und dem Nockengriff aus dem Gerät.



Verwenden Sie immer zwei Hände, um das Gewicht der Steuerung zu unterstützen.

5. Setzen Sie den Ersatzcontroller in das Gerät ein.
 - a. Drehen Sie den Controller um, so dass die abnehmbare Abdeckung nach unten zeigt.
 - b. Schieben Sie den Steuerknebel in die geöffnete Stellung, und schieben Sie ihn bis zum Gerät.
 - c. Bewegen Sie den Nockengriff nach links, um die Steuerung zu verriegeln.
 - d. Ersetzen Sie die Kabel und SFPs.
6. Schalten Sie das Gerät ein, und überwachen Sie die Controller-LEDs und die Sieben-Segment-Anzeigen.

Nachdem die Controller erfolgreich gestartet wurden, sollten in den sieben Segment-Displays folgende Werte angezeigt werden:

- Controller der E2800 Serie:

Der endgültige Zustand ist 99.

- E5700SG Controller:

Der endgültige Zustand ist HA.

7. Vergewissern Sie sich, dass der Appliance Storage Node im Grid Manager angezeigt wird und keine Alarme angezeigt werden.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Verwandte Informationen

["NetApp E-Series Systems Documentation Site"](#)

Tauschen Sie andere Hardwarekomponenten aus

Möglicherweise müssen Sie einen Controller-Akku, ein Laufwerk, einen Lüfter oder ein Netzteil in dem StorageGRID-Gerät austauschen.

Bevor Sie beginnen

- Sie haben das Verfahren zum Austausch der E-Series Hardware.
- Das Gerät war "[Wird in den Wartungsmodus versetzt](#)" Wenn das Verfahren zum Austausch von Komponenten erfordert, schalten Sie das Gerät aus.

Über diese Aufgabe

Anweisungen zum Austauschen des E2800 Controllers finden Sie in diesen Anweisungen. Diese Anweisungen beschreiben, wie Sie den Controller aus dem Gerät entfernen, den Akku aus dem Controller entfernen, den Akku einbauen und den Controller austauschen.

Um ein Laufwerk, einen Behälter mit Netzlüfter, einen Lüfterbehälter, einen Netzbehälter oder eine Laufwerksschublade im Gerät zu ersetzen, greifen Sie auf die Verfahren der E-Series zu, um die E2800 Hardware zu warten.

Anweisungen zum Austausch der SG5712-Komponente

FRU	Weitere Informationen finden Sie in den Anweisungen zur E-Series
Laufwerk	Austausch eines Laufwerks bei Shelves der E2800 mit 12 Laufwerken oder mit 24 Laufwerken
Lüfter-Behälter	Austausch eines Power-Fan-Behälters in E2800 Shelves

Anweisungen zum Austausch der SG5760 Komponenten

FRU	Weitere Informationen finden Sie in den Anweisungen zur E-Series
Laufwerk	Ersetzen eines Laufwerks in E2860 Shelves
Leistungsbehälter	Austausch eines Netzkanisters in E2860 Shelves
Gebläsebehälter	Austausch eines Lüftergehäuses in E2860 Shelves
Laufwerksschublade	Austauschen eines Laufwerksschubs in E2860 Shelves

Verwandte Informationen

["E2800 Controller austauschen"](#)

["NetApp E-Series Systems Documentation Site"](#)

SG5600-Appliance warten

Die SG5600 Appliance hat das Ende des Supports erreicht. Weitere Informationen zu Hardware-Aktualisierungen erhalten Sie von Ihrem NetApp Vertriebsmitarbeiter.

Wenn Sie Wartungsverfahren für SG5600-Hardware durchführen müssen, verwenden Sie die ["Anweisungen für StorageGRID 11.6"](#).

Instandhaltung der SG100 und SG1000 Hardware

Wartung von SG100 und SG1000 Appliances

Möglicherweise müssen Sie Wartungsarbeiten am Gerät durchführen. Bei den Verfahren

in diesem Abschnitt wird davon ausgegangen, dass die Appliance bereits als Gateway-Node oder Admin-Node in einem StorageGRID-System bereitgestellt wurde.

In diesem Abschnitt finden Sie spezifische Verfahren zur Wartung Ihrer SG100- oder SG1000-Appliance.

Siehe "[Allgemeine Verfahren](#)" Für Wartungsverfahren, die von allen Geräten verwendet werden.

Siehe "[Richten Sie die Hardware ein](#)" Für Wartungsverfahren, die auch während der Erstinstallation und -Konfiguration der Appliance durchgeführt werden.

Verfahren zur Wartungskonfiguration

Ein- und Ausschalten der Controller-ID-LED

Die blaue Identify-LED auf der Vorder- und Rückseite des Controllers kann eingeschaltet werden, um das Gerät in einem Datacenter zu lokalisieren.

Bevor Sie beginnen

Sie haben die BMC-IP-Adresse des Controllers, den Sie identifizieren möchten.

Schritte

1. Rufen Sie die BMC-Schnittstelle des Geräts auf.
2. Wählen Sie **Server Identify** Aus.

Der aktuelle Status der Identifizieren-LED ist ausgewählt.

3. Wählen Sie **EIN** oder **AUS**, und wählen Sie dann **Aktion ausführen**.

Wenn Sie **EIN** auswählen, leuchten die blauen Identifizieren-LEDs auf der Vorderseite (abgebildet) und der Rückseite des Geräts.



Wenn eine Blende auf dem Controller installiert ist, kann es schwierig sein, die vordere Identify-LED zu erkennen.

4. Schalten Sie die LED nach Bedarf ein und aus.

Verwandte Informationen

["Controller im Datacenter finden"](#)

"Greifen Sie auf die BMC-Schnittstelle zu"

Controller im Datacenter finden

Suchen Sie den Controller, um Hardware-Wartungsarbeiten oder Upgrades durchzuführen.

Bevor Sie beginnen

- Sie haben festgestellt, welcher Controller gewartet werden muss.
- (Optional) um den Controller in Ihrem Datacenter zu finden, "[Schalten Sie die blaue Identify-LED ein](#)".

Schritte

1. Ermitteln Sie den für die Wartung im Datacenter erforderlichen Controller.
 - Suchen Sie nach einer blau leuchtenden LED an der Vorder- oder Rückseite des Controllers.

Die vordere Identify-LED befindet sich hinter der Frontblende des Controllers und kann schwierig feststellen, ob die Blende montiert ist.



- Überprüfen Sie, ob die an der Vorderseite des jeden Controllers angebrachten Tags eine übereinstimmende Teilenummer erhalten.
2. Entfernen Sie die Frontverkleidung des Controllers, wenn eine installiert ist, um auf die Bedienelemente und Anzeigen auf der Vorderseite zuzugreifen.
3. Optional: Schalten Sie die blaue Identify-LED aus, wenn Sie sie zur Lokalisierung des Controllers verwendet haben.
 - Drücken Sie den Schalter Identifikation LED an der Vorderseite des Controllers.
 - Verwenden Sie die BMC-Schnittstelle des Controllers.

Fahren Sie die Service Appliance herunter

Fahren Sie die Service-Appliance herunter, um Hardware-Wartungsarbeiten durchzuführen.

Bevor Sie beginnen

- Sie haben den physischen Standort der Service-Appliance gefunden, die im Datacenter gewartet werden muss.

["Lokalisierung des Controllers in einem Rechenzentrum"](#).

Über diese Aufgabe

Um Serviceunterbrechungen zu vermeiden, sollten Sie die Services-Appliance während eines geplanten Wartungsfensters herunterfahren, wenn mit den üblichen Serviceunterbrechungen gerechnet wird.

Schritte

1. Fahren Sie das Gerät herunter:



Sie müssen ein kontrolliertes Herunterfahren des Geräts durchführen, indem Sie die unten angegebenen Befehle eingeben. Es ist eine Best Practice, nach Möglichkeit eine kontrollierte Abschaltung durchzuführen, um unnötige Warnmeldungen zu vermeiden, sicherzustellen, dass vollständige Protokolle verfügbar sind und Serviceunterbrechungen zu vermeiden.

- a. Wenn Sie sich noch nicht beim Grid-Knoten angemeldet haben, melden Sie sich mit PuTTY oder einem anderen ssh-Client an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

- b. Schalten Sie das Service-Gerät aus:

`shutdown -h now`

Dieser Befehl kann bis zu 10 Minuten in Anspruch nehmen.

2. Überprüfen Sie anhand einer der folgenden Methoden, ob das Gerät ausgeschaltet ist:
 - Sehen Sie sich die LED-Betriebsanzeige an der Vorderseite des Geräts an, und vergewissern Sie sich, dass sie ausgeschaltet ist.
 - Überprüfen Sie auf der Seite Power Control der BMC-Schnittstelle, ob das Gerät ausgeschaltet ist.

Ändern der Link-Konfiguration der Services Appliance

Sie können die Ethernet-Link-Konfiguration der Services Appliance ändern. Sie können den Port Bond-Modus, den Netzwerk-Bond-Modus und die Verbindungsgeschwindigkeit ändern.

Bevor Sie beginnen

- Das ist schon "[Das Gerät in den Wartungsmodus versetzt](#)".



In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den Wartungsmodus versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.

Über diese Aufgabe

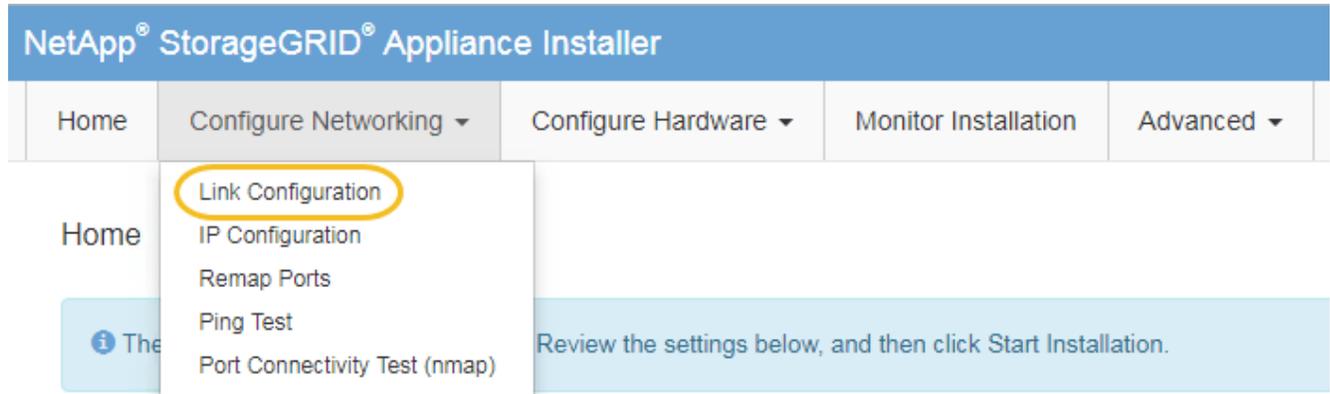
Die Ethernet Link-Konfiguration der Services Appliance kann wie folgt geändert werden:

- Ändern des **Port Bond Modus** von Fixed zu Aggregate oder von Aggregat zu Fixed

- Ändern des **Netzwerk-Bond-Modus** von Active-Backup zu LACP oder von LACP zu Active-Backup
- Aktivieren oder Deaktivieren von VLAN-Tagging oder Ändern des Werts einer VLAN-Tag-Nummer
- Ändern der Verbindungsgeschwindigkeit

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren** > **Link-Konfiguration** aus.



2. Nehmen Sie die gewünschten Änderungen an der Verbindungskonfiguration vor.

Weitere Informationen zu den Optionen finden Sie unter "[Netzwerkverbindungen konfigurieren](#)".

3. Wenn Sie mit Ihrer Auswahl zufrieden sind, klicken Sie auf **Speichern**.



Wenn Sie Änderungen am Netzwerk oder an der Verbindung vorgenommen haben, über die Sie verbunden sind, können Sie die Verbindung verlieren. Wenn die Verbindung nicht innerhalb von 1 Minute wiederhergestellt wird, geben Sie die URL für den StorageGRID-Appliance-Installer erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:

`https://services_appliance_IP:8443`

4. Nehmen Sie alle erforderlichen Änderungen an den IP-Adressen der Appliance vor.

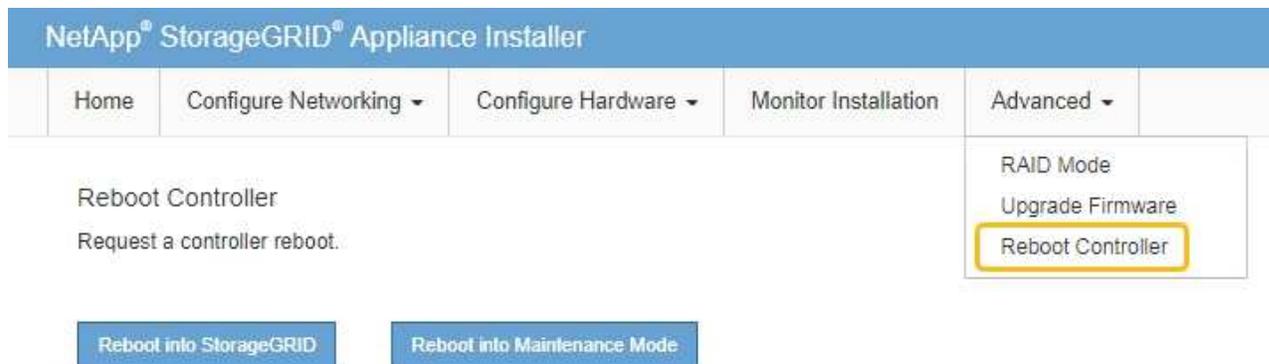
Wenn Sie Änderungen an den VLAN-Einstellungen vorgenommen haben, hat sich das Subnetz für die Appliance möglicherweise geändert. Informationen zum Ändern der IP-Adressen für die Appliance finden Sie unter "[Konfigurieren Sie StorageGRID-IP-Adressen](#)".

5. Wählen Sie im Menü die Option **Netzwerk konfigurieren** > **Ping-Test** aus.
6. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in Netzwerken zu prüfen, die möglicherweise von den Änderungen der Verbindungskonfiguration betroffen sind, die Sie bei der Konfiguration der Appliance vorgenommen haben.

Zusätzlich zu allen anderen Tests, die Sie durchführen möchten, bestätigen Sie, dass Sie die Grid Network IP-Adresse des primären Admin-Knotens und die Grid-Netzwerk-IP-Adresse von mindestens einem anderen Knoten pinggen können. Gehen Sie gegebenenfalls zu den Anweisungen für die Konfiguration von Netzwerkverbindungen zurück, und beheben Sie etwaige Probleme.

7. Sobald Sie zufrieden sind, dass die Änderungen an der Link-Konfiguration funktionieren, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

- Wählen Sie **Neustart in StorageGRID** aus, um den Controller neu zu starten, wobei der Knoten wieder in das Raster integriert wird. Wählen Sie diese Option, wenn Sie im Wartungsmodus ausgeführt werden und den Node in den normalen Betrieb zurückkehren möchten.
- Wählen Sie **Neustart im Wartungsmodus** aus, um den Controller neu zu starten, wobei der Knoten noch im Wartungsmodus bleibt. (Diese Option ist nur verfügbar, wenn sich der Controller im Wartungsmodus befindet.) Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Auf der Seite **NODES** sollte ein normaler Status (grünes Häkchen-Symbol) angezeigt werden (✓ Links neben dem Node-Namen) für den Appliance-Node. Dies bedeutet, dass keine Warnmeldungen aktiv sind und der Node mit dem Grid verbunden ist.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Hardware-Verfahren

Tauschen Sie ein oder beide Netzteile in der Service Appliance aus

Das Services-Gerät verfügt über zwei Netzteile für Redundanz. Wenn eines der Netzteile ausfällt, müssen Sie es so schnell wie möglich ersetzen, um sicherzustellen, dass der Compute-Controller über redundante Stromversorgung verfügt. Beide im Controller ausgeführten Netzteile müssen das gleiche Modell und die gleiche Stromleistung aufweisen.

Bevor Sie beginnen

- Das ist schon "[Physisch gelegener Controller](#)" Bei zu ersetzenden Netzteilen.
- Wenn Sie nur ein Netzteil ersetzen:
 - Sie haben das Ersatznetzteil entpackt und sichergestellt, dass es das gleiche Modell und die gleiche Stromleistung wie das Netzteil ist, das Sie ersetzen.
 - Sie haben bestätigt, dass das andere Netzteil installiert ist und in Betrieb ist.
- Wenn Sie beide Netzteile gleichzeitig ersetzen:
 - Sie haben die Ersatz-Netzteile entpackt und sichergestellt, dass sie das gleiche Modell und die gleiche Wattzahl haben.

Über diese Aufgabe

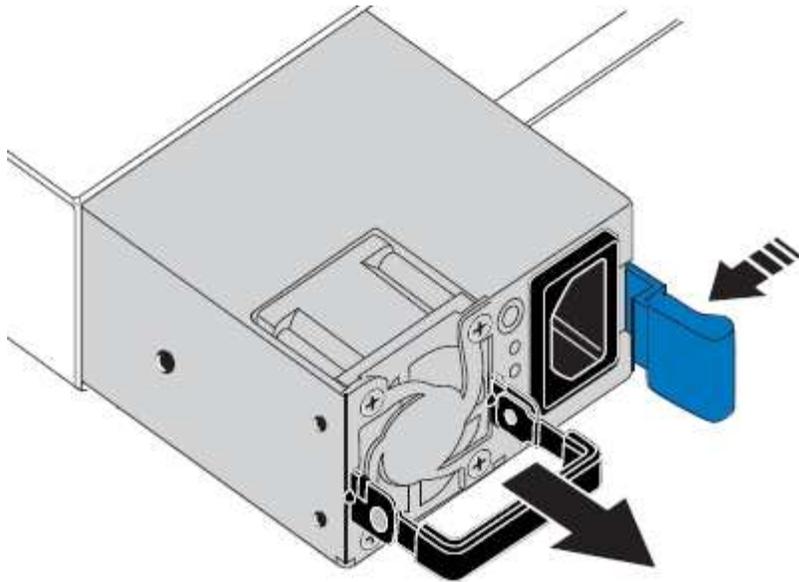
Die Abbildung zeigt die beiden Netzteile des SG100, auf die von der Rückseite des Geräts zugegriffen werden kann.



Die Netzteile für den SG1000 sind identisch.

Schritte

1. Wenn Sie nur ein Netzteil ersetzen, müssen Sie das Gerät nicht herunterfahren. Wechseln Sie zum [Ziehen Sie das Netzkabel ab](#) Schritt: Wenn Sie beide Netzteile gleichzeitig ersetzen, gehen Sie folgendermaßen vor, bevor Sie die Netzkabel abziehen:
 - a. "[Schalten Sie das Gerät aus](#)".
2. `[[Trenne den Netzstecker_Power_cordel, Start=2]]` Trennen Sie das Netzkabel von jedem zu ersetzenden Netzteil.
3. Den Nockengriff an der ersten zu ersetzenden Versorgung anheben.
4. Drücken Sie auf den blauen Riegel, und ziehen Sie das Netzteil heraus.

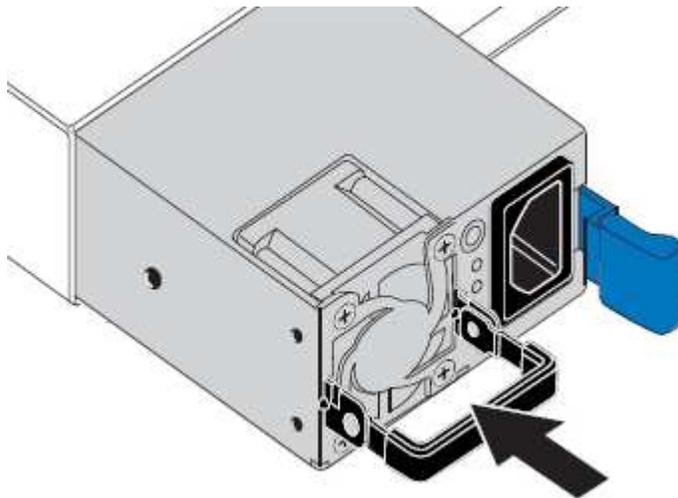


5. Schieben Sie das Ersatznetzteil mit der blauen Verriegelung nach rechts in das Gehäuse.



Beide Netzteile müssen das gleiche Modell und die gleiche Wattzahl haben.

Stellen Sie sicher, dass sich die blaue Verriegelung auf der rechten Seite befindet, wenn Sie die Ersatzeinheit einschieben.



6. Drücken Sie den Nockengriff nach unten, um die Ersatzstromversorgung zu sichern.

7. Wenn Sie beide Netzteile austauschen, wiederholen Sie die Schritte 2 bis 6, um das zweite Netzteil auszutauschen.

8. **"Schließen Sie die Stromkabel an die ersetzten Geräte an, und wenden Sie Strom an".**

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

Ersetzen Sie den Lüfter in der Service-Appliance

Die Service-Appliance verfügt über acht Lüfter. Wenn einer der Lüfter ausfällt, müssen Sie ihn so schnell wie möglich austauschen, um sicherzustellen, dass das Gerät

ordnungsgemäß gekühlt wird.

Bevor Sie beginnen

- Sie haben den Ersatzlüfter ausgepackt.
- Das ist schon "[Das Gerät befindet sich physisch](#)".
- Sie haben bestätigt, dass die anderen Lüfter installiert sind und ausgeführt werden.

Über diese Aufgabe

Auf den Geräteknoten kann nicht zugegriffen werden, wenn Sie den Lüfter austauschen.

Das Foto zeigt einen Ventilator für die Service Appliance. Die Lüfter sind zugänglich, nachdem Sie die obere Abdeckung vom Gerät entfernt haben.



Jede der beiden Netzteile enthält zudem einen Lüfter. Diese Lüfter sind in diesem Verfahren nicht enthalten.



Schritte

1. Fahren Sie das Gerät herunter.

a. Melden Sie sich beim Grid-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

b. Schalten Sie das Service-Gerät aus:

shutdown -h now

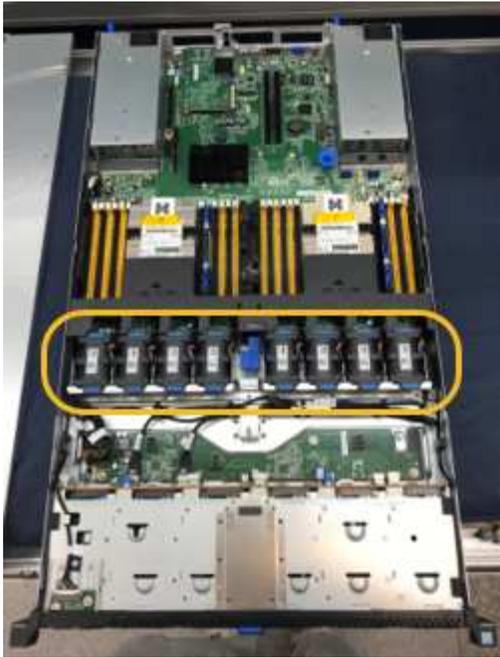
2. Verwenden Sie eine von zwei Methoden, um zu überprüfen, ob die Stromversorgung für die Service-Appliance ausgeschaltet ist:

- Die Betriebsanzeige-LED an der Vorderseite des Geräts ist aus.
- Die Seite Power Control der BMC-Schnittstelle zeigt an, dass das Gerät ausgeschaltet ist.

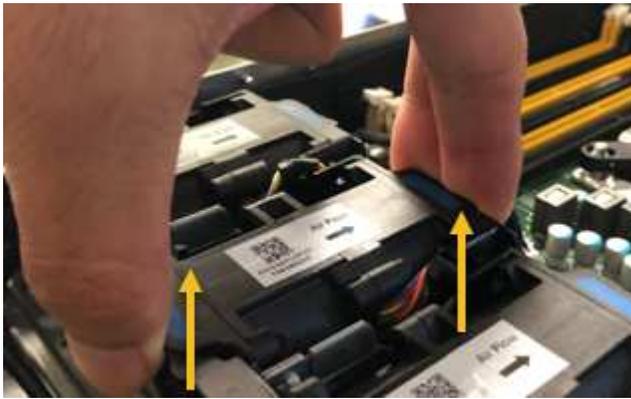
3. Ziehen Sie das Gerät aus dem Rack.

4. Heben Sie die Verriegelung an der oberen Abdeckung an, und entfernen Sie die Abdeckung vom Gerät.

5. Suchen Sie den Lüfter, der ausgefallen ist.

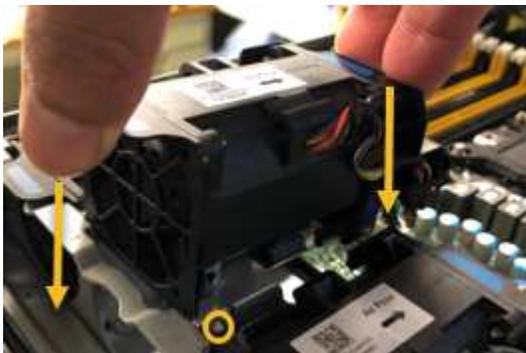


6. Heben Sie den defekten Lüfter aus dem Gehäuse.

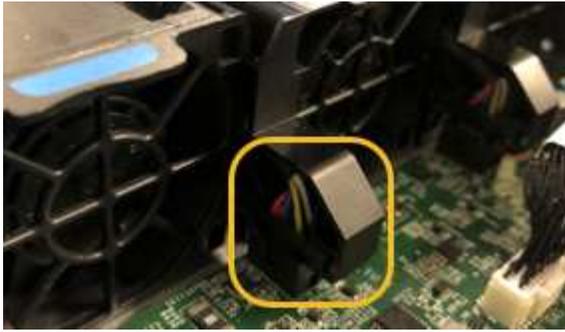


7. Schieben Sie den Ersatzlüfter in den offenen Steckplatz des Gehäuses.

Führen Sie die Kante des Lüfters mit dem Führungsstift nach oben. Der Stift ist im Foto eingekreist.



8. Drücken Sie den Lüfteranschluss fest in die Leiterplatte.



9. Setzen Sie die obere Abdeckung wieder auf das Gerät, und drücken Sie die Verriegelung nach unten, um die Abdeckung zu sichern.
10. Schalten Sie das Gerät ein, und überwachen Sie die Controller-LEDs und die Boot-Codes.

Verwenden Sie die BMC-Schnittstelle, um den Boot-up-Status zu überwachen.

11. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe ["Teilerückgabe Austausch"](#) Seite für weitere Informationen.

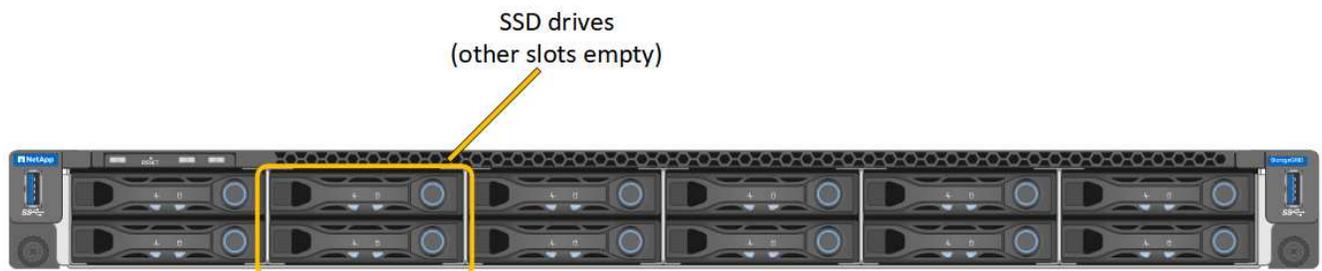
Ersetzen Sie das Laufwerk in der Services Appliance

Die SSDs in der Services-Appliance enthalten das Betriebssystem StorageGRID. Wenn die Appliance als Admin-Node konfiguriert ist, enthalten die SSDs außerdem Prüfprotokolle, Kennzahlen und Datenbanktabellen. Die Laufwerke werden aus Redundanzgründen mithilfe von RAID1 gespiegelt. Wenn eines der Laufwerke ausfällt, müssen Sie es so schnell wie möglich ersetzen, um Redundanz sicherzustellen.

Bevor Sie beginnen

- Das ist schon ["Das Gerät befindet sich physisch"](#).
- Sie haben überprüft, welches Laufwerk ausgefallen ist, indem Sie die linke LED gelb blinken.

Die beiden SSDs werden wie in der folgenden Abbildung gezeigt in die Steckplätze eingesetzt:



Wenn Sie das Arbeitslaufwerk entfernen, wird der Appliance-Node heruntergefahren. Informationen zur Anzeige von Statusanzeigen zur Überprüfung des Fehlers finden Sie unter.

- Sie haben das Ersatzlaufwerk erhalten.

- Sie haben einen angemessenen ESD-Schutz erhalten.

Schritte

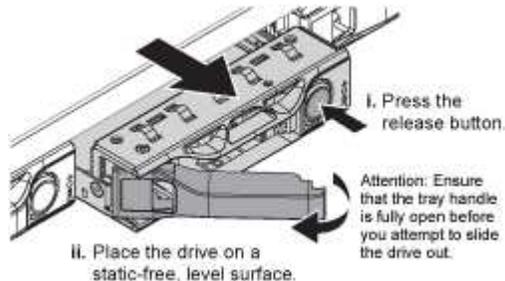
1. Stellen Sie sicher, dass die linke LED des zu ersetzenden Laufwerks gelb blinkt. Wenn im Grid Manager oder BMC UIs ein Laufwerkproblem gemeldet wurde, beziehen sich HDD02 oder HDD2 auf das Laufwerk im oberen Steckplatz und HDD03 oder HDD3 auf das Laufwerk im unteren Steckplatz.

Sie können den Status der SSDs auch mit Grid Manager überwachen. Wählen Sie **KNOTEN**. Wählen Sie anschließend aus **Appliance Node > Hardware**. Wenn ein Laufwerk ausgefallen ist, enthält das Feld Speicher-RAID-Modus eine Meldung darüber, welches Laufwerk ausgefallen ist.

2. Wickeln Sie das Gurt-Ende des ESD-Armbands um Ihr Handgelenk, und befestigen Sie das Clip-Ende auf einer Metallmasse, um eine statische Entladung zu verhindern.
3. Packen Sie das Ersatzlaufwerk aus und legen Sie es in der Nähe des Geräts auf eine statische, Ebene Fläche.

Alle Verpackungsmaterialien speichern.

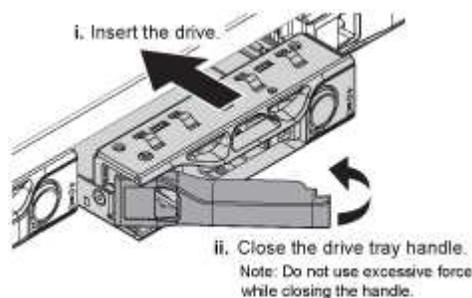
4. Drücken Sie die Entriegelungstaste am ausgefallenen Laufwerk.



Der Griff an den Antriebsfedern öffnet sich teilweise, und das Laufwerk löst sich aus dem Schlitz.

5. Öffnen Sie den Griff, schieben Sie das Laufwerk heraus und legen Sie es auf eine statisch freie, Ebene Oberfläche.
6. Drücken Sie die Entriegelungstaste am Ersatzlaufwerk, bevor Sie es in den Laufwerkschacht einsetzen.

Die Verriegelungsfedern öffnen sich.



7. Setzen Sie das Ersatzlaufwerk in den Steckplatz ein, und schließen Sie dann den Laufwerkgriff.



Beim Schließen des Griffs keine übermäßige Kraft anwenden.

Wenn das Laufwerk vollständig eingesetzt ist, hören Sie einen Klick.

Das Laufwerk wird automatisch mit gespiegelten Daten aus dem Arbeitslaufwerk neu aufgebaut. Sie

können den Status der Neuerstellung mithilfe des Grid Manager überprüfen. Wählen Sie **KNOTEN**. Wählen Sie anschließend aus **Appliance Node > Hardware**. Das Feld Speicher-RAID-Modus enthält eine Meldung „reBuilding“, bis das Laufwerk komplett neu aufgebaut ist.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Service-Appliance ersetzen

Möglicherweise müssen Sie das Gerät austauschen, wenn es nicht optimal funktioniert oder es ausgefallen ist.

Bevor Sie beginnen

- Sie haben ein Ersatzgerät mit der gleichen Teilenummer wie das Gerät, das Sie austauschen.
- Sie verfügen über Etiketten, um jedes Kabel zu identifizieren, das mit dem Gerät verbunden ist.
- Das ist schon "[Das Gerät befindet sich physisch](#)".

Über diese Aufgabe

Auf den StorageGRID-Node kann nicht zugegriffen werden, wenn Sie die Appliance ersetzen. Wenn das Gerät ausreichend funktioniert, können Sie zu Beginn dieses Verfahrens eine kontrollierte Abschaltung durchführen.



Wenn Sie die Appliance vor der Installation der StorageGRID-Software ersetzen, können Sie nach Abschluss dieses Verfahrens möglicherweise nicht sofort auf den StorageGRID Appliance Installer zugreifen. Sie können zwar von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm der StorageGRID-Appliance zugreifen, können jedoch nicht von Hosts in anderen Subnetzen darauf zugreifen. Diese Bedingung sollte sich innerhalb von 15 Minuten lösen (wenn ein ARP-Cache-Eintrag für die ursprüngliche Appliance-Zeit vorliegt), oder Sie können den Zustand sofort löschen, indem Sie alle alten ARP-Cache-Einträge manuell vom lokalen Router oder Gateway löschen.

Schritte

1. Zeigt die aktuellen Konfigurationen des Geräts an und zeichnet sie auf.
 - a. Melden Sie sich bei der zu ersetzenden Appliance an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
 - b. Geben Sie Ein: `run-host-command ipmitool lan print` Zeigt die aktuellen BMC-Konfigurationen für die Appliance an.
2. Fahren Sie das Gerät herunter: `shutdown -h now`
3. Wenn eine der Netzwerkschnittstellen auf dieser StorageGRID-Appliance für DHCP konfiguriert ist, müssen Sie möglicherweise die permanenten DHCP-Lease-Zuordnungen auf den DHCP-Servern aktualisieren, um auf die MAC-Adressen der Ersatz-Appliance zu verweisen. Das Update stellt sicher, dass der Appliance die erwarteten IP-Adressen zugewiesen werden. Siehe "[Aktualisieren Sie die MAC-](#)

Adressenverweise".

4. Entfernen und ersetzen Sie das Gerät:

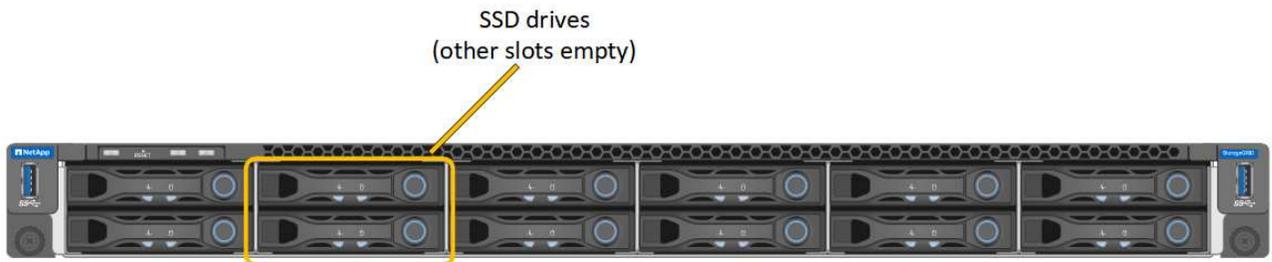
- a. Beschriften Sie die Kabel und trennen Sie dann die Kabel und alle Netzwerk-Transceiver.



Um Leistungseinbußen zu vermeiden, sollten Sie die Kabel nicht verdrehen, falten, zusammendrücken oder treten.

- b. Entfernen Sie das ausgefallene Gerät aus dem Schrank oder Rack.
- c. Übertragen Sie die beiden Netzteile, acht Lüfter und zwei SSDs von der ausgefallenen Appliance auf die Ersatz-Appliance.

Die beiden SSDs werden wie in der folgenden Abbildung gezeigt in die Steckplätze eingesetzt:



HDD02 oder HDD2 beziehen sich auf das Laufwerk im oberen Steckplatz, und HDD03 oder HDD3 beziehen sich auf das Laufwerk im unteren Steckplatz.

Befolgen Sie die Anweisungen zum Austausch dieser Komponenten.

- a. Setzen Sie das Ersatzgerät in den Schrank oder Rack ein.
- b. Ersetzen Sie die Kabel und optische Transceiver.
- c. Schalten Sie das Gerät ein, und warten Sie, bis es wieder in das Stromnetz eingesetzt wird.
- d. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

5. Melden Sie sich bei der ersetzten Appliance an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

6. Stellen Sie die BMC-Netzwerkverbindung für die ersetzte Appliance wieder her. Es gibt zwei Möglichkeiten:

- Verwenden Sie statische IP, Netzmaske und Gateway
 - Verwenden Sie DHCP, um eine IP, eine Netzmaske und ein Gateway zu erhalten
- i. Geben Sie zum Wiederherstellen der BMC-Konfiguration für die Verwendung einer statischen IP, Netzmaske und eines Gateways die folgenden Befehle ein:

```
run-host-command ipmitool lan set 1 ipsrc static
```

```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP
```

```
run-host-command ipmitool lan set 1 netmask Netmask_IP
```

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

- i. Geben Sie den folgenden Befehl ein, um die BMC-Konfiguration so wiederherzustellen, dass DHCP zum Abrufen einer IP, einer Netmask und eines Gateways verwendet wird:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

7. Stellen Sie nach dem Wiederherstellen der BMC-Netzwerkverbindung eine Verbindung zur BMC-Schnittstelle her, um die zusätzlich angewendete benutzerdefinierte BMC-Konfiguration zu prüfen und wiederherzustellen. Sie sollten beispielsweise die Einstellungen für SNMP-Trap-Ziele und E-Mail-Benachrichtigungen bestätigen. Siehe "[Konfigurieren Sie die BMC-Schnittstelle](#)".
8. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

Verwandte Informationen

["Statusanzeigen anzeigen anzeigen anzeigen"](#)

["Anzeigen von Startcodes für die Appliance"](#)

StorageGRID in Ihrer Umgebung aktivieren

Gehen Sie zu ["StorageGRID in Ihrer Umgebung aktivieren"](#) Um zu erfahren, wie Sie Applikationen in Ihrer StorageGRID Umgebung testen und einsetzen.

Die Dokumentationswebsite **storagegrid-enable** enthält Beispiele und Kochbücher, die die Produktdokumentation auf dieser Website erweitern und einige nächste Schritte zur Bewertung und Integration mit StorageGRID beschreiben.

Einige der Informationen enthalten:

- Liste validierter Lösungen von Drittanbietern für frühere und aktuelle StorageGRID Versionen.
- Produktfunktionshandbücher. Diese Leitfäden bieten beispielsweise alle Informationen, die Sie zum Erstellen von Cloud-Speicherpools benötigen.
- Tool- und Anwendungsleitfäden.
- API-Beispiele zur Verwendung von StorageGRID Funktionen wie S3-Verschlüsselung und S3-Objektsperre.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

["https://www.netapp.com/company/legal/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 der jeweiligen Eigentümer sein.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Datenschutzrichtlinie

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

https://library.netapp.com/ecm/ecm_download_file/ECMLP2885794

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.